Questa formola trasforma in prodotto la differenza tra il prodotto dei medi e quello degli estremi di un gruppo simmetrico qualunque $v_{n-\varrho}, v_n, v_s, v_{s-\varrho}$. Cambiando notazione (per comodità di quello che segue) si rappresenti il gruppo simmetrico con $v_\alpha, v_\beta, v_\gamma, v_\delta$; allora se si pone $\gamma-\beta=d$, $\beta-\alpha=\delta-\gamma=d'$ essa assume la forma

$$v_\beta v_\gamma - v_\alpha v_\delta = (-l)^\alpha v_{d'} v_{d+d'}. \tag{3'}$$

b) Ciò premesso sia $V_{n-\varrho}, V_n, V_s, V_{s+\varrho}$ un gruppo simmetrico della successione V. Se si costruisce l'espressione $V_n V_s - V_{n-\varrho} V_{s+\varrho}$ si avrà tenendo conto della (2)

$$V_n V_s - V_{n-\varrho} V_{s+\varrho} = (\beta v_{n-1} + l\alpha v_{n-2})(\beta v_{s-1} + l\alpha v_{s-2}) - \\ -(\beta v_{n-\varrho-1} + l\alpha v_{n-\varrho-2})(\beta v_{s+\varrho-1} + l\alpha v_{s+\varrho-2})$$

che sviluppando i prodotti assume la forma

$$V_n V_s - V_{n-\varrho} V_{s+\varrho} = l^2\alpha^2(v_{n-2} v_{s-2} - v_{n-\varrho-2} v_{s+\varrho-2}) + \\ + \beta^2(v_{n-1}v_{s-1} - v_{n-\varrho-1}v_{s+\varrho-1}) + l\alpha\beta[(v_{n-1}v_{s-2} - v_{n-\varrho-1}v_{s+\varrho-2}) + \\ + (v_{n-2}v_{s-1} - v_{n-\varrho-2}v_{s+\varrho-1})].$$

Le quantità entro le parentesi tonde sono differenze tra il prodotto dei medi e quello degli estremi dei seguenti gruppi simmetrici

$$v_{n-\varrho-2},\ v_{n-2},\ v_{s-2},\ v_{s+\varrho-2}$$
$$v_{n-\varrho-1},\ v_{n-1},\ v_{s-1},\ v_{s+\varrho-1}$$
$$v_{n-\varrho-1},\ v_{n-1},\ v_{s-2},\ v_{s+\varrho-2}$$
$$v_{n-\varrho-2},\ v_{n-2},\ v_{s-1},\ v_{s+\varrho-1}.$$

Ponendo $s-n=\delta$, e tenuto conto delle differenze tra gli indici, si avrà applicando la (3')

$$v_{n-2}v_{s-2} - v_{n-\varrho-2}v_{s+\varrho-2} = (-l)^{n-\varrho-2} v_\varrho v_{\delta+\varrho}$$
$$v_{n-1}v_{s-1} - v_{n-\varrho-1}v_{s+\varrho-1} = (-l)^{n-\varrho-1} v_\varrho v_{\delta+\varrho}$$
$$v_{n-1}v_{s-2} - v_{n-\varrho-1}v_{s+\varrho-2} = (-l)^{n-\varrho-1} v_\varrho v_{\delta+\varrho-1}$$
$$v_{n-2}v_{s-1} - v_{n-\varrho-2}v_{s+\varrho-1} = (-l)^{n-\varrho-2} v_\varrho v_{\delta+\varrho+1}$$

e quindi sostituendo si troverà

$$V_n V_s - V_{n-\varrho} V_{s+\varrho} = (-l)^{n-\varrho-1} v_\varrho v_{\delta+\varrho}(-\alpha^2 l + \beta^2) + \\ + (-l)^{n-\varrho-1}(l v_{\delta+\varrho-1} - v_{\delta+\varrho+1})\alpha\beta v_\varrho.$$

La differenza entro l'ultima parentesi, si trasforma in prodotto osservando che per la definizione è

$$v_{\delta+\varrho+1} = h v_{\delta+\varrho} + l v_{\delta+\varrho-1}$$

e quindi

$$l v_{\delta+\varrho-1} - v_{\delta+\varrho+1} = -h v_{\delta+\varrho}$$

e pertanto sarà ancora

$$V_n V_s - V_{n-\varrho} V_{s+\varrho} = (-l)^{n-\varrho-1}(\beta^2 - \alpha^2 l - h\alpha\beta) v_\varrho v_{\delta+\varrho} \tag{4}$$

Questa formola trasforma la differenza tra il prodotto dei termini medi e quello degli estremi di un gruppo simmetrico qualunque $V_{n-\varrho}$, V_n, V_s, $V_{s+\varrho}$. Applicandola al gruppo equisimmetrico $V_{n-\varrho-1}$, V_{n-1}, V_{s-1}, $V_{s+\varrho-1}$ avremo

$$V_{n-1} V_{s-1} - V_{n-\varrho-1} U_{s+\varrho-1} = (-l)^{n-\varrho-2} (\beta^2 - \alpha^2 l - h\alpha\beta)\, v_\varrho\, v_{\delta+\varrho}$$

e quindi si ha

$$(5) \qquad \frac{V_n V_s - V_{n-\varrho} V_{s+\varrho}}{V_{n-1} V_{s-1} - V_{n-\varrho-1} V_{s+\varrho-1}} = -l$$

che dimostra appunto il teorema enunciato.

5. Il procedimento tenuto nella dimostrazione precedente è valido, come si vede facilmente, anche per $s = n$; in questa ipotesi osservando che è $\delta = s - n = 0$ le formole (3) (4) (5) divengono

$$(6) \qquad v^2_n - v_{n+\varrho} v_{n-\varrho} = (-l)^{n-\varrho} v_\varrho^2$$

$$(7) \qquad V^2_n - V_{n+\varrho} V_{n-\varrho} = (-l)^{n-\varrho-1} (\beta^2 - \alpha^2 l - h\alpha\beta)\, v_\varrho^2$$

$$(8) \qquad \frac{V^2_n - V_{n-\varrho} V_{n+\varrho}}{V^2_{n-1} - V_{n-\varrho-1} V_{n+\varrho=1}} = -l$$

Le prime due forniscono una trasformazione della differenza tra il quadrato del termine medio ed il prodotto degli estremi nei gruppi simmetrici di tre termini, $(v_{n-\varrho}\, v_n\, v_{n+\varrho})$ e $(V_{n-\varrho}\, V_n\, V_{n+\varrho})$, l'ultima contiene il seguente

Teorema. — *In ogni sistema ordinato di gruppi equisimmetrici di tre termini, le differenze tra il quadrato del termine medio ed il prodotto degli estremi in ciascun gruppo, formano una progressione geometrica avente per quoziente il numero intero negativo* —l.

6. Insieme alla successione V consideriamone un'altra

$$V' \equiv V'_1, V'_2, V'_3, \ldots V'_n, \ldots$$

in cui i termini iniziali V'_1, V'_2 sono rispettivamente uguali a due interi positivi α', β' comunque scelti, e gli altri termini sono individuati mediante la relazione

$$V'_n = hV_{n-1} + lV_{n-2}$$

dove h, l sono i coefficienti *già fissati*. Calcoliamo il determinante di secondo ordine

$$\begin{vmatrix} V_n & V_s \\ V'_n & V'_s \end{vmatrix} \quad (n < s)$$

formato con due coppie corrispondenti nelle due successioni, cioè l'espressione $V_n V'_s - V'_n V_s$. Sostituendo alle V le loro espressioni in funzione delle v calcolate per mezzo della (2) si avrà

$$V_n V'_s - V_s V'_n = (\beta v_{n-1} + l\alpha v_{n-2})(\beta' v_{s-1} + l\alpha' v_{s-2}) -$$
$$- (\beta v_{s-1} + l\alpha v_{s-2})(\beta' v_{n-1} + l\alpha' v_{n-2})$$

che sviluppando i prodotti diviene

$$V_n V'_s - V_s V'_n = l(\alpha'\beta - \alpha\beta')(v_{n-1} v_{s-2} - v_{s-1} v_{n-2}).$$

Si consideri il gruppo simmetrico

$$v_{n-2},\ v_{n-1},\ v_{s-2},\ v_{s-1}$$

Posto $s - n = \delta$, la differenza degli indici medi è

$$(s-2) - (n-1) = \delta - 1$$

e quindi applicando la formola (3') si avrà

$$v_{n-1} v_{s-2} - v_{n-2} v_{s-1} = (-l)^{n-2} v_1 v_\delta$$

e poichè $v_1 = 1$, risulterà, sostituendo

(9) $$V_n V'_s - V_s V'_n = -(-l)^{n-1} (\alpha'\beta - \alpha\beta') v_\delta$$

che è la formola cercata.

7. Sostituendo ad s il suo uguale $n + \delta$ si ha

$$V_n V'_{n+\delta} - V_{n+\delta} V'_n = -(-l)^{n-1} (\alpha'\beta - \alpha\beta') v_\delta$$

per qualunque valore di n; mutando quindi n in $n + \rho$ e dividendo membro a membro si ha

$$\frac{V_{n+\rho} V'_{n+\delta+\rho} - V_{n+\delta+\rho} V'_{n+\rho}}{V_n V'_{n+\rho} - V_{n+\delta} V'_n} = (-l)^\rho$$

surrogando nuovamente $n + \delta$ con s si ha

$$\frac{V_{n+\rho} V'_{s+\rho} - V_{s+\rho} V'_{n+\rho}}{V_n V'_s - V_s V'_n} = (-l)^\rho.$$

E poichè gli indici del numeratore superano di ρ quelli del denominatore, così questa relazione prova che *la successione di determinanti di secondo ordine*

$$\ldots \begin{vmatrix} V_n & V_s \\ V'_n & V'_s \end{vmatrix} \begin{vmatrix} V_{n+\rho} & V_{s+\rho} \\ V'_{n+\rho} & V'_{s+\rho} \end{vmatrix} \begin{vmatrix} V_{n+2\rho} & V_{s+2\rho} \\ V'_{n+2\rho} & V'_{s+2\rho} \end{vmatrix} \ldots$$

costituisce una progressione geometrica che ha per quoziente il numero intero $(-l)^\rho$.

8. Della formola (9) faremo subito un'altra applicazione. Come abbiamo visto in principio del numero precedente possiamo scrivere per valori arbitrari di n, δ

$$V_n V'_{n+\delta} - V_{n+\delta} V'_n = -(-l)^{n-1} (\alpha'\beta - \alpha\beta') v_\delta$$

Cangiando n in $n + \delta$ si ha:

$$V_{n+\delta} V'_{n+2\delta} - V_{n+2\delta} V'_{n+\delta} = -(-l)^{n+\delta-1} (\alpha'\beta - \alpha\beta') v_\delta$$

Moltiplicando la prima per $(-l)^\delta$ si ricava

$$V_{n+\delta} V'_{n+2\delta} - V_{n+2\delta} V'_{n+\delta} = (-l)^\delta V_n V'_{n+\delta} - (-l)^\delta V_{n+\delta} V'_n$$

ossia

$$\frac{V_{n+2\delta} + (-l)^\delta V_n}{V_{n+\delta}} = \frac{V'_{n+2\delta} + (-l)^\delta V'_n}{V'_{n+\delta}}.$$

Questa relazione prova che fissati n, δ il rapporto $\frac{V_{n+2\delta} + (-l)^\delta V_n}{V_{n+\delta}}$ ha un valore che è *indipendente* dai termini iniziali della successione, e per conseguenza sarà anche

$$\frac{V_{n+2\delta} + (-l)^\delta V_n}{V_{n+\delta}} = \frac{v_{n+2\delta} + (-l)^\delta v_n}{v_{n+\delta}}$$

(non essendo altro la v che la V quando $\alpha = 1$, $\beta = h$), ed anche mutando n in $n - \delta$

$$\frac{V_{n+\delta} + (-l)^\delta V_{n-\delta}}{V_n} = \frac{v_{n+\delta} + (-l)^\delta v_{n-\delta}}{v_n}.$$

Proponiamoci ora di calcolare il quoziente che è al secondo membro; a tal fine osserviamo che nel gruppo simmetrico

$$v_{\delta-1},\ v_\delta,\ v_{n-1},\ v_n$$

la differenza d tra gli indici medi è $n - \delta - 1$, quella d' tra un indice estremo e quello medio prossimo è 1, quindi applicando la (3') si avrà

$$v_\delta v_{n-1} - v_n v_{\delta-1} = (-l)^{\delta-1} v_{n-\delta}$$

e moltiplicando per l

$$l v_\delta v_{n-1} - l v_n v_{\delta-1} = -(-l)^\delta v_{n-\delta}.$$

Ma per la (1) è

$$v_{n+\delta} = v_{\delta+1} v_n + l v_\delta v_{n-1}$$

che sottratta dalla precedente dà

$$v_{n+\delta} + (-l)^\delta v_{n-\delta} = v_n (l v_{\delta-1} + v_{\delta+1})$$

e perciò

$$\frac{v_{n+\delta} + (-l)^\delta v_{n-\delta}}{v_n} = l v_{\delta-1} + v_{\delta+1}.$$

Si conclude in generale

$$\frac{V_{n+\delta} + (-l)^\delta V_{n-\delta}}{V_n} = l v_{\delta-1} + v_{\delta+1} \ (*) \tag{10}$$

(*) È escluso dal procedimento tenuto il caso di $\delta = 1$; la formola trovata in tal caso diviene $\frac{V_{n+1} - l V_{n-1}}{V_n} = l v_0 + v_2$ col secondo membro privo di significato.

Ma poichè dalla definizione della successione V risulta $\frac{V_{n+1} - l V_{n-1}}{V_n} = h = v_2$ così la (10) diviene ancora applicabile ponendo $v_0 = 0$.

Il secondo membro è intero; positivo, indipendente da α, β e da n, pertanto possiamo concludere:

La funzione

$$\frac{V_{n+\delta} + (-l)^{\delta}\, V_{n-\delta}}{V_n}$$

è un intero positivo costante al variare di n, *e indipendente dai termini iniziali* α, β *della successione* V

Osservando che dal gruppo simmetrico

$$V_{n-\delta}\,,\ V_n\,,\ V_{n+\delta}$$

al variare del solo n si deducono tutti i gruppi ad esso equisimmetrici, il teorema precedente può enunciarsi anche così:

La funzione

$$\frac{V_{n+\delta} + (-l)^{\delta}\, V_{n-\delta}}{V_n}$$

formata coi termini del gruppo simmetrico $V_{n-\delta}$, V_n, $V_{n+\delta}$, *è un intero positivo, costante in tutti i gruppi equisimmetrici al dato, ed è indipendente inoltre da* α, β

II.

9. Passiamo ora ad occuparci di alcune proprietà speciali della successione v. Dalla relazione fondamentale (1), dove n, s sono arbitrari, discende subito col porre $n = s + 1$

$$v_{2s+1} = v^2_{s+1} + l v^2_s$$

Quindi: *Ogni termine di indice dispari in* v *è rappresentabile mediante la forma quadratica* $x^2 + ly^2$. *e con un sistema di valori per* x, y *che sono termini consecutivi della successione stessa.*

In altri termini: *L'equazione indeterminata quadratica*

$$x^2 + ly^2 = x_{2s+1}$$

ammette la soluzione in numeri interi

$$x = \pm\, v_{s+1}\,,\ y = \pm\, v_s\,.$$

10. Dalla (1) si ricava ancora che *se* r *è multiplo di* i *è anche* v_r *multiplo di* v_i.

Infatti, supposto $r = mi$ con $m > 1$, vi si faccia $s = i$ $n = (m-1)i$; si deduce

$$v_{mi} = v_{i+1} \cdot v_{(m-1)i} + l v_i v_{(m-1)i-1}$$

e quindi

$$(1') \qquad \frac{v_{mi}}{v_i} = l v_{(m-1)i-1} + v_{i+1} \frac{v_{(m-1)i}}{v_i}$$

Affinchè sia intero il quoziente $\frac{v_{mi}}{v_i}$, è dunque sufficiente che sia tale $\frac{v_{(m-1)i}}{v_i}$. Ma per $m=2$ si ha:

$$\frac{v_{2i}}{v_i} = l v_{i-1} + v_{i+1}.$$

Essendo dunque intero $\frac{v_{2i}}{v_i}$ saranno interi ancora $\frac{v_{3i}}{v_i}\ \frac{v_{4i}}{v_i} \ldots \frac{v_{mi}}{v_i} \ldots$ Del resto è facile esprimere in generale il quoziente $\frac{v_{mi}}{v_i}$ sotto forma intera. Se infatti nella (1') si attribuiscono successivamente ad m i valori 2, 3, 4, ... si ricava facilmente valendosi ogni volta della relazione precedente

$$\frac{v_{mi}}{v_i} = l v_{(m-1)i-1} + l v_{(m-2)i-1} \cdot v_{i+1} + l v_{(m-3)i-1} v_{i+1}^2 + \ldots$$
$$+ l v_{2i-1} \cdot v_{i+1}^{m-3} + l v_{i-1} \cdot v_{i+1}^{m-2} + v_{i+1}^{m-1}.$$

Un'altra espressione, notevole, del quoziente $\frac{v_{mi}}{v_i}$ si ottiene così: nella (1) si ponga invece $s=(m-1)i$, $n=i$ e si divida poi i due membri dell'eguaglianza trovata per v_i; risulta

$$\frac{v_{mi}}{v_i} = v_{(m-1)i+1} + l v_{i-1} \frac{v_{(m-1)i}}{v_i}$$

e da questa ponendo successivamente $m=2, 3, 4, \ldots, m$ si deduce la formula

$$\frac{v_{mi}}{v_i} = v_{(m-1)i+1} + l v_{(m-2)i+1} \cdot v_{i-1} + l^2 v_{(m-3)i+1} \cdot v_{i-1}^2 +$$
$$+ l^3 v_{(m-4)i+1} \cdot v_{i-1}^3 + \ldots + l^{m-2} v_{i+1} v_{i+1}^{m-2} + l^{m-1} v_{i-1}^{m-1}$$

ed altre ancora, sempre valendosi della (1), si potrebbero stabilire.

II. Quando i numeri h, l sono dati comunque, può accadere che nella successione v cadano oltre i termini v_{mi} $(m=1, 2, 3, \ldots \infty)$ altri multipli di v_i; ma se supponiamo *h, l primi tra loro* possiamo dimostrare che *la successione*

$$v_i, v_{2i}, v_{3i}, \ldots, v_{mi}, \ldots$$

contiene tutti i multipli di v_i *appartenenti alla successione* v. Premettiamo a tal fine i seguenti lemmi:

1°. *Se* h, l *sono primi tra loro* v_n, l *sono pure primi tra loro per qualunque valore di* n.

Infatti dalla relazione

$$v_n = hv_{n-1} + lv_{n-2}$$

discende che ogni divisore d comune ai numeri v_n, l è divisore del prodotto hv_{n-1}: ma a causa dell'ipotesi è d primo con h quindi sarà pure divisore di v_{n-1}. Il numero d essendo così divisore comune ai numeri v_{n-1}, l sarà pure divisore di v_{n-2} e così pure di $v_{n-3}, v_{n-4}, \dots v_1$. Ma è per ipotesi $v_1 = 1$ quindi $d = 1$ come si voleva dimostrare.

2°. *Se* h, l *sono primi tra loro, due termini consecutivi* v_{n-1}, v_n *sono pure primi tra loro.*

Infatti dalla relazione

$$v_n = hv_{n-1} + lv_{n-2}$$

risulta che ogni divisore d comune ai termini v_{n-1}, v_n è pure divisore del prodotto lv_{n-2}; ma per il lemma precedente v_n, l sono primi tra loro, quindi anche d (che è divisore di v_n) sarà primo con l e perciò sarà divisore di v_{n-2}. Il numero d è dunque un divisore comune ai termini v_{n-1}, v_{n-2}; si concluderà dunque che è divisore di v_{n-3}, $v_{n-4}, \dots v_1$. Ma $v_1 = 1$, onde $d = 1$ come si voleva provare.

Ciò premesso, torniamo alla questione enunciata in principio del paragrafo, e supponiamo che tra due multipli di v_i come v_{mi}, $v_{(m+1)i}$ cada un termine multiplo anch'esso di v_i: esso sarà necessariamente della forma $v_{mi+\rho}$ con $\rho < i$. Ora se nella (1) si cangia n in mi ed s in ρ si trova

$$v_{mi+\rho} = v_{mi}\, v_{\rho+1} + lv_\rho\, v_{mi-1}.$$

E poichè $v_{mi+\rho}$, v_{mi} sono multipli di v_i tale sarà pure il prodotto $lv_\rho v_{mi-1}$. Ma v_i ed l sono, per il lemma 1°, primi fra loro; e primi tra loro sono pure v_i e v_{mi-1}; (perchè ogni loro divisore comune d è pure divisore comune ai termini v_{mi}, v_{mi-1} quindi per il lemma 2°, è $d = 1$) dovrà essere dunque v_ρ multiplo di v_i; ciò che è assurdo poichè essendo per ipotesi $\rho < i$, è anche $v_\rho < v_i$.

Il teorema è pertanto dimostrato, e potremo concludere riassumendo:

Teorema. — *Se* h, l *sono primi fra loro, la condizione necessaria e sufficiente affinchè* v_r *sia multiplo di* v_i *è chè* r *sia multiplo di* i.

Corollario I. — *I termini von indice composto maggiore di 4, sono numeri composti,*(*) *e se* $h > 1$ *è composto anche* v_4. (**)

Infatti se v_α è uno di tali termini, α avrà un divisore $i > 2$ e quindi v_α ammetterà il divisore $v_i > 1$, perchè è sempre $v_3 > 1$ e la

(*) Con queste parole devesi enunciare il corollario primo al n. 5 della nota citata.

(**) Dalla v per $h = l = 1$ si deriva la successione particolare

1, 1, 2, 3, 5, 8 . .

nella quale è $v_4 = 3$ un numero *primo*. Similmente per $h = 1$, $l = 3$ si l'altra 1, 1, 4, 7, 19 . . . nella quale è primo $v_4 = 7$.

successione è crescente. Il termine v_4 poi ammette il divisore $v_2 = h$ quindi se $h > 1$ è composto anch'esso.

Corollario II. — *Un termine* v_r *ha tanti divisori nella successione quanti ne ha il suo indice* r *nella serie dei numeri naturali.*

Corollario III. — *Un termine con indice primo ammette per divisori nella successione solamente sè stesso e l'unità.*

Corollario IV. — *Alquanti termini* $v_\alpha, v_\beta, v_\gamma \ldots$ *hanno tanti divisori comuni nella successione, quanto ne hanno di comuni i loro indici nelle serie dei numeri naturali.*

Corollario V. — *Se* m *è il minimo multiplo comune a più numeri* r, s, t, ..., *sarà* v_m *il minimo multiplo comune, nella successione, dei termini* $v_r, v_s, v_t \ldots$ *ecc.*

12. Restando sempre nell' ipotesi di h, l *primi tra loro (come in tutto ciò che segue)* passiamo a determinare il massimo comun divisore ordinario di più termini della successione v. Si hanno le seguenti proprietà:

a) *Se* α *è divisibile per* β *il massimo comun divisore di* v_α, v_β *è* v_β.

Infatti, pel teorema del paragrafo precedente, è v_α divisibile per v_β.

b) *Se* r *è il resto della divisione di* α *per* β *il massimo comun divisore di* v_α, v_β *è uguale a quello di* v_β, v_r.

Infatti posto $\alpha = \beta q + r$, $(r < \beta)$, si faccia nella (1) $n = \beta q$, $r = s$; risulta

$$v_\alpha = v_{\beta q} v_{r+1} + l v_r v_{\beta q - 1}.$$

Ora ogni divisore d comune a v_α, v_β, essendo divisore di $v_{\beta q}$, sarà pure divisore del prodotto $l v_r v_{\beta q-1}$. Ma per quanto precede (§ 11) d è primo con l e con $v_{\beta q - 1}$, quindi dovrà dividere v_r. Reciprocamente, discende ancora dall'ultima eguaglianza che ogni divisore comune a v_β, v_r, essendo divisore di $v_{\beta q}$, è divisore di v_α. Le due coppie $(v_\alpha\ v_\beta)$ $(v_\beta\ v_r)$ hanno dunque i medesimi divisori comuni e quindi il medesimo massimo comune divisore. (*)

c) *Se* m *è il massimo comune divisore dei due indici* α, β, *sarà* v_m *il massimo comun divisore dei due termini* v_α, v_β.

Infatti se insieme ai numeri

$$\alpha, \beta, r, s, \ldots u, m,$$

dove $r, s, \ldots u, m$ sono i successivi resti ottenuti nella ordinaria ricerca del massimo comun divisore di α, β, consideriamo i termini

$$v_\alpha, v_\beta, v_r, v_s, \ldots, v_u v_m$$

(*) In modo analogo si dimostra: *Se* m *è un divisore comune a più termini* $v_\alpha, v_\beta, v_\gamma \ldots$ *sarà* m *un divisore di* $v_{p\alpha \pm q\beta \pm s\gamma \ldots}$

si riconosce, a causa del precedente teorema, che le coppie (v_α, v_β) (v_β, v_γ) $(v_\gamma, v_\delta) \ldots (v_u, v_m)$ hanno il medesimo massimo comun divisore; ma è u multiplo di m quindi esso sarà v_m, come si voleva provare.

Si deduce immediatamente:

d) *Se* m *è il massimo comun divisore di alquanti indici* $\alpha, \beta, \gamma, \ldots$, *sarà* v_m *il massimo comun divisore dei termini* $v_\alpha, v_\beta, v_\gamma, \ldots$

Questi teoremi riducono la ricerca del massimo comun divisore dei termini della successione a quella del massimo comun divisore dei loro indici.

13. Da quanto è stabilito nel paragrafo precedente *c)*, deriva che due termini v_α, v_β saranno primi tra loro sempre e soltanto quando è $v_m = 1$, essendo m il massimo comun divisore degli indici α, β. Ma essendo per definizione,

$$v_1 = 1,\ v_2 = h,\ v_3 = h^2 + 1, \ldots$$

si riconosce subito che se $h > 1$, è soltanto $v_1 = 1$ e quindi necessariamente $m = 1$, ossia *i due indici* α, β *sono anch'essi primi tra loro*: se è invece $h=1$ si ha $v_1=1, v_2=1$ e perciò necessariamente $m=1$, oppure $m=2$; ossia *i due indici* α, β *sono primi tra loro od hanno per massimo comun divisore* 2. Possiamo dunque enunciare i seguenti teoremi:

a) *Se* $h > 1$, *la condizione necessaria e sufficiente affinchè due termini* v_α, v_β *siano primi tra loro è che i loro indici* α, β *siano primi tra loro.*

b) *Se* $h = 1$, *la condizione necessaria e sufficiente affinchè due termini* v_α, v_β *siano primi tra loro è che i loro indici* α, β *abbiano un massimo comun divisore non maggiore di* 2.

14. Denotando con $\overline{\varphi(v_\alpha)}$ il numero dei termini della successione v non maggiori di v_α e primi con esso, e con $\varphi(\alpha)$ la funzione di Gauss rappresentante il numero dei numeri non maggiori di α e primi con esso, si dedurrà dai teoremi dimostrati ora:

1°. Se $h > 1$,

$$\overline{\varphi(v_\alpha)} = \varphi(\alpha) \tag{11}$$

2°. Se $h = 1$,

$$\overline{\varphi(v_\alpha)} = \varphi(\alpha) + \varphi\left(\frac{\alpha}{2}\right) \tag{12}$$

con $\varphi\left(\frac{\alpha}{2}\right) = 0$ quando α è dispari.

La funzione $\overline{\varphi}$ gode della seguente proprietà:

Se α, β *sono primi tra loro si ha*

$$\overline{\varphi(v_\alpha)}\ \overline{\varphi(v_\beta)} = \overline{\varphi(v_{\alpha\beta})} \tag{A}$$

Per la dimostrazione premettiamo che nella fatta ipotesi si ha, come è noto,

(B) $$\varphi(\alpha)\,\varphi(\beta) = \varphi(\alpha\beta).$$

Supposto dapprima $h > 1$, questa relazione si trasforma subito nella (A) perchè è allora, per qualunque valore di n, $\overline{\varphi(v_n)} = \varphi(n)$.

Se invece $h = 1$ si ha $\overline{\varphi(v_n)} = \varphi(n)$ *solamente* per valori *dispari di* n, e quindi se α, β sono *entrambi dispari* si ricaverà ancora la (A) dalla (B) come nel caso precedente. Se al contrario dei due numeri α, β (primi tra loro per ipotesi) *uno* è pari, ad esempio α. dalle relazioni

$$\overline{\varphi(v_\alpha)} = \varphi(\alpha) + \left(\frac{\alpha}{2}\right)$$
$$\overline{\varphi(v_\beta)} = \varphi(\beta)$$

si dedurrà

$$\overline{\varphi(v_\alpha)}\;\overline{\varphi(v_\beta)} = \varphi(\alpha)\,\varphi(\beta) + \varphi\left(\frac{\alpha}{2}\right)\varphi(\beta).$$

E poichè anche $\frac{\alpha}{2}$, β sono primi tra loro, si avrà ad un tempo

$$\varphi(\alpha)\,\varphi(\beta) = \varphi(\alpha\beta), \quad \varphi\left(\frac{\alpha}{2}\right)\varphi(\beta) = \varphi\left(\frac{\alpha\beta}{2}\right)$$

e quindi

$$\overline{\varphi(v_\alpha)}\;\overline{\varphi(v_\beta)} = \varphi(\alpha\beta) + \varphi\left(\frac{\alpha\beta}{2}\right)$$

ovvero a causa delle (12)

$$\overline{\varphi(v_\alpha)}\;\overline{\varphi(v_\beta)} = \overline{\varphi(v_{\alpha\beta})}.$$

La proprietà enunciata è così dimostrata per tutti i casi.

15. Più generalmente denotando con $v_\delta > 1$ un divisore di v_α appartenente alla successione, e con N il numero dei termini della successione stessa *minori di* v_α *ed aventi con esso per massimo comun divisore* v_δ, possiamo esprimere N per mezzo di $\overline{\varphi}$. Infatti se v_α, v_x hanno per massimo comun divisore v_δ, gli indici α, x, hanno per massimo comun divisore δ e reciprocamente (§ 12, c). Si conclude che il numero N è uguale a quello dei numeri *inferiori ad* α *ed aventi con esso per massimo comun divisore* δ, e quindi in ogni caso

$$N = \varphi\left(\frac{\alpha}{\delta}\right)$$

Ora se $h > 1$, si avrà anche, a causa della (11),

$$N = \overline{\varphi\left(v_{\frac{\alpha}{\delta}}\right)}$$

Se invece $h=1$ dalla (12) si deduce

$$\overline{\varphi\left(v_{\frac{\alpha}{\delta}}\right)}=\varphi\left(\frac{\alpha}{\delta}\right)+\varphi\left(\frac{\alpha}{2\delta}\right).$$

ossia

$$\mathrm{N}=\overline{\varphi\left(v_{\frac{\alpha}{\delta}}\right)}-\varphi\left(\frac{\alpha}{2\delta}\right).$$

Se $\frac{\alpha}{2\delta}$ è fratto il secondo membro si riduce al primo termine, ma se è intero si ricaverà dalla (12) col mutarvi α in $\frac{\alpha}{2\delta}$.

$$\overline{\varphi\left(v_{\frac{\alpha}{\delta}}\right)}=\varphi\left(\frac{\alpha}{2\delta}\right)+\varphi\left(\frac{\alpha}{4\delta}\right).$$

Sostituendo nella precedente il valore di $\varphi\left(\frac{\alpha}{2\delta}\right)$ di qui ricavato si ha:

$$\mathrm{N}=\overline{\varphi\left(v_{\frac{\alpha}{\delta}}\right)}-\overline{\varphi\left(v_{\frac{\alpha}{2\delta}}\right)}+\varphi\left(\frac{\alpha}{4\delta}\right).$$

Se $\frac{\alpha}{4\delta}$ è fratto il secondo membro si riduce ai due primi termini, nel caso contrario si muterà nella (12) α in $\frac{\alpha}{4\delta}$, e procedendo poi in modo analogo si avrà in generale

$$\mathrm{N}=\overline{\varphi\left(v_{\frac{\alpha}{\delta}}\right)}-\overline{\varphi\left(v_{\frac{\alpha}{\delta}}\right)}+\overline{\varphi\left(v_{\frac{\alpha}{\delta}}\right)}-\ldots\ldots+(-1)^{n}\,\overline{\varphi\left(v_{\frac{\alpha}{2^{n}.\delta}}\right)}$$

essendo 2^n la massima potenza di 2 che divide $\frac{\alpha}{\delta}$.

16. Un termine v_p avente per indice un numero primo può essere *primo* o *composto*, (*) ma per quanto precede (§ 11) non ammette *nella successione* divisori diversi da sè stesso e dall'unità. Tra i termini di indice composto il *solo* v_4 gode questa proprietà e nel *solo* caso di $h=1$, giacchè allora i divisori del v_4 appartenenti alla successione sono v_4 e $v_1=v_2=h=1$. Chiameremo perciò *primi nella successione* i termini con indice primo in ogni caso, ed anche v_4 quando $h=1$. Ciò premesso si hanno i seguenti teoremi:

TEOREMA I. — *Ogni termine* v_α *ammette un divisore primo nella successione.*

Infatti se α è primo il teorema è dimostrato; se α è composto e non è una potenza di 2, detto p un suo fattore primo dispari, sarà

(*) Per $h=l=1$ si ha, ad esempio, la successione $u\equiv 1, 1, 2, 3, 5, 7, 13, 21, 34, 55, 89, 144, 233, 377, 610, 987, 157, 2184, 4181, \ldots$ nella quale sono primi i termini di indice primo minore di 19, ed è composto $u_{19}=4181=37.113$.

Per $h=2$, $l=1$ si ha la successione $1, 2, 5, 12, 29, 70, 169, \ldots$ nella quale è composto $u'_7=169$.

$v_p \geqq v_3 > 1$ uno dei divisori cercati. Finalmente se a è una potenza di 2 posto $a = 2^k$ i divisori di v_a appartenenti alla successioni sono

$$v_1 = 1,\ v_2 = h,\ v_4,\ v_8, \ldots v_a$$

e quindi se $h > 1$ sarà v_2 il divisore cercato; se invece $h = 1$ sarà v_4.

Teorema II. — *Se un termine* v_γ *primo nella successione divide un prodotto di più fattori* $v_\lambda, v_\mu, v_\nu \ldots$ *divide uno di essi.*

Cominciamo da supporre γ primo. Se v_γ non dividesse alcuno dei fattori $v_\lambda, v_\mu, v_\nu \ldots$ neanche l'indice γ dividerà (§ 11) alcuno degli indici $\lambda, \mu, \nu \ldots$. e perciò essendo primo, sarà primo con ciascuno di essi. Ne consegue (§ 13) che v_γ è primo con ciascuno dei fattori $v_\lambda, v_\mu, v_\nu, \ldots$ e quindi col loro prodotto ciò che è contro l'ipotesi.

Se poi $\gamma = 4$ e v_4 non dividesse alcuno dei termini $v_\lambda, v_\mu, v_\nu, \ldots$ neanche 4 dividerà alcuni degli indici $\lambda, \mu, \nu, \ldots$ ed avrà con ciascuno di essi un massimo comun divisore non maggiore di 2, onde v_4 sarà primo con $v_\lambda, v_\mu, v_\nu, \ldots$ e si concluderà come nel caso precedente.

Di qui si deducono facilmente i seguenti:

3°. *Se un termine* v_γ *primo nella successione divide una potenza* $(v_\lambda)^m$, *divide anche la base.*

4°. *Se un termine* v_γ *primo nella successione divide un prodotto di più altri* $v_\lambda, v_\mu, \ldots$ *primi nella successione, è uguale ad uno di essi.*

Di quest'ultimo è poi facile conseguenza l'altro:

5°. *Se un numero* N *è decomponibile nel prodotto di più fattori* $v_\nu, v_\mu, v_\lambda, \ldots$ *primi nella successione è decomponibile in un modo soltanto.*

Osservazione. — Segue di qui che un numero N non può essere rappresentabile che in un modo soltanto sotto la forma

$$N = v_\lambda^p v_\mu^q v_\nu^r \ldots$$

quando $\lambda, \mu, \nu, \ldots$ sono *numeri primi differenti, od uno di essi al più è eguale a* 4.

6°. *Se due numeri* m, n(m > n) *sono prodotti di fattori* v_x *primi nella successione* v, *la condizione necessaria e sufficiente affinchè* m *sia divisibile per* n *è che il dividendo contenga ogni fattore primo, nella successione, del divisore con esponente almeno uguale.*

La condiz. è necessaria: supponiamo infatti $m = nz$ con $m = v_\lambda^p v_\mu^q v_\nu^r \ldots$, $n = v_\alpha^r . v_\beta^s . v_\gamma^t \ldots$ dove $v_\lambda, v_\mu, \ldots$ sono primi nella successione e differenti tra loro, e così anche $v_\alpha, v_\beta, v_\gamma \ldots$ sono primi nella successione e differenti tra loro. Essendo v_α divisore di n sarà pure, a causa dell'ipotesi divisore di m, e quindi per la precedente proprietà (4) sarà ad esempio $v_\alpha = v_\lambda$; ne segue sostituendo

$$m = v_\alpha^p v_\mu^q v_\nu^r \ldots$$

È poichè per le ipotesi v_α^r divide m, ed inoltre è primo (§ 13) con ciascuno dei fattori v_μ^q, $v_\nu^r \ldots$, così si concluderà che v_α^r divide v_α^p e quindi p è almeno uguale ad r. Se ora si pone

$$m_1 = v_\alpha^{p-r} \cdot v_\mu^q \cdot v_\nu^r \ldots, \quad n_1 = v_\beta^s \, v_\gamma^t \ldots\ldots$$

si dedurrà $m_1 = n_1 z$, ed analogamente a quanto precede, che v_β è ad esempio uguale a v_μ (non a v_α perchè per ipotesi è α diverso da β) e conseguentemente $q \geq s$. Resta pertanto provato quanto abbiamo asserito. Che la condizione enunciata sia sufficiente è cosa ovvia.

17. Se chiamiamo *primi tra loro nella successione* v due termini v_α v_β che non hanno altro divisore comune *nella successione* che $v_1 = 1$, si può vedere facilmente che v_α, v_β *sono primi tra loro in senso ordinario.* Basta a tal fine provare che i loro indici α, β sono primi tra loro se $h > 1$, e che hanno un massimo comune divisore non maggiore di 2 se $h = 1$. (13. a, b). Detto infatti m il massimo comun divisore degli indici, se fosse $m > 1$ o $m > 2$ a seconda del caso, sarebbe $v_m > 1$. Ma v_m è divisore comune (anzi è il massimo) ai termini v_α, v_β; dunque v_α, v_β avrebbero un divisore comune $v_m > 1$ ciò che è contro l'ipotesi. Quindi necessariamente $m = 1$ o m non maggiore di 2, come si voleva dimostrare.

Del resto si può anche notare che due termini qualunque v_α, v_β ammettono a divisori comuni in v tutti e *soltanto* quei termini v_d nei quali d è divisore comune di α, β (§ 11). Conseguentemente se è $v_1 = 1$ il *solo* divisore comune a $v_\alpha v_\beta$ in v, è 1 il solo divisore comune ad α, β e quindi v_α, v_β (§ 13) sono primi tra loro. Se poi nella successione v è anche $v_2 = h = 1$ allora α, β potranno avere per massimo comun divisore 2 e si concluderà come nel caso precedente.

18. Del teorema del § 11 faremo ancora un'applicazione per dimostrare una proprietà della successione V. Rispetto ad un termine V_s di essa si considerino le due coppie simmetriche $(V_{s+\mu}, U_{s-\mu})$ $(V_{s+\nu}\, V_{s-\nu})$ si ha allora il seguente

Teorema. — *Il quoziente*

$$\frac{V_{s+\mu} - (-l)^\mu \, V_{s-\mu}}{V_{s+\nu} - (-l)^\nu \, V_{s-\nu}}$$

è intero sempre quando μ *e multiplo di* ν *e lo è soltanto allora, se i coefficienti* h, l *sono primi tra loro; esso è inoltre costante al variare di* s *ed indipendente dai termini iniziali* α, β *della successione* V.

Conviene, per la dimostrazione, premettere una relazione tra i termini della successione v. A tal fine consideriamo il gruppo simmetrico

$$v_{n-1}, \; v_{n+1}, \; v_s, \; v_{s+1}$$

Applicandovi la formola (3') del § 4, poichè è qui $d' = 1$, $d = s - n - 1$, si trova subito

$$(-l)^n v_{s-n} = v_s v_{n+1} - v_{s+1} v_n$$

Ma dalla (1) scambiando n con s si deduce

$$v_{n+s} = v_s v_{n+1} + l v_n v_{s-1}$$

quindi resulterà sottraendo

$$(13)\ (^*) \qquad v_{s+n} - (-l)^n v_{s-n} = v_n (l v_{s-1} + v_{s+1})$$

Ciò premesso se valendoci della (2), calcoliamo l'espressione $V_{s+n} - (-l)^n V_{s-n}$ in funzione delle v_x si ha subito

$$V_{s+n} - (-l)^n V_{s-n} = (\beta v_{s+n-1} + l\alpha v_{s+n-2}) - (-l)^n (\beta v_{s-n-1} + l\alpha v_{s-n-2})$$

che diviene

$$V_{s+n} - (-l)^n V_{s-n} = \beta [v_{s+n-1} - (-l)^n v_{s-n-1}] + \\ + l\alpha [v_{s+n-2} - (-l)^n v_{s-n-2}]$$

Le quantità entro le parentesi si trasformano per mezzo della (13) nella quale si muti una prima volta s in $s - 1$ ed un'altra volta s in $s - 2$; si troverà quindi sostituendo

$$V_{s+n} - (-l)^n V_{s-n} = \beta v_n (l v_{s-2} + v_s) + l\alpha v_n (l v_{s-3} + v_{s-1})$$

ed anche

$$V_{s+n} - (-l)^n V_{s-n} = v_n [l(\beta v_{s-2} + l v_{s-3}) + (\beta v_s + l\alpha v_{s-1})]$$

Ma per mezzo della (2) si riconosce che le due quantità entro le parentesi interne del secondo membro sono rispettivamente V_{s-1}, V_{s+1} e quindi sarà

$$V_{s+n} - (-l)^n V_{s-1} = v_n [l V_{s-1} + V_{s+1}].$$

Mutando n in μ una prima volta, poi in ν e dividendo membro a membro le relazioni ottenute si ha:

$$\frac{V_{s+\mu} - (-l)^\mu \ V_{s-\mu}}{V_{s+\nu} - (-l)^\nu \ V_{s-\nu}} = \frac{v_\mu}{v_\nu}.$$

Il secondo membro è indipendente da s, e dai valori iniziali α, β; inoltre è sempre intero quando μ è multiplo di ν, ed è tale in questo caso *solamente* se h, l sono primi tra loro (§ 11). Il teorema è pertanto dimostrato.

La Spezia, Ottobre 1900.

ALBERTO TAGIURI.

(*) Si deduce di qui che il rapporto $\frac{v_{s+n} - (-l)^n v_{s-n}}{v_n} = l v_{s-1} + v_{s+1}$ è intero e costante al variare di n.

PODARIE RISPETTO ALLA PARABOLA

Sia la parabola rappresentata dall'equazione

$$y^2 = 2px.$$

Una tangente avendo per equazione

$$y = mx + \frac{p}{2m}, \tag{1}$$

la perpendicolare ad essa condotta da un punto $P(\alpha, \beta)$ del piano ha per equazione

$$y - \beta = -\frac{1}{m}(x - \alpha). \tag{2}$$

L'eliminazione di m fra le (1) e (2) da l'equazione della cubica podaria

$$(x^2 + y^2 - \alpha x - \beta y)(x - \alpha) + \frac{p}{2}(y - \beta)^2 = 0 \tag{3}$$

ovvero

$$y^2\left(x - \alpha + \frac{p}{2}\right) - \beta y(x - \alpha + p) + x(x - \alpha)^2 + \frac{p\beta^2}{2} = 0. \tag{4}$$

Se si trasportano gli assi parallelamente a loro stessi in modo che l'origine venga nel punto P, si ha

$$x = X + \alpha \quad , \quad y = Y + \beta$$

e la (3) diviene

$$X(X^2 + Y^2) + \alpha X^2 + \beta XY + \frac{p}{2} Y^2 = 0. \tag{5}$$

Questa rappresenta una cubica circolare unicursale, avente un asintoto parallelo all'asse delle y e un punto doppio in P.

Le tangenti nel punto doppio non sono reali che nel caso in cui sia $\beta^2 - 2p\alpha > 0$, cioè se il punto P è situato fuori della parabola. La curva che è tangente in un punto alla parabola, ha la forma strofoidale, con un cappio a punto doppio.

Allorchè il punto P è situato sulla parabola o interno ad essa, la curva, che assume una forma cissoidale, ha un punto doppio isolato. Essa è tangente alla parabola in tre punti o in un sol punto, secondo che P è interno o esterno alla sviluppata della parabola. Qualunque sia la posizione del punto P, la cubica taglia il suo asintoto in un punto Q di cui calcoleremo le coordinate.

Per la (4) l'equazione dell'asintoto è il coefficiente di y^2 eguagliato a zero. Essa è dunque

$$x = \alpha - \frac{p}{2} \tag{6}$$

Questo valore posto nella (4) dà per l'ordinata y di Q

$$y = \beta + \frac{p(2\alpha - p)}{4\beta} \tag{7}$$

Queste formule danno luogo a interessanti applicazioni.

L'equazione generale della cubica circolare unicursale a punto doppio può sempre mettersi sotto la forma

$$X(X^2 + Y^2) + \lambda X^2 + \mu XY + \nu Y^2 = 0. \tag{8}$$

La (5) si può rendere identica alla (8) ponendo

$$\lambda = \alpha, \quad \mu = \beta, \quad \nu = \frac{p}{2},$$

e quindi, se il punto P percorre tutto il piano, la sua podaria dà luogo a tutte le varietà possibili di cubiche circolari unicursali a punto doppio.

Le varietà più interessanti hanno luogo, quando P è situato sulla tangente nel vertice o sulla direttrice.

1°. P *è situato sulla tangente nel vertice.*

Allora $\alpha = 0$, e l'equazioni (4) e (5) divengono

$$y^2\left(x + \frac{p}{2}\right) - \beta y(x + p) + x^2 + \frac{p\beta^2}{2} = 0 \tag{9}$$

$$X(X^2 + Y^2) + \beta XY + \frac{p}{2} Y^2 = 0 \tag{10}$$

La curva ha sempre una forma strofoidale ed ha per asintoto la direttrice.

Le coordinate del punto Q sono allora

$$x = -\frac{p}{2} \quad , \quad y = \beta - \frac{p^2}{4\beta}. \tag{11}$$

Se dunque il punto P ha per coordinate $\alpha = 0$, $\beta = \frac{p}{2}$, il punto Q è il piede della direttrice.

Se il punto P è il vertice ($\alpha = 0, \beta = 0$), l'equazione (9) diviene

$$x(x^2 + y^2) + \frac{py^2}{2} = 0.$$

È la sola cubica di questa serie che abbia forma cissoidale. È d'altronde, come è noto, una cissoide retta.

2°. P *è sulla direttrice.*

In questo caso $\alpha = -\frac{p}{2}$, e l'equazioni (4) e (5) divengono

$$y^2(x+p) - \beta y\left(x+\frac{3p}{2}\right) + x\left(x+\frac{p}{2}\right)^2 + \frac{p\beta^2}{2} = 0, \tag{12}$$

$$X(X^2+Y^2) - \frac{p}{2}(X^2-Y^2) + \beta XY = 0. \tag{13}$$

Le tangenti nel punto doppio P sono perpendicolari. La cubica è dunque una strofoide obliqua, che ha per asintoto la retta $x = -p$.

Le coordinate del punto Q sono in questo caso

$$x = -p, \quad y = \beta - \frac{p^2}{2\beta}. \tag{14}$$

Se dunque P ha le coordinate $\alpha = -\frac{p}{2}$, $\beta = \frac{p}{\sqrt{2}}$, il punto Q ha le coordinate $x = -p, y = 0$.

Se il punto P è il piede della direttrice ($\alpha = -\frac{p}{2}$, $\beta = 0$), l'equazioni (12) e (13) diventano

$$y^2(x+p) + x\left(x+\frac{p}{2}\right)^2 = 0,$$

$$X(X^2+Y^2) - \frac{p}{2}(X^2-Y^2) = \theta,$$

rappresentano una strofoide retta di cui il vertice coincide con quello della parabola.

3°. P *è nel fuoco della parabola.*

Allora, essendo $\alpha = \frac{p}{2}$, $\beta = 0$, la (4) diviene

$$x\left[\left(x-\frac{p}{2}\right)^2 + y^2\right] = 0,$$

cioè il luogo si compone della tangente nel vertice e del fuoco (come punto isolato).

Abbiamo esposti questi risultati per l'unità di questa nota.

Ecco ora altre proprietà che crediamo inedite.

I. — *La retta* P,Q *è fissa per uno stesso punto* P *e per tutte le parabole aventi lo stesso asse e lo stesso vertice.*

Infatti l'equazione di questa retta è

$$\begin{vmatrix} x & y & 1 \\ \alpha & \beta & 1 \\ \alpha - \frac{p}{2} & \beta + \frac{p(2\alpha-\beta)}{4\beta} & 1 \end{vmatrix} =$$

ovvero

$$(15) \qquad (2\alpha-\beta)x+2\beta y=2\alpha^2+2\beta^2-\alpha\beta,$$

che è indipendente dal parametro p della parabola.

Ne risulta che:

1°. *Se il punto* P *percorre una retta fissa, cioè se fra* α *e* β *esiste una relazione*

$$\beta=m\alpha+q,$$

l'inviluppo della retta PQ *è una parabola.*

2°. *Se il punto* P *si sposta sulla parabola data (il che dà luogo alla relazione* $\beta^2=2p\alpha$*), l'inviluppo di* PQ *è una cubica.*

II. — *Per tutti i punti* P *situati sopra la retta fissa* $y=\beta$, *il punto* Q *è situato sopra una retta, e quando* β *varia, questa retta rimane tangente alla parabola data.*

Infatti l'eliminazione di α fra le equazioni (6) e (7) dà

$$(16) \qquad y=\beta+\frac{px}{2\beta}\cdot$$

III. — *Per un punto* P *fisso e per tutte le parabole aventi lo stesso asse e lo stesso vertice, il luogo del punto* Q *è una parabola.*

Infatti l'eliminazione di p fra le (6) e (7) dà

$$(17) \qquad x^2-\alpha x+\beta y-\beta^2=0.$$

IV. — *Se il punto* P *percorre una retta fissa, il luogo di* Q *è una conica.*

V. — *Se il punto* P *percorre la parabola data, il luogo del punto* Q *è la cubica*

$$(18) \qquad 8y^2(2x+p)=p(5x+2p)^2.$$

VI. — *Se le parabole hanno lo stesso asse e lo stesso vertice, e se il punto* P *è situato sulla direttrice ed ha una distanza costante* β *dall'asse, il luogo del punto* Q *è la parabola.*

$$(19) \qquad x^2+2\beta y-2\beta^2=0.$$

La retta PR inviluppa la parabola

$$(20) \qquad x^2-\beta x+4\beta y-\frac{15\beta^2}{4}=0.$$

VII. — *L'antipodaria di una strofoide obliqua rapporto al suo punto doppio è una parabola la cui direttrice passa per il punto doppio.*

E in generale.

L'antipodaria d'una cubica unicursale a punto doppio rapporto al suo punto doppio è una parabola la cui direttrice è parallela all'asintoto della cubica.

Ricerca dell'area compresa fra la podaria di P e il suo asintoto, quando P è sull'asse della parabola.

L'equazione (5) che rappresenta la podaria riferita agli assi PX e PY diviene, ponendovi $\beta=0$,

$$X(X^2+Y^2)+\alpha X^2+\frac{p}{2}Y^2=0,$$

ossia

(21) $$Y=X\sqrt{\frac{-\alpha-X}{X+\frac{p}{2}}}.$$

L'area compresa fra la curva ed il suo asintoto è

$$U=2\int_{-\alpha}^{-\frac{p}{2}}X\sqrt{\frac{-\alpha-X}{X+\frac{p}{2}}}\,dX.$$

Poniamo

$$\frac{-\alpha-X}{X+\frac{p}{2}}=\tan^2\varphi.$$

Ne risulta

$$X=-\left(\alpha\cos^2\varphi+\frac{p}{2}\operatorname{sen}^2\varphi\right),$$
$$dX=(2\alpha-p)\operatorname{sen}\varphi\,.\cos\varphi\,d\varphi$$

e quindi

$$U=\int_0^{\frac{\varphi}{2}}(p-2\alpha)\operatorname{sen}^2\varphi\left(\alpha\cos^2\varphi+\frac{p}{2}\operatorname{sen}^2\varphi\right)d\varphi$$

e

$$U=2(p-2\alpha)\left\{\alpha\int^{\frac{\varphi}{2}}\operatorname{sen}^2\varphi\cos\varphi\,d\varphi+\frac{p}{2}\int_0^{\frac{\varphi}{2}}\operatorname{sen}^4\varphi\,d\varphi\right\}.$$

Ma si sa che

$$\int_0^{\frac{\varphi}{2}}\operatorname{sen}^2\varphi\,.\cos\varphi\,d\varphi=\frac{\pi}{16}\quad,\quad\int_0^{\frac{\varphi}{2}}\operatorname{sen}^4\varphi\,d\varphi=\frac{3\pi}{16}.$$

Dunque

(22) $$U=\frac{p(p-2\alpha)(2\alpha+3p)}{16}.$$

Ecco per alcuni casi particolari interessanti l'equazione della podaria e l'area di essa.

1°. Se $\alpha=\frac{p}{2}$, $\quad(X^2+Y^2)\left(X+\frac{p}{2}\right)=0,\qquad U=0.$

Il punto P è il fuoco, la cubica è la tangente nel vertice col fuoco come punto doppio isolato.

2°. Se $\alpha = 0$, $$Y^2 = \frac{-X^3}{X + \frac{p}{2}}, \qquad U = \frac{3\pi p^2}{16}.$$

Il punto P è il vertice della parabola, e la cubica è una *cissoide retta.*

3°. Se $\alpha = -\frac{p}{2}$, $$Y = X\sqrt{\frac{\frac{p}{2} - X}{\frac{p}{2} + X}}, \qquad U = \frac{\pi p^2}{4}.$$

Il punto P è il piede della direttrice, e la cubica è una *strofoide retta.*

4°. Se $\alpha = -\frac{3p}{2}$, $$Y = X\sqrt{\frac{3p - 2X}{2X + p}}, \qquad U = 0.$$

L'area $U = 0$ indica che per questa curva, che è una *trisettrice di Mac-Laurin* e che deriva dal *folium di Descartes,* di cui l'equazione è

$$Y = \frac{X}{\sqrt{3}}\sqrt{\frac{3p - 2X}{2X + p}},$$

l'area del cappio è equivalente a quella compresa fra il resto della curva ed il suo asintoto.

Queste due aree essendo algebricamente di segno contrario, ne risulta $U = 0$.

Questa interessante proprietà delle aree è comune alla *trisettrice di Mac-Laurin* e al *folium di Descartes.* L'area del cappio della trisettrice è $\frac{3p^2\sqrt{3}}{4}$.

Su questo proposito mi permetto di esporre ai nostri amabili corrispondenti il seguente *desideratum.*

Nel caso in cui il punto P è qualunque, la podaria della parabola rapporto a P deve avere l'area compresa fra la curva ed il suo asintoto finita. Sarebbe interessante poterne calcolare il valore ed auguro che un corrispondente sia più fortunato di me in questa ricerca.

E.-N. BARISIEN.

SULLA DETERMINAZIONE DI ALCUNI COEFFICENTI NUMERICI
di uno sviluppo nella teoria delle forme

1. Se con f indichiamo una funzione di due variabili $x(x_1, x_2)$, $y(y_1 y_2)$, omogenea e di grado m nelle x_1, x_2, omogenea e di grado n nelle y_1, y_2, se a Δ, D, Ω diamo i soliti significati relativi alle ben note operazioni del calcolo simbolico avremo l'uguaglianza:

$$a) \qquad f = \Delta^n D^n f + \alpha_1^{(n)}(xy)\Delta^{n-1} D^{n-1}\Omega f + \alpha_2^{(n)}(xy)^2\Delta^{n-2} D^{n-2}\Omega^2 f + \\ + \dots\dots + \alpha_n^{(n)}\Omega^n f,$$

in cui le $D^n f$, $D^{n-1}\Omega f$, $D^{n-2}\Omega^2 f$; .... sono funzioni delle sole x, (x_1, x_2).

I termini del secondo membro della $a)$ sono affetti da coefficenti numerici, dipendenti dai gradi m, n e dall'ordine corrispondente al posto che occupano.

Essi sono legati dalle note formole di ricorrenza:

$$1)\quad \alpha_1^{(n)} = \alpha_1^{(n-1)} + \frac{m^2}{(m+n-1)(m+n)}$$

$$2)\quad \alpha_2^{(n)} = \alpha_2^{(n-1)} + \frac{(m-1)^2}{(m+n-3)(m+n-2)}\alpha_2^{(n-1)}$$

$$3)\quad \alpha_3^{(n)} = \alpha_3^{(n-1)} + \frac{(m-2)^2}{(m+n-5)(m+n-4)}\alpha_2^{(n-1)}$$

. . . .

$$\lambda)\quad \alpha_\lambda^{(n)} = \alpha_\lambda^{(n-1)} + \frac{(m-\lambda+1)^2}{(m+n-2\lambda+1)(m+n-2\lambda+2)}\alpha_{\lambda-1}^{(n-1)} \; .$$

La determinazione di questi coefficenti è fatta dal Clebsch con artifici che si riferiscono alla teoria delle forme. Mi propongo di pervenire all'espressione di uno qualunque di questi coefficenti col solo sussidio delle cognizioni algebriche.

2. Osserviamo anzitutto che λ non può superare n, che cioè per $\lambda > n$ tutte le α corrispondenti sono nulle.

Poniamo nella 1) $n = 1$

$$\alpha'_1 = \alpha_1^0 + \frac{m^2}{m \,.\, m+1}$$

ossia:

$$\alpha' = \frac{m}{m+1}$$

E successivamente per $m = 2, = 3, = 4, = n$ avremo:

$$b) \begin{cases} \alpha_1^2 = \alpha'_1 + \dfrac{m^2}{m+1 \,.\, m+2} \\ \alpha_1^3 = \alpha_1^2 + \dfrac{m^2}{m+2 \,.\, m+3} \\ \dots\dots\dots\dots \\ \alpha_1^n = \alpha_1^{n-1} + \dfrac{m^2}{m+n-1 \,.\, m+n} \end{cases}$$

Sommando le *b)* e riducendo:

$$c) \qquad \alpha_1^{(n)} = \sum_{n=1}^{n} \frac{m^2}{m+n-1 \,.\, m+n} = m^2 \sum_{n=1}^{n} \frac{1}{m+n-1 \,.\, m+n},$$

e poichè

$$\sum_{n=1}^{n} \frac{1}{m+n-1 \,.\, m+n} = \sum_{n=1}^{n} \frac{1}{m+n-1} - \sum_{n=1}^{n} \frac{1}{m+n},$$

si ha

$$\sum_{n=1}^{n} \frac{1}{m+n-1 \,.\, m+n} = \sum_{n=0}^{n-1} \frac{1}{m+n} - \sum_{n=1}^{n} \frac{1}{m+n} = \frac{1}{m} - \frac{1}{m+n} = \frac{n}{m \,.\, m+n}$$

e per sostituzione nella *c)*

$$c') \qquad \alpha_1^{(n)} = \frac{m \,.\, n}{m+n} = \frac{\binom{m}{1}\binom{n}{1}}{\binom{m+n}{1}},$$

formola simmetrica in m, n. —

Dalla *c')* si ha

$$\alpha_1^{(n-1)} = \frac{m \,.\, n-1}{m+n-1},$$

che per sostituzione nella 2) dà

$$\alpha_2^{(n)} = \alpha_2^{(n-1)} + \frac{(m-1)^2 m \,.\, (n-1)}{(m+n-3)(m+n-2)(m+n-1)},$$

nella quale fatto $n = 2, 3, \ldots n$ si hanno le formole di ricorrenza

$$\alpha_2^{(2)} = \alpha_2^{(1)} + \frac{m \,.\, (m-1)}{m-1 \,.\, m \,.\, m+1}$$

$$\alpha_2^{(3)} = n_2^{(2)} + \frac{m \,.\, m+1 \,.\, +2}{2 \,.\, (m-1)^2 m \,.}$$

. . . .

$$\alpha_2^{(n)} = \alpha_2^{(n-1)} + \frac{(n-1)(m-1)^2 m}{(m+n-3)(m+n-2) \,.\, (m+n-1)},$$

da cui, per via di somma,

$$d) \qquad \alpha_2^{(n)} = m(m-1)^2 \sum_{n=2}^{n} \frac{n-1}{(m+n-3) \,.\, (m+n-2)(m+n-1)};$$

posto

$$m+n-3 = \xi_3^{(n)} \quad m+n-2 = \xi_2^{(n)} \quad m+n-1 = \xi_1^{(n)},$$

si avrà

$$\sum_{n=2}^{n} \frac{n-1}{\xi_1^{(n)} \xi_2^{(n)} \xi_3^{(n)}} = \sum_{n=2}^{n} \frac{\xi_1^{(n)} - m}{\xi_1^{(n)} \xi_2^{(n)} \xi_3^{(n)}} = \sum_{n=2}^{n} \frac{1}{\xi_2^{(n)} \xi_3^{(n)}} - m \sum_{n=2}^{n} \frac{1}{\xi_1^{(n)} \xi_2^{(n)} \xi_3^{(n)}};$$

ora

$$\sum_{n=2}^{n} \frac{1}{\xi_1^{(n)} \xi_2^{(n)} \xi_3^{(n)}} = \frac{1}{2} \sum_{n=2}^{n} \frac{1}{\xi_2^{(n)} \xi_3^{(n)}} - \frac{1}{2} \sum_{n=2}^{n} \frac{1}{\xi_2^{(n)} \xi_1^{(n)}} =$$

$$= \frac{1}{2}\left(\frac{1}{m \,.\, m-1} - \frac{1}{m+n-2 \,.\, m+n-1}\right)$$

e

$$\sum_{n=2}^{n} \frac{1}{\xi_2^{(n)}\,\xi_3^{(n)}} = \frac{1}{m-1} - \frac{1}{m+n-2};$$

quindi

$$\sum_{n=2}^{n} \frac{n-1}{(m+n-3)(m+n-2)(m+n-1)} = \frac{1}{m-1} - \frac{1}{2(m-1)} - \frac{1}{m+n-2} +$$
$$+ \frac{m}{2(m+n-1)(m+n-2)} = \frac{n \,.\, n-1}{2(m-1)(m+n-2)(m+n-1)};$$

e per sostituzione nella *d)*

d') $$\alpha_2^{(n)} = \frac{m \,.\, m-1 \,.\, n \,.\, n-1}{2 \,.\, (m+n-1)(m+n-2)} = \frac{\binom{m}{2}\binom{n}{2}}{\binom{m+n-1}{2}}.$$

Dalle formole *c)* e *d')* si scorge la legge di successione dei valori di $\alpha_\lambda^{(n)}$. Mostriamo che se essa è verificata per $n = \lambda - 1$, sarà verificata anche per $n = \lambda$.

Supposto cioè che sia

$$\alpha_{\lambda-1}^{(n)} = \frac{\binom{m}{\lambda-1}\binom{n}{\lambda-1}}{\binom{m+n-\lambda+2}{\lambda-1}},$$

proviamo che

$$\alpha_\lambda^{(n)} = \frac{\binom{m}{\lambda}\binom{n}{\lambda}}{\binom{m+n-\lambda+1}{\lambda}}.$$

Ora avremo immediatamente che

$$\alpha_{\lambda-1}^{n-1} = \frac{\binom{m+n-\lambda+1}{\lambda-1}}{\binom{m}{\lambda-1}\binom{n-1}{\lambda-1}},$$

e per sostituzione nella λ), col solito metodo di somma, ricaviamo

e) $$\alpha_\lambda^{(n)} = (m-\lambda+1)^2 \binom{m}{\lambda-1} \sum_{n=\lambda}^{n} \frac{\binom{n-1}{\lambda-1}}{\binom{m+n-\lambda+1}{\lambda-1}(m+n-2\lambda+1)(m+n-2\lambda+2)},$$

che può porsi sotto la forma

$$\alpha_\lambda^{(n)} = (m-\lambda+1)\binom{m}{\lambda} \sum_{n=\lambda}^{n} \frac{\binom{n-1}{\lambda-1}}{\binom{m+n-\lambda+1}{\lambda}(m+n-2\lambda+1)}.$$

Non è agevole calcolare direttamente. Diamo dei valori particolari.

Poniamo $n = \lambda$; avremo

$$\alpha_\lambda^\lambda = (m-\lambda+1)\binom{m}{\lambda} \frac{\binom{\lambda-1}{\lambda-1}}{\binom{m+1}{\lambda}(m+\lambda-1)} = \binom{m}{\lambda} \frac{1}{\binom{m+1}{\lambda}}$$

per $n = \lambda + 1$

$$\alpha_\lambda^{\lambda+1} = (m - \lambda + 1)\binom{m}{\lambda}\left\{\frac{1}{\binom{m+1}{\lambda}(m-\lambda+1)} + \frac{\lambda}{\binom{m+2}{\lambda}(m-\lambda+2)}\right\},$$

e per essere

$$\binom{m+1}{\lambda} = \binom{m+2}{\lambda}\frac{m-\lambda+2}{m+2},$$

avremo

$$\alpha_\lambda^{\lambda+1} = (m-\lambda+1)\binom{m}{\lambda}\frac{1}{\binom{m+2}{\lambda}(m-\lambda+2)}\left\{\frac{m+2}{m-\lambda+1} + \lambda\right\}$$

$$= (m-\lambda+1)\binom{m}{\lambda}\frac{1}{\binom{m+2}{\lambda}(m-\lambda+2)}\,\frac{m+2+\lambda(m-\lambda+2)-\lambda}{m-\lambda+1}$$

$$= \frac{\lambda+1}{\binom{m+2}{\lambda}}\binom{m}{\lambda}.$$

Poniamo ora

$$n = \lambda + 2;$$

avremo

$$\alpha_\lambda^{\lambda+2} = (m-\lambda+1)\binom{m}{\lambda}\left\{\frac{\lambda+1}{\binom{m+2}{\lambda}(m-\lambda+1)} + \frac{\lambda\,.\,\lambda+1}{2\binom{m+3}{\lambda}(m-\lambda+3)}\right\},$$

da cui raccogliendo

$$\alpha_\lambda^{\lambda+2} = (m-\lambda+1)\binom{m}{\lambda}\frac{\lambda+1}{2\binom{m+3}{\lambda}(m-\lambda+1)}\,\frac{2(m+3)+\lambda\,.\,(m-\lambda+1)}{m-\lambda+3}$$

$$= \binom{m}{\lambda}\frac{\lambda+1}{2\binom{m+3}{\lambda}}\,\frac{(m-\lambda+3)(\lambda+2)}{m-\lambda+3} = \binom{m}{\lambda}\frac{\binom{\lambda+1}{2}}{\binom{m+3}{\lambda}}.$$

Ora dall' ispezione dei valori del sommatorio per $n = \lambda,\ \lambda+1,\ \lambda+2$, si scorge la legge di successione dei valori del sommatorio stesso. Supposto infatti che per n, si prende il valore $n - 1$, e si abbia per valore del sommatorio

$$\frac{\binom{n-1}{\lambda}}{(m-\lambda+1)\binom{m+n-\lambda}{\lambda}},$$

troverò per il valore n l'espressione

$$\frac{\binom{n}{\lambda}}{(m-\lambda-1)\binom{m+n-\lambda+1}{\lambda}}.$$

Infatti per n, il sommatorio sarebbe eguale alla somma delle espressioni

$$\frac{\binom{n-1}{\lambda}}{(m-\lambda+1)\binom{m+n-\lambda}{\lambda}} + \frac{\binom{n-1}{\lambda-1}}{\binom{m+n-\lambda+1}{\lambda}(m+n-2\lambda+1)};$$

e poichè

$$\binom{n-1}{\lambda} = \binom{n}{\lambda}\frac{n-\lambda}{n} \quad \text{e} \quad \binom{n-1}{\lambda-1} = \binom{n}{\lambda}\frac{\lambda}{n}$$

si avrà per sostituzione

$$\binom{m+n-\lambda}{\lambda} = \binom{m+n-\lambda+1}{\lambda}\frac{m+n-2\lambda+1}{m+n-\lambda+1},$$

$$\frac{\binom{n}{\lambda}\frac{n-\lambda}{n}}{\binom{m+n-\lambda+1}{\lambda}\frac{m+n-2\lambda+1}{m+n-\lambda+1}(m-\lambda+1)} + \frac{\binom{n}{\lambda}\frac{\lambda}{n}}{\binom{m+n-\lambda+1}{\lambda}(m+n-2\lambda+1)},$$

da cui raccogliendo ed eseguendo i calcoli, si ricava

$$\frac{\binom{n}{\lambda}}{\binom{m+n-\lambda+1}{\lambda}(m-\lambda+1)}.$$

Resta con ciò provato che il valore del sommatorio è, per il valore n, dato da

$$\frac{\binom{n}{\lambda}}{(m-\lambda+1)\binom{m+n-\lambda+1}{\lambda}},$$

e quindi per sostituzione nella *e)*

$$\alpha_\lambda^{(n)} = \frac{\binom{n}{\lambda}\binom{m}{\lambda}}{\binom{m+n-\lambda,+1}{\lambda}}$$

La legge che regola la successione dei valori della $\alpha_\lambda^{(n)}$ per qualunque valore di λ, ed n, è dunque verificata.

Dott. A. Bassi.

Sulla risoluzione dei problemi mediante la sola riga

Si consideri la riga, non come atta soltanto a *tracciare* una retta, ma come uno strumento che permetta inoltre, mediante punti di riferimento che vi si suppongono segnati, di portare una lunghezza data sopra una retta *già tracciata*. È da prevedere che *taluni* problemi, che si ritengono non risolubili senza l'aiuto del compasso, diventino invece risolubili mediante la sola riga così definita, poichè una tal riga ha, per così dire, qualche cosa del compasso. Cominciamo dai più semplici:

a) *Ad una retta data condurre una parallela.* Si congiunga un punto qualunque C, preso fuori della retta, a due punti A e B della retta stessa; si prenda CX = AC, CY = BC; evidentemente XY sarà parallela ad AB.

b) *Ad una retta data condurre la parallela per un punto dato.* Per questo punto C si conduca una retta qualunque, che incontra in D la data retta AB. Si tracci poi una parallela a CD: questa incontra in E la retta data; e se si prende $EX = DC$, è chiaro che CX sarà la parallela richiesta.

Dopo ciò si vede che si può, *senza compasso,* costruire una quarta proporzionale, o una terza proporzionale, ed in generale qualunque espressione della forma $x = \frac{abcd}{efg}$. Ed anche si può dividere un segmento rettilineo dato in un qualsiasi numero di parti uguali, o proporzionali a lunghezze date.

c) *Tracciare un angolo retto, che abbia il vertice in un punto dato.* Per questo punto A si conduca una retta qualunque; per un punto B di questa si tracci un'altra retta XY, e su questa si portino, nei due sensi, le lunghezze $BX = BY = AB$. In tal modo XAY risulterà un angolo retto.

d) *Ad una retta data condurre la perpendicolare per un punto dato.* Si costruiscano due angoli retti, aventi il vertice nel dato punto C; siano A e B, rispettivamente, i punti d'incontro di due lati del primo e del secondo angolo con la retta data, e si tracci per A la parallela all'altro lato del secondo angolo, e per B la parallela all'altro lato del primo angolo: sia X il punto d'incontro di tali parallele. È chiaro che CX è la perpendicolare richiesta, giacchè le altezze del triangolo ABC debbono concorrere in un punto. La costruzione diventa illusoria quando C è dato sulla retta; ma si può allora cominciare dal sostituire questa con una sua parallela.

Dalle cose fin qui dette segue che si può, *senza compasso,* costruire qualunque espressione irrazionale della forma $x = \sqrt{a^2 + b^2 + c^2 + \ldots}$, e per conseguenza $a\sqrt{3}$, o un triangolo equilatero, o un esagono regolare di lato a, ed anche gli angoli di $45°$, $60°$, $30°$, ed in generale ogni angolo definito della formula $\tan\theta = \sqrt{\frac{\alpha}{\beta}}$, con α e β razionali.

Ora, per riassumere, e per vedere fin dove si può fare a meno del compasso nel costruire le espressioni, che si sa di poter costruire mediante la riga ed il compasso, ricordiamo che tali costruzioni si possono ricondurre a quella di una delle seguenti espressioni:

a) $x = \frac{\varphi}{\psi}$, con φ e ψ polinomi razionali omogenei, dei gradi rispettivi $n+1$ ed n. Dividendo numeratore e denominatore per a^{n-1}, dove a indica una lunghezza qualunque, si riducono al primo grado i termini di ψ, quindi tutto il denominatore ad un monomio; poi x alla somma di tante espressioni del primo grado, che si sanno costruire senza compasso, per quanto si è osservato in seguito alla risoluzione dei primi due problemi.

b) $x = \sqrt{a^2 + b^2 + \ldots}$, che si può costruire, come si è detto, senza compasso.

c) $x = \sqrt{ab}$, $x = \sqrt{a^2 - b^2}$, espressioni che si trasformano immediatamente l'una nell'altra, sicchè il problema di " *costruire la media geometrica di a e b* " equivale all'altro: *costruire un triangolo rettangolo, conoscendone un lato e l'ipotenusa.* Quando a e b ammettono una comune misura c, ponendo $a = c\alpha$, $b = c\beta$, si ha $x = c\sqrt{\alpha\beta}$ o $x = c\sqrt{\alpha^2 - \beta^2}$, e si ricade nel caso precedente.

Adunque il solo problema, in cui le considerazioni che precedono non valgono a dispensarci dall'uso del compasso, è la *ricerca della media geometrica fra due lunghezze, tra loro incommensurabili.*

Prof. G. Cesàro
DELL'UNIVERSITÀ DI LIEGI.

LUOGHI ED INVILUPPI (*)

(ESERCIZI DI GEOMETRIA ANALITICA)

29. Sia OA un raggio fisso di un circolo, OB ed OC due raggi mobili tali che sia $A\widehat{O}C = 2A\widehat{O}B$.

1° Il luogo delle intersezioni delle tangenti al circolo nei punti B e C è (oltre alla retta OA) una *trisettrice di Mac-Laurin*.

2° Se da B si conduce la parallela ad OA e da C la perpendicolare alla OA stessa, il luogo delle intersezioni di queste due rette è una *parabola*.

3° Se invece si conduce da B la perpendicolare e da C la parallela ad OA, il luogo delle intersezioni è una *quartica nodale*.

30. Se A e B sono due vertici fissi di un triangolo ABC ed è $\widehat{C} = 3\widehat{A}$, il luogo di C è una *quartica circolare* con un punto triplo in A. Le tangenti in A sono la perpendicolare alla AB e le rette inclinate su AB di $\pm\frac{\pi}{4}$. La curva ha due assintoti reali inclinati di $\pm\frac{\pi}{8}$ su AB e incrociantesi in A.

31. Il luogo dei centri dei cerchi iscritti nei triangoli determinati da un raggio fisso e da uno mobile di uno stesso circolo è una *strofoide retta*.

32. Si considerino tutte le coniche simili di cui è dato un fuoco F e la corrispondente direttrice passa per un punto dato D; il luogo dei centri di tali coniche è un *circolo*; l'inviluppo delle coniche stesse è pure un *circolo*.

33. Sieno C^2 e C'^2 due cerchi concentrici in O e supponiamo che C'^2 sia interno a C^2. Da un punto S di C'^2 si conduca una retta mobile che tagli C^2 in A e A' e C'^2 ulteriormente in T. Se R è l'altro estremo del diametro di C'^2 passante per S, le intersezioni della TR con le OA, OA' descrivono una *curva di Jerabek*.

34. Un cerchio di raggio r rotola sopra una retta data. Da un punto fisso A di questa retta si conduce la seconda tangente al cerchio; il luogo dei punti di contatto è una *cubica circolare*.

35. Sia OA un raggio fisso di un circolo O^2, M ed N due punti di questo circolo tali che sia $\widehat{AN} = 2\widehat{AM}$; il luogo del baricentro dei punti A, M, N ed O è una *Conchiglia di Pascal*.

36. Una retta mobile perpendicolare ad un diametro fisso AB di un cerchio di centro O taglia questa curva nei punti P, Q: il luogo delle intersezioni delle rette AP e QO; AQ e PO è (oltre alla retta AB contata due volte) una *iperbole*.

37. Sieno AB ed A'B' due rette parallele ed O un punto fisso della

(*) Continuazione v. Vol. preced. a pag. 59.

bisettrice della striscia da esse determinata. Si conduca per O una retta mobile che tagli in M ed N rispettivamente le AB ed A'B'; il luogo delle intersezioni della perpendicolare condotta da M ad MN e della bisettrice dell'angolo MNB' è una *cubica mista*.

38. Il luogo del vertice mobile di un triangolo di cui è data la base AB e si sa che è $\widehat{A} = 2\widehat{B}$, è una *quartica* con un punto isolato in A e che ha due assintoti inclinati di $\pm \frac{\pi}{3}$ sulla retta AB.

39. Sieno date due rette ortogonali OX ed OY ed un segmento a. L'inviluppo dei cerchi che hanno per centro un punto A di OX e passano per un punto B di OY, in modo che sia $OA + OB = a$, è una *ellisse*.

40. Sia AP una retta mobile intorno ad un punto fisso di un circolo O^2 di centro O che incontri ulteriormente il cerchio in P, PT la tangente in P che incontri in T il diametro passante per A; se TI è la perpendicolare condotta da T ad AP, il luogo di I è una *quartica* (inversa di *folium parabolicum*).

41. Sia NM una corda mobile di un cerchio, parallela ad un dato diametro AB; si unisca A con M e da N si conduca la perpendicolare ad AB; il luogo delle intersezioni di queste due rette è una *Cissoide di Diocle*.

42. L'inviluppo di tutte le coniche simili che hanno un fuoco sopra un cerchio dato e la corrispondente direttrice è una data retta, è una coppia di *coniche* della stessa specie di quelle date.

43. Sia O un punto fisso ed A uno mobile di un cerchio e sia OO' il diametro passante per O; il luogo delle bisettrici dell'angolo AOO' con la parallela condotta da A ad OO' è un *trifolium retto*.

44. Sia PQ una retta mobile perpendicolare all'asse maggiore AB di un'ellisse. Il luogo delle intersezioni della tangente in P all'ellisse con la retta QA è (oltre alla tangente in A all'ellisse) un'*iperbole*.

45. Il luogo dei vertici I di un triangolo variabile MNI tale che MN sia diametro di un cerchio dato C^2, MI sia tangente a questo cerchio ed NI passi costantemente per un punto A di C^2 è una *cissoide di Diocle*.

46. Se dal punto doppio di una cubica razionale circolare si conducono due rette ortogonali che taglino la curva ulteriormente nei punti P e Q, il luogo del punto medio del segmento PQ è una *retta*.

47. Sia OA un raggio fisso e OP uno mobile di un circolo O^2 e QQ' il diametro perpendicolare a questo raggio. Il luogo delle intersezioni delle rette QA e QA' con OP è una *strofoide retta*.

48. Sia A un punto fisso ed M uno mobile di un circolo O^2 di centro O; il luogo delle intersezioni della retta OM col cerchio A(AM) è una *Conchiglia di Pascal*; così pure il luogo delle intersezioni della tangente in M ad O^2 con lo stesso cerchio A(AM) è una *Conchiglia di Pascal*.

49. Sia C^2 un cerchio fisso e C'^2 un altro cerchio che rotoli su C^2; il luogo delle intersezioni di C'^2 con la parallela condotta del punto di contatto dei due cerchi ad una direzione fissa, è, in generale, un'*ellisse* (oltre al circolo C'^2).

50. Sia MN una retta mobile, perpendicolare all'asse maggiore di un'ellisse di centro O ed incontri in M, N la curva. Il luogo delle intersezioni della OM con la tangente in N e della ON con la tangente in M è una *kreuzcurva*.

Se si considera invece un circolo, si ha una *kreuzcurva equilatera*.

Se invece di considerare un'ellisse si considera un'iperbole, si ha per il luogo una *quartica* che ha un punto doppio nel centro dell'iperbole e le tangenti in questo punto coincidono con gli assintoti dell'iperbole.

Se l'iperbole è equilatera la suddetta quartica è una *lemniscata di Bernoulli*.

G. Cardoso-Laynes.

MOVIMENTO ED EGUAGLIANZA

1. L'articolo " Il postulato del movimento „ scritto da Anton Maria Bustelli nel *Bollettino di matematiche e scienze fisiche*, anno I, n. 13-14, contiene diversi concetti degni di essere meditati. Io, unicamente mosso dal desiderio di veder chiaro in una questione che ha occupato molti nostri valorosi insegnanti e cultori di scienze matematiche, come il Burali-Forti, il De Amicis, il Veronese, il Bustelli, ecc., scrivo le mie considerazioni.

2. Base di tutta la geometria elementare è il concetto di eguaglianza dimostrata col movimento. Questo principio tacitamente incluso in Euclide e in tutti gli elementi di geometria fino a Legendre, fu poi posto in evidenza da diversi autori che vennero dopo Legendre, e in questi ultimi tempi il De Amicis, il Bustelli ed altri ne spiegarono la grande importanza. Nella seduta quarta del congresso promosso dall'associazione Mathesis in Torino nel 1898, dissi, e lo stesso prof. De Amicis ammise, essere conveniente sostituire, nella formola del detto principio, la parola " *verificare* „ alla parola " *dimostrare* „. Ora partirò da questa formula " *Base di tutta la geometria elementare è il concetto di eguaglianza verificata col movimento* „ e cercherò di spiegarmi sul significato e sull'estensione de' suoi tre principali elementi, moto, verifica, eguaglianza.

Tutti abbiamo le nozioni intuitive di:

corpo fisico ossia tutto ciò che genera le nostre sensazioni le quali vanno sotto il nome di " proprietà dei corpi fisici „ p. e. colore, peso, porosità, impenetrabilità, ecc.

corpo geometrico ossia tutto ciò che si ottiene pensando al corpo fisico, e nello stesso tempo facendo astrazione dai nostri sensi ossia dalle proprietà dei corpi fisici e da altre possibili sensazioni non ancora riconosciute e classificate sotto la denominazione " proprietà fisiche dei corpi „.

forma ed estensione ossia elementi comuni a tutti gli individui della classe " corpo geometrico „

punto geometrico o semplicemente punto ossia ciò che si ottiene pensando al corpo geometrico e nello stesso tempo facendo astrazione dai detti elementi, forma ed estensione.

3. Il movimento dei corpi è concetto primitivo fornitoci dall'esperienza.

A tutte le cose, che cadono o che potrebbero cadere sotto i nostri sensi (che generano o che potrebbero generare le nostre sensazioni), si associa il concetto di movimento. Ma tale concetto non si può associare nè alle sensazioni o affezioni dell'uomo (p. e. dolore, ambizione, virtù, avarizia ecc.) nè alle cose che non cadono e non possono cadere sotto i nostri sensi (p. e. numeri, valore, proposizione, operazioni aritmetiche, ecc.) nè ai risultati dell'astrazione su certe classi di cose (p. e. il dolce, l'amaro, la durezza, la trasparenza, l'impenetrabilità, ecc.) risultati ottenuti pensando prima a classi di cose materiali che producono in noi certe sensazioni, e poi facendo astrazione da tutto ciò che non è comune a tutti gl'individui delle classi. Perciò nè alle cosidette proprietà dei corpi fisici, nè al corpo geometrico, si può associare il concetto di movimento.

Quando si dice che un punto si move e genera una linea, si deve intendere che un punto fisico si move e genera la rappresentazione di una linea. Quando si dice che una linea si move e genera una superficie, si deve intendere che, un corpo fisico, il quale si ritiene come la rappresentazione di una linea, si muove e genera la rappresentazione di una superficie. Analogamente la rappresentazione di una superficie può muoversi a generare la rappresentazione di un corpo. In conclusione, in geometria, il moto si riferisce sempre a rappresentazioni di enti geometrici le quali generano rappresentazioni di altri enti geometrici.

Fermiamoci un poco sopra i concetti precedenti, e per semplicità e varietà di linguaggio chiamiamo *forma* un corpo geometrico, e chiamiamo *figura* la rappresentazione di una forma (qui s'intende la rappresentazione naturale e non già il disegno che è la rappresentazione di rappresentazione). Ad ogni corpo fisico corrisponde una forma ed una rappresentazione della forma ossia una figura: la figura è cosa che cade sotto i sensi dell'uomo: la forma non cade più sotto i sensi dell'uomo. Per es. fissiamo alcune palle da bigliardo le quali producano su l'uomo le stesse sensazioni; per ognuna, dopo l'astrazione da tutte le proprietà fisiche, rimarrà sempre ciò che in geometria vien chiamato figura e che determina una sensazione: ora facendo astrazione anche da quest'ultima sensazione rimarrà un elemento comune a tutte le dette palle e che dicesi forma o corpo geometrico. Quando un corpo fisico si toglie dal campo dell'osservatore, nella percezione dell'osservatore non esisterà più nè il corpo fisico nè la figura corrispondente al corpo fisico, ma esisterà sempre (date le buone condizioni intellettuali dell'osservatore) il corpo geometrico ossia la forma corrispondente al corpo fisico. Non si può negare che la rappresentazione di una forma sia un corpo (inteso con questo nome non già il solo corpo fisico ma una cosa che cade sotto i sensi ossia generante una sensazione anche diversa da quelle che vanno sotto il nome di proprietà fisiche): questo corpo non è corpo fisico, non avendo più le proprietà fisiche come l'elasticità, la porosità, l'impenetrabilità; però esso è sempre una cosa a cui si associa la nozione di moto precisamente come pei corpi fisici.

Invece la forma non è più corpo (inteso sempre con questa parola una cosa che genera una sensazione) e ad essa, come già si disse, non si associa la nozione di moto.

Riepilogando brevemente diremo: in geometria, per movimento di un corpo si deve sempre intendere il movimento della figura di detto corpo; e poichè questa non è corpo fisico, così al suo movimento sono sempre estranei i fenomeni fisici, quindi il fenomeno fisico della deformazione è completamente estraneo al movimento geometrico.

Il Bustelli colpì nel segno quando scrisse " .... a nessuno sarebbe venuto in animo di screditare, per via di dubbi e di diffidenze, quel postulato (il postulato del movimento nella veste datagli dall'Hoüel) se non vi si fossero ficcate le parole invariabile di forme .... "

4. Si verifica che la distanza tra due paesi è di un dato numero di km; che la cassa contiene un dato numero di monete di data specie; che un corpo ha un dato peso; che una merce è di data qualità; ecc.; si verifica, in un dato ambiente, la legge di gravità, la porosità di corpi dati, ecc.

Si dimostra una proposizione su un triangolo, su un'operazione d'aritmetica, su formole algebriche ecc.; si dimostra, la ragione o il torto di un contendente, un diritto, come un fatto debba essere avvenuto in un modo piuttosto che in un altro ecc.

Verificare significa disporre, ordinare, dei corpi fisici in modo da ottenere un determinato effetto; tale effetto o fatto sperimentale sarà poi indicato con una voce o con un segno o con una proposizione. Dimostrare significa disporre, ordinare, delle proposizioni (in generale delle cose che non sono corpi) in modo da otte- nere, come conseguenza logica, una determinata proposizione.

Nel primo caso, come risultato della verifica, coi sensi si acquista la coscienza dell'effetto: nel secondo caso, come risultato della dimostrazione, si ha il così detto sentimento dell'evidenza. La verifica è, in tutto o in parte, operazione dei sensi, e per essa è proprio l'aggettivo sperimentale: la dimostrazione è essenzialmente operazione di logica e per essa è proprio l'aggettivo razionale, logica.

Per quanto già si è detto, il moto non è operazione che si fa su enti geometrici, ma si bene un operazione che si può fare sulle rappresentazioni di enti geometrici cioè figure; quindi il moto non potrà valere per dimostrare proposizioni su enti geometrici, ma potrà valere per verificare dei fatti (fatti indicati da proposizioni) sulle figure.

Ma intanto, come va che le operazioni di moto e le proposizioni su figure si intendono (e ciò per comodità nello sviluppo della geometria e senza cadere in equivoci o contraddizione) come operazioni di moto e proposizioni su gli enti geo- metrici dei quali esse sono le rappresentazioni? Ecco il nodo della questione.

5. Cominciamo prima di tutto ad intenderci sulla noziono di *identità*.

Avviene spesso che una stessa cosa si indica con due segni diversi, o si nomina con due vocaboli diversi; in tal caso si usa dire che le due cose corrispondenti ai due segni, ai due vocaboli, sono identiche. Quindi identità non esprime altro che una stessa cosa indicata in modi diversi o chiamata con nomi diversi. Non si deve dimenticare che i segni diversi od i vocaboli diversi, attribuiti ad una stessa cosa, corrispondono a diversi istanti, nei quali si pensa alla cosa. La frase " una cosa è identica a sè stessa " non è che un modo per avvertire che la cosa si presenta al pensiero in due istanti diversi. Da una stessa cosa pensata in di- versi istanti, e quindi indicata con segni diversi o chiamata con diversi vocaboli, nasce il sentimento dell'identità. La frase " due forme identiche " non è che un modo per dire " si ha una sola forma pensata in due istanti cioè ottenuta due volte come risultato di astrazione su un corpo fisico o su due distinti corpi fisici. La parola " *replicazione* o *multilocazione* " che si legge nello scritto del Bustelli, sarebbe conveniente per esprimere il suddetto concetto di *identità di forma*.

Parlando di figure, all'identita si dà il nome speciale di *coincidenza* o *sovrap- posizione*: così si dice che, due punti coincidono o sono sovrapposti, per dire che si ha una sola rappresentazione di punto geometrico pensata in due diversi istanti e chiamata con nomi diversi: si dice che, due figure coincidono o sono sovrapposte, per dire che si ha una sola figura con nomi diversi, ossia tutto ciò che si pensa per la figura corrispondente ad un nome vale anche per la figura corrispondente all'altro nome.

Qui può nascere un'obbiezione: considerando le figure come classi di rappresentazioni di punti geometrici, possiamo avere due figure coincidenti secondo la definizione "*due figure coincidono quando ogni punto di una qualunque di esse appartiene anche all'altra*", ma tali che esista una corrispondenza fra la prima ed una terza figura, ed un'altra diversa corrispondenza fra la seconda e la terza: ciò può far dubitare che questa *coincidenza* non sia compresa nel concetto di coincidenza sopra spiegato: ma si deve osservare che la corrispondenza fra la prima e la terza figura è nello stesso tempo corrispondenza tra la seconda e la terza; che la corrispondenza tra la seconda e la terza è nello stesso tempo corrispondenza tra la prima e la terza; che quindi il detto fatto si riduce a porre due diverse corrispondenze tra una figura sola ed una terza figura.

6. Definizione. — *Due figure si dicono eguali quando sono rappresentazioni di una stessa forma (corpo geometrico), o, ciò che è lo stesso, di identiche forme.*

Ricordando quanto si disse al n. 3 sarà chiaro che: quando un corpo fisico si move, ai diversi istanti si fa corrispondere sempre lo stesso corpo fisico e quindi la stessa forma; e le figure, che rappresentano sempre la stessa forma nei diversi istanti, ossia le figure corrispondenti ai diversi istanti, non sono coincidenti ma sono eguali; e ciò stando al significato dato precedentemente alla parola eguale.

L'obbiezione del movimento fisico, reale, non conforme al concetto precedente, è distrutta dal gran principio che caratterizza tutti i rami della matematica e delle altre scienze positive come l'economia politica, la sociologia; principio che nella mente del D'Alembert ha preso questa veste "Le vérités mathématiques sont en quelque sort l'asymptote des vérités physiques".

Volendo introdurre nei ragionamenti la voce *deformazione,* questa si deve prendere per indicare una classe di forme oppure la corrispondente classe di figure: così i termini "forma variabile, figura variabile" si spiegano in modo analogo ai termini "numero variabile, grandezza variabile, valore variabile", i quali sono presi per indicare, classe di numeri, classi di grandezze, classi di valori. Quando si dice "gli agenti fisici agiscono in un certo intervallo di tempo sopra un corpo, modificandone le proprietà fisiche e la figura e la forma", il geometra intende che: si ha una determinata classe di corpi, ad ogni istante dell'intervallo considerato corrisponde un corpo con la sua figura e forma.

Il movimento geometrico (al quale sono estranei i fenomeni fisici) si traduce nella percezione, di un solo corpo fisico in diversi istanti, e di molte figure eguali (una per istante), e di una sola forma: invece il movimento con deformazione si traduce nella percezione, di una classe di corpi (uno per istante), e di molte figure (una per istante), e di molte forme (una per istante). Con altre parole si dirà: ad una classe di istanti, l'operazione di movimento geometrico fa corrispondere uno stesso corpo fisico, una stessa forma, una classe di figure eguali; invece l'operazione di movimento con deformazione fa corrispondere una classe di corpi, una classe di forme, una classe di figure.

In conclusione la voce "deformazione" deve essere bandita dalla geometria elementare, prima perchè indica un concetto totalmente estraneo alla geometria elementare, secondariamente perchè indica un concetto molto più complesso di quello del movimento geometrico, invero, è molto più semplice, chiara, distinta, la visione di un corpo e di una forma che non la visione di una classe di corpi e di una classe di forme. Il movimento con deformazione, introdottosi di nascosto e fraudolentemente, nella geometria per mezzo delle frasi « senza deformazione, invariabilità di una figura, ecc. », ha generato confusione ed ha fatto credere che il provare l'eguaglianza delle figure con l'operazione di movimento sia un circolo vizioso.

7. Per togliere di mezzo alcune obbiezioni che si potrebbero fare sulle precedenti conclusioni, le quali sono in sostanza basate su queste tre cose distinte, corpo fisico, sua figura, sua forma, ritorniamo su ciò che già si è detto al n. 3, e riprendiamo l'esempio delle palle da bigliardo, le quali producono su noi le identiche sensazioni. Fissiamone una, e su questa facciamo astrazione da una proprietà fisica (la quale si traduce poi in una sensazione) p. e. dalla gravità. Dopo ciò, noi diremo forse che si ha ancora lo stesso corpo? È vero che per i nostri cinque sensi non vi sarà forse modificazione alcuna, è vero che un altro uomo non può accorgersi della nostra astrazione, possono essere vere tante altre belle cose, ma noi diremo sempre di non avere più la palla di prima e di avere un'altra cosa, che però è sempre un corpo (inteso con questo nome una cosa che genera sensazioni). Continuiamo a far successivamente astrazione dall'elasticità, dalla porosità, e avremo successivi corpi derivati e tra loro differenti. Facciamo ancora astrazione dalla durezza e dal colore.

Quale sarà il risultato finale di quest'ultime astrazioni? Certamente sarà cosa che non ha più relazione coi, così detti, due sensi fondamentali del tatto e della vista; però non sarà assurdo immaginare che abbia relazioni con altri sensi dell'uomo; ma se anche, relativamente all'uomo, non ha più relazione con alcun senso, possiamo noi dire che esso non sia cosa atta a generare sensazioni su strutture organiche più perfezionate della struttura umana? Non si dica che tolte tutte le proprietà fisiche, a noi cognite, il corpo resta distrutto. Invece non si deve dimenticare che, tutte le proprietà fisiche di un corpo sono funzioni dei diversi organi della sensibilità degli uomini, e che, fatta astrazione da tutte le proprietà fisiche, per necessità logica, rimarrà sempre quell'essenza a noi ignota la quale in presenza di strutture organiche superiori a quelle degli uomini, può determinare nuove e più potenti sensazioni. Bisogna poi anche osservare che si ha sovente il fatto di diverse sensazioni simultanee; queste nel mondo fisico, empirico, devono stare sempre insieme, ma nel campo del pensiero si separano e si considerano indipendentemente l'una dall'altra.

Per quanto si è detto, non è nè metafisico, nè oscuro, nè difficile l'ammettere che: per la fissata palla da bigliardo, simultaneamente alle sensazioni del tatto e della vista, vi ha un'altra sensazione che chiameremo *sensazione della figura*. E questa sensazione non corrisponde ancora alla « forma », poichè resta nella coscienza anche senza l'esistenza delle altre palle dell'esempio proposto. Ripetiamo: per ognuna delle palle vi ha un qualcosa, che in noi produce una sensazione, la quale nel mondo fisico è sempre simultanea ad altre, un qualcosa che non ha più le proprietà fisiche dell'elasticità, dell'impenetrabilità ecc., un qualcosa a cui si associa il moto, o a cui si dà il nome di figura. Finalmente l'ultima astrazione dalla sensazione di figura dà per risultato un elemento non più speciale per ogni palla, ma comune a tutte le palle, un elemento logico a cui si dà il nome di forma o corpo geometrico comune a tutte le palle dell'esempio proposto.

Ad ogni corpo fisico corrisponde la sua figura e la sua forma; e, per la definizione al n. 6, ad ogni classe di figure eguali corrisponde una sola forma o corpo geometrico. Certamente, la definizione formale di eguaglianza tra figure, non contiene il movimento, perchè essa si traduce in identità delle forme rappresentate dalle figure. Però data una figura, come è mai possibile ottenere altre figure ad essa eguali senza il movimento della figura data? Il movimento è l'unico generatore delle figure eguali ad una data; senza il movimento la definizione di eguaglianza tra figure sarebbe sterile, ossia priva di un contenuto utile.

A questo punto apriamo una parentesi. Pare che la " definizione di eguaglianza tra segmenti „ data dal Veronese, sia in qualche modo in opposizione colle precedenti conclusioni. Vediamo un po'.

L'eguaglianza di due segmenti, per il Veronese, si riduce a corrispondenza fra parti oppure punti di segmenti; dunque per il Veronese il segmento esiste in quanto che è un complesso o classe di cose dette o parti di segmento, oppure punti. Ma se noi, come vedremo fra poco, intenderemo il segmento per una cosa, ossia individuo e non per una classe, certamente non accetteremo più la definizione del Veronese. Un individuo non può mai identificarsi con una classe. Avviene spesso il caso in cui una stessa cosa (per es. segmento) viene considerata sotto due aspetti differenti: questo modo di esprimersi è una forma linguistica popolare e poco esatta poichè, rigorosamente parlando, le differenze di aspetto o di punto di vista costituiscono differenze di obbietto: quando si dice che due teorie trattano della medesima cosa o del medesimo fenomeno da punti di vista differenti, si vuol intendere di considerare in una stessa cosa, *caratteri tipici differenti;* e questi caratteri tipici differenti costituiscono effettivamente obbietti differenti rispetto alla logica.

La definizione del Veronese è il capo saldo di una nuova e pregevole teoria, la quale, nei principi, non può essere nè in accordo nè in opposizione alla teoria basata sul movimento: queste due teorie si possono paragonare a due viandanti che sono incamminati su strade differenti e che senza punto mai disturbarsi arrivano alla stessa meta.

8. Fin qui si è sempre parlato delle figure e forme corrispondenti ai corpi fisici, dimenticando quelle cose che s' intuiscono come elementi delle figure, cioè le superficie, le linee, i punti. Queste sono strettamente unite al concetto indefinibile di limite, anzi costituiscono lo stesso concetto considerato nel solo campo geometrico. Basterà accennare brevemente che:

la superficie è il limite tra due parti di una figura oppure tra la figura e tutto ciò che è diverso dalla figura;

la linea è il limite tra due parti di una superficie oppure tra la superficie e tutto ciò che è diverso dalla superficie;

il punto è il limite tra due parti di una linea oppure tra la linea e tutto ciò che è diverso dalla linea.

In seguito alla superficie ed alla linea si diede un significato più esteso per poter comprendere sotto queste denominazioni anche ciò che vien chiamato superficie e linea illimitata: invero dal corpo fisico e dalla corrispondente figura non può sorgere il concetto di " *illimitato* „ questo può sorgere solamente da postulato o da considerazioni speciali da farsi sulle stesse superficie o linee. Finalmente si presero a formulare certi postulati da applicarsi a superficie e linee, e scaturirono determinati concetti di piano e di retta illimitata.

Alla voce figura si diede poi un senso più ampio, comprendendo sotto questa denominazione anche le superficie, le linee, i punti, ed associando il movimento anche a questi elementi, ed estendendo a questi tutto ciò che s'è detto per le figure corrispondenti a corpi fisici.

Certamente per la logica è molto più comodo e vantaggioso partire da quegli elementi caratterizzati da maggior numero di postulati, ed è per questa ragione che nello studio della geometria s'incomincia dalla retta e dal piano. Però le nostre conoscenze si succedono secondo quest'ordine: corpo fisico; figura corrispondente al corpo fisico; superficie; linea; punto; porzione di piano; segmento; piano; retta; forme; eguaglianza di figure e moto come mezzo per verificare l'eguaglianza di figure; infine moti su punto, su linea, su superficie, considerati come generatori delle figure dette linea, superficie, e delle figure corrispondenti a corpi fisici. Cerchiamo di seguire lo sviluppo di un bambino posto in ambiente normale, vedremo che si metterà in rapporto col mondo a grado a grado, e seguendo con grande approssimazione la successione su detta.

9. Data una *figura* (intesa, d'ora in avanti, in senso lato come si spiegò al n. precedente) diremo che il moto è l'unico generatore delle figure eguali alla data ed eguali tra loro: date due figure, alla questione " riconoscere se sono eguali " si può dare l'espressione " riconoscere se una delle due figure appartiene alla classe generata dal moto dell'altra ".

Ora osserviamo che di solito, per constatare se una data cosa appartiene ad una certa classe, non è necessario avere presenti tutti gli individui della classe per poi riconoscere l'identità di uno di essi con la cosa data, ma bastano alcune relazioni logiche tra la cosa data e la classe. Così per constatare, se una di due figure date appartiene alla classe delle eguali all'altra, non è necessario nè eseguire realmente il movimento su una figura, nè avere la sensazione dello stesso movimento, ma bastano alcune proposizioni relative al moto di figure; proposizioni che si possono intendere o come postulati del movimento o come postulati delle figure.

Gamalero, 16 Settembre 1900.

Prof. Pietro Buffa.

RISOLUZIONI DELLE QUISTIONI 228, 526, 527, 528, 530, 532

228. *Per un punto* S, *ad un cerchio* φ *si conducano le secanti arbitrarie* SBC, SMM′, *e la secante* SAD, *perpendicolare al diametro che passa per* B; *si avrà*

$$\tan\frac{BC}{2}\cdot\tan\frac{BM}{2}\tan\frac{BM'}{2}-\tan^2\frac{BA}{2}\left(\tan\frac{BM}{2}+\tan\frac{BM'}{2}-\tan\frac{BC}{2}\right)=0.$$

A. Del Re.

Risoluzione del dott. Roberto Volpi a Modena.

Si riferisca la figura a due assi ortogonali coll'origine nel centro di φ e colla parte positiva dell'asse OX passante per B; si dicano a, b le coordinate di S, ed m il coefficiente angolare della MM′. L'ascissa di A è a, quindi, se r è il raggio di φ, si ha subito $\tan^2\frac{1}{2}\,BA=\frac{r-a}{r+a}$. Di più $\frac{1}{2}\,B(O)C=C(B)O$, perchè la bisettrice di B(O)C e la AD sono perpendicolari ai lati di C(B)O; quindi si ha $\tan\frac{1}{2}\,BC=\frac{r-a}{b}$.

Nota. — Nel numero precedente fu per errore dimenticato il nome del prof. G. Mola fra i risolutori delle questioni 521, 522, 523, 524.

Inoltre si osserva facimente che la perpendicolare per O alla MM' fa con OB un angolo $= \frac{1}{2}$ B (O) M $+ \frac{1}{2}$ B (O) M', e quindi che è $\tan \frac{1}{2}(\mathrm{BM} + \mathrm{BM'}) = -\frac{1}{m}$. Tenendo conto di queste uguaglianze e della formula $\tan\alpha + \tan\beta = \tan(\alpha + \beta)(1 - \tan\alpha\tan\beta)$, l'uguaglianza proposta si trasforma nella equivalente

$$\tan\frac{\mathrm{BM}}{2}\tan\frac{\mathrm{BM'}}{2} = \frac{b + m(r - a)}{b - m(r + a)}.$$

Ora facendo sistema delle equazioni di φ e di MM', per determinare le ascisse x ed x' di M ed M' si ha l'equazione $(b - am + mx)^2 + x^2 = r^2$, dalla quale si ha subito

$$\tan\frac{\mathrm{BM}}{2}\tan\frac{\mathrm{BM'}}{2} = \sqrt{\frac{r - x}{r + x}}\sqrt{\frac{r - x'}{r + x'}} = \pm\frac{b + m(r - a)}{b - m(r - a)}.$$

Una facile ispezione della figura, che per la generalità delle formule usate può limitarsi ad un solo caso particolare, mostra la convenienza del segno superiore, e resta in tal modo dimostrata l'uguaglianza enunciata.

526. *Il circolo osculatore in un punto* M *variabile d'un'ellissi incontra l'ellissi in* P. *Trovare l'area della curva inviluppo della perpendicolare abbassata da* M *sulla tangente all'ellissi nel punto* P.

E.-N. Barisien.

Risoluzione del dott. Roberto Volpi a Modena.

È noto che se φ è l'angolo eccentrico corrispondente al punto M, quello corrispondente a P vien dato da -3φ (v. p. es. Salmon, *Sez. Con.*, trad. *Dino*, p. 221). Essendo allora $a\cos 3\varphi$ e $-b\,\mathrm{sen}\,3\varphi$ le coordinate cartesiane di P rispetto agli assi dell'ellissi, si ricava per il coefficiente angolare della tangente in P : $\frac{b\cos 3\varphi}{a\,\mathrm{sen}\,3\varphi}$, e per l'equazione della perpendicolare da M sulla tangente in P, dopo poche trasformazioni:

$$(1)\qquad a\,\mathrm{sen}\,3\varphi\,.\,\mathrm{X} + b\cos 3\varphi\,.\,\mathrm{Y} = \frac{1}{2}(a^2 + b^2)\,\mathrm{sen}\,4\varphi + \frac{1}{2}(a^2 - b^2)\,\mathrm{sen}\,2\varphi;$$

e derivando rapporto a φ,

$$(2)\qquad 3a\cos 3\varphi\,.\,\mathrm{X} - 3b\,\mathrm{sen}\,3\varphi\,.\,\mathrm{Y} = 2(a^2 + b^2)\cos 4\varphi + (a^2 - b^2)\cos 2\varphi.$$

Dalle (1) e (2), trasformando in somme i prodotti di seni e coseni, si deduce:

$$\mathrm{X} = \frac{1}{12a}[(a^2 + b^2)\cos 7\varphi - (a^2 - b^2)\cos 5\varphi + 2(6a^2 + b^2)\cos\varphi]$$

$$\mathrm{Y} = \frac{1}{12b}[-(a^2 + b^2)\,\mathrm{sen}\,7\varphi + (a^2 - b^2)\,\mathrm{sen}\,5\varphi + 2(a^2 + 6b^2)\,\mathrm{sen}\varphi],$$

donde

$$d\mathrm{X} = \frac{1}{12a}[-7(a^2 + b^2)\,\mathrm{sen}\,7\varphi + 5(a^2 - b^2)\,\mathrm{sen}\,5\varphi - 2(6a^2 + b^2)\,\mathrm{sen}\varphi]$$

$$d\mathrm{Y} = \frac{1}{12b}[-7(a^2 + b^2)\cos 7\varphi + (a^2 - b^2)\cos 5\varphi + 2(a^2 + 6b^2)\cos\varphi].$$

Ora è facile osservare, anche senza entrare in dettagli di calcolo, che, trasformando sempre in somme i prodotti di seni e coseni, le espressioni di XdY e YdX contengono un termine indipendente da φ e dei termini con solo fattore variabile della forma $\mathrm{sen}\,2k\,\varphi$, che nell'integrazione da 0 a $\frac{\pi}{2}$ vengono evidentemente a sparire. Curandosi soltanto del calcolo del termine indipendente da φ e posto mente alla manifesta simmetria dell'inviluppo rispetto agli assi, si trova senza difficoltà:

$$\text{area} = 4\int_0^b \mathrm{X}d\mathrm{Y} = 4\int_0^a \mathrm{Y}d\mathrm{X} = \frac{a^4 + 12a^2b^2 + b^4}{6\,ab}\int_0^{\frac{\pi}{2}} d\varphi = \frac{a^4 + 12a^2b^2 + b^4}{12\,ab}\,\pi.$$

527. *Si trovi:*

1° *il luogo dei centri dei circoli inscritti ed ex-inscritti a tutti i triangoli, che, essendo inscritti in un circolo dato, hanno due loro lati paralleli a due direzioni date;*

2° *l'inviluppo del terzo lato di questi triangoli.*

E.-N. Barisien.

Risoluzione del dott. Roberto Volpi a Modena.

1°. Sul circolo dato C di centro O si segnino le coppie di punti A, A' e B, B' per cui passano le tangenti rispettivamente parallele alle due direzioni fisse a e b. Scelto un punto qualunque X sopra C, si dicano M ed N i punti in cui le parallele per X ad a e b tornano ad incontrare C. Le bisettrici del triangolo XMN uscenti da X sono costantemente parallele a quelle dell'angolo (ab), quelle uscenti da M passano una per B e l'altra per B', essendo B e B' punti di mezzo degli archi XN e quelle uscenti da N passano per A ed A'. Detto poi Y il punto comune a tre di queste bisettrici, si osserva che uno degli angoli formati dalle MY ed NY è supplemento di Y(M)N + Y(N)M e quindi manifestamente uguale al complemento della metà di uno degli angoli (ab). Essendo adunque costanti gli angoli formati dalle MY ed NY e passando queste rette per due dei quattro punti A, A', B, B', si deduce che Y deve trovarsi su uno di quattro circoli fissi passanti rispettivamente per le coppie di punti AB', B'A', A'B, BA. Di più si osserva subito che questi circoli (per la grandezza degli angoli insistenti sulle corde corrispondenti alle coppie di punti testè nominati) debbono avere i centri nei vertici del parallelogrammo circoscritto a C coi lati perpendicolari alle rette a e b, e che debbono essere uguali a C, perchè, detto ad es. O_1 il centro di quello che passa per A e B, si ha $B(O_1)A = B(O)A$, essendo entrambi questi angoli uguali ad uno di quelli delle rette a e b. Finalmente si nota che scelto un punto qualunque Y sopra uno dei quattro circoli, per es., quello di centro O_1, le AY e BY incontrano nuovamente C in M ed N e che la corda MN è capace in C di un angolo MBA' = A(Y)B — A(A')B = ang. (ab), e quindi che le parallele per M ad a e b s'incontrano in un punto X di C, dando luogo ad un triangolo XMN inscritto in C ed avente Y come centro del circolo iscritto o di uno degli ex-iscritti. Resta così provato che il luogo richiesto è costituito dall'assieme di quei quattro circoli.

2°. Il terzo lato MN, essendo una corda di C su cui insiste un angolo costante (ab) è di lunghezza costante, e quindi inviluppa un circolo concentrico al dato e di facilissima costruzione.

528. *Sulla tangente in un punto M di una parabola di fuoco F si prendano due punti M', M'', tali che sia MM' = MM'' = MF. Il luogo di questi punti M', M'' è una cubica. Si trovi l'area compresa fra questa curva e il suo asintoto.*

E.-N. Barisien.

Risoluzione del prof. G. Mola a Campobasso.

Un punto M della parabola riferita al fuoco F, se θ è l'angolo che il vettore FM fa con l'asse, ed a la distanza focale, può rappresentarsi con l'equipollenza

$$M = \frac{a\varepsilon^{\theta}}{\operatorname{sen}^2 \frac{\theta}{2}}.$$

Derivando, abbiamo

$$DM = \frac{-a\cos\frac{\theta}{2}\,.\,\text{sen}\frac{\theta}{2}}{\text{sen}^4\frac{\theta}{3}}\,\varepsilon^{\theta} + i\frac{a}{\text{sen}^2\frac{\theta}{2}}\,\varepsilon^{\theta} = \frac{-a\left(\cos\frac{\theta}{2} - i\,\text{sen}\,\frac{\theta}{2}\right)}{\text{sen}^3\frac{\theta}{2}}\,\varepsilon^{\theta} = \frac{-a}{\text{sen}^3\frac{\theta}{2}}\,\varepsilon^{\frac{\theta}{2}}.$$

Il modulo di questa espressione indica un segmento della tangente menata alla curva dal punto M. Esso, moltiplicato per sen $\frac{\theta}{2}$, diventa eguale in grandezza al vettore FM. Onde se MM' e MM'' sono due segmenti opposti presi sulla tangente dal punto M, ed eguali ad FM, sussisteranno le equipollenze

$$MM' = \frac{-a\varepsilon^{\frac{\theta}{2}}}{\text{sen}^2\frac{\theta}{2}},\qquad MM'' = \frac{a\varepsilon^{\frac{\theta}{2}}}{\text{sen}^2\frac{\theta}{2}},$$

ovvero, poichè $FM' = FM + MM'$, $FM'' = FM + MM'$,

$$FM' = \frac{a}{\text{sen}^2\frac{\theta}{2}}\left(\varepsilon^{\theta} - \varepsilon^{\frac{\theta}{2}}\right),\ FM'' = \frac{a}{\text{sen}^2\frac{\theta}{2}}\left(\varepsilon^{\theta} + \varepsilon^{\frac{\theta}{2}}\right).$$

Possiamo sostituire ad $\varepsilon^{\theta} - \varepsilon^{\frac{\theta}{2}}$, $\varepsilon^{\theta} + \varepsilon^{\frac{\theta}{2}}$, $\text{sen}^2\frac{\theta}{2}$, rispettivamente i valori $2i\,\text{sen}\frac{\theta}{4}\,\varepsilon^{\frac{3\theta}{4}}$, $2\cos\frac{\theta}{4}\,\varepsilon^{\frac{3\theta}{4}}$, $4\,\text{sen}^2\frac{\theta}{4}\cos^2\frac{\theta}{4}$, e porre $\frac{\varphi}{3}$ invece di $\frac{\theta}{4}$; avremo allora che i luoghi di M' e M'' sono dati da

$$M' = \frac{ai\varepsilon^{\varphi}}{\text{sen}\,\frac{2\varphi}{3}\,.\,\cos\frac{\varphi}{3}},\quad M'' = \frac{a\varepsilon^{\varphi}}{\text{sen}\,\frac{2\varphi}{3}\,\text{sen}\,\frac{\varphi}{3}}.$$

Quando diamo a φ il valore zero, M' e M'' indicheranno punti infinitamente lontani, M'' nella direzione positiva dell'asse, M' nella direzione positiva della perpendicolare elevata da F. Per $\varphi = \frac{\pi}{2}$, abbiamo

$$FM' = \frac{-4a}{3},\quad FM'' = \frac{4ai}{\sqrt{3}},$$

cioè vengono determinati due punti, uno A, sull'asse, e l'altro B sulla perpendicolare elevata da F. E per $\varphi = \pi$, otteniamo $FM' = \frac{-4ai}{\sqrt{3}}$, $FM'' = \frac{-4a}{3}$, che mostrano che M', è in B', simmetrico di B, e M'' in A. Dunque si hanno due rami di curve che hanno un punto all'infinito sull'asse, e che si tagliano nel punto A; due loro parti simmetriche tagliano dalla perpendicolare il segmento BB', e le altre due parti hanno questa perpendicolare per asintoto.

Derivando il valore del vettore M', si ha

$$DM' = \frac{\left(ai\,\text{sen}\,\frac{\varphi}{3}\,\text{sen}\,\frac{2\varphi}{3} - 2ai\cos\frac{\varphi}{3}\cos\frac{2\varphi}{3}\right)\varepsilon^{\varphi}}{3\cos^2\frac{\varphi}{3}\,.\,\text{sen}^2\frac{2\varphi}{3}} - \frac{a\varepsilon^{\varphi}}{\cos\frac{\varphi}{3}\,\text{sen}\,\frac{2\varphi}{3}},$$

che, riducendo, si trasforma in

$$\mathrm{DM}' = -\frac{a\varepsilon^{\frac{2\varphi}{3}}}{3\cos^2\frac{\varphi}{3}\cdot\operatorname{sen}\frac{2\varphi}{3}} - \frac{2ai\varepsilon^{\frac{\varphi}{3}}}{3\cos\frac{\varphi}{3}\cdot\operatorname{sen}^2\frac{\varphi 2}{3}}.$$

Onde per trovare il valore dell'area elementare $d\mathrm{A}$ descritto dal vettore M', ed espressa da

$$d\mathrm{A} = \frac{i}{4}(\mathrm{M}'\cdot cjd\mathrm{M}' - d\mathrm{M}'\cdot cj\mathrm{M}'),$$

dobbiamo in questa formula sostituire i valori

$$M' = \frac{ai\varepsilon^{\varphi}}{\cos\frac{\varphi}{3}\operatorname{sen}\frac{2\varphi}{3}},\ d\mathrm{M}' = -\frac{a\varepsilon^{\frac{2\varphi}{3}}\cdot d\varphi}{3\cos^2\frac{\varphi}{2}\operatorname{sen}\frac{2\varphi}{3}} - \frac{2ai\varepsilon^{\frac{\varphi}{3}}\cdot d\varphi}{3\cos\frac{\varphi}{3}\operatorname{sen}^2\frac{2\varphi}{3}}$$

ed i coniugati dei medesimi

$$cj\mathrm{M}' = \frac{-ai\varepsilon^{-\varphi}}{\cos\frac{\varphi}{3}\operatorname{sen}\frac{2\varphi}{4}},\ cjd\mathrm{M}' = -\frac{a\varepsilon^{-\frac{2\varphi}{3}}\cdot d\varphi}{3\cos^2\frac{\varphi}{3}\cdot\operatorname{sen}\frac{2\varphi}{3}} + \frac{2ai\varepsilon^{-\frac{\varphi}{3}}\cdot d\varphi}{3\cos\frac{\varphi}{3}\cdot\operatorname{sen}^2\frac{2\varphi}{3}}.$$

Dopo facili riduzioni si trova

$$d\mathrm{A} = \frac{a^2}{2}\frac{d\varphi}{\cos^2\frac{\varphi}{3}\operatorname{sen}^2\frac{2\varphi}{3}},$$

che, integrata, tra i valori limiti $\frac{\pi}{2}$ e π di φ, dà $\mathrm{A} = \frac{10}{9}\sqrt{3}\cdot a^2$. Onde tutta l'area finita compresa tra la curva ed il segmento BB' dell'asintoto è ugnale a $\frac{20}{9}\sqrt{3}\,a^2$.

530. *Se si porta sopra ogni raggio vettore focale* FM *d'un'ellisse un segmento uguale ad un semidiametro coniugato a quello che passa per* M, *il luogo dell'estremo di questo segmento è una quartica di cui l'area è equivalente a quella dell'ellisse.*

E.-N. Barisien.

Risoluzione del dott. Roberto Volpi a Modena.

Se x ed y sono le coordinate di M rispetto agli assi dell'ellisse, come è noto, la lunghezza del semidiametro coniugato a quello che passa per M è data da $\sqrt{a^2 - e^2x^2}$, sicchè chiamando ρ e φ le coordinate polari di un punto del luogo cercato, rispetto ad F (di ascissa positiva) ed all'asse maggiore dell'ellisse, per equazioni parametriche del luogo medesimo si ottiene subito:

$$\text{(I)} \qquad \rho = \pm\sqrt{a^2 - e^2x^2} \qquad \tan\varphi = \frac{b\sqrt{a^2 - x^2}}{a(x - ae)}.$$

Queste mostrano che ad ogni valore di φ corrispondono quattro valori per ρ e quindi che una retta passante per F (ed anche una retta, qualunque del piano) incontra la locale in quattro punti: in altri termini che essa è una *quartica*.

Quanto all'area, detto ω l'angolo che la tangente in M fa colla parte positiva dell'asse delle x, e λ la grandezza assoluta dell'angolo acuto che la tangente stessa fa colla MF, si ha che è $\varphi = \omega - \lambda$, e per il punto M', diametralmente opposto ad M, $\varphi' = \omega - \lambda$; e ciò in forza della simmetria dell'ellisse rispetto ai suoi assi e della nota proprietà degli angoli che una tangente all'ellisse fa coi raggi focali del punto di contatto. Osservando ancora che nei punti M ed M' i valori di ρ e ρ sono manifestamente uguali, si ha che la somma dei due elementi di area corrispondenti ai punti M ed M' è data da:

$$\frac{1}{2}\rho^2 d\varphi + \frac{1}{2}\rho'^2 d\varphi' = \rho^2 d\omega$$

e quindi subito: area $= \int_0^{\pi} \rho^2 d\omega$, che è evidentemente l'area dell'ellisse, essendo ρ la lunghezza di un semidiametro corrente, e $d\omega$ il differenziale dell'angolo che esso fa coll'asse maggiore.

È da notarsi che la locale (1) si compone di due pezzi chiusi, uguali e simmetrici rispetto all'asse maggiore dell'ellisse, aventi ciascuno area uguale all'ellisse etc. etc.

532. *Se* y *è una funzione della variabile* x, *ponendo* $x = e^t$, *ed assumendo* t *come nuova variabile indipendente si ha, qualunque sia* n,

$$x^n \frac{d^n y}{dx^n} = \frac{d^n y}{dt^n} - s_1 \frac{d^{n-1} y}{dt^{n-1}} + s^2 \frac{d^{n-2} y}{dt^{n-2}} - \ldots + (-1)^h s_h \frac{d^{n-h} y}{dt^{n-h}} + \ldots + (-1)^{n-1}(n-1)!\frac{dy}{dt},$$

dove s_h *indica la somma dei* $\binom{n-1}{h}$ *prodotti dei numeri* $1, 2, \ldots, n-1$, *combinati ad* h *ad* h *in tutti i modi possibili.*

M. Chini.

Risoluzione del dott. Roberto Volpi.

Derivando i due membri dell'uguaglianza rapporto a t, e risolvendo rispetto a $x^{n+1}\frac{d^{n+1} y}{dt^{n+1}}$, si ottiene

$$x^{n+1}\frac{d^{n+1} y}{dx^{n+1}} = \frac{d^{n+1} y}{dt^{n+1}} + \sum_{h=0}^{h=n-1}(-1)^h (s_h + ns_{h-1})\frac{d^{n-h} y}{dt^{n-h}} + (-1)^n n!\frac{dy}{dt},$$

ed avendosi manifestamente $s_h + ns_{h-1} =$ somma degli $\binom{n}{h}$ prodotti dei numeri $1, 2, \ldots, n$, combinati ad h ad h in tutti i modi possibili, resta dimostrata per induzione la formula enunciata, giacchè essa è valida per $n = 1$.

Altra risoluzione del sig. Santacroce, studente di Napoli.

QUISTIONI PROPOSTE

531. *(Errata nel num. precedente).* Dimostrare che

$$\int_{15}^{27} \frac{(x-15)\,dx}{\sqrt{12x-(x^2-9)^2}} = \frac{36}{5}.$$

533. Sia M un punto variabile di un'ellisse, C il centro di curvatura relativo al punto M; H e H_1 due punti situati sulla tangente in M tali che sia $MH = MH_1 = MC$; C_1 il simmetrico di C rapporto ad M. Trovare le aree delle curve, luoghi dei punti H, H_1, C_1 e dei punti di mezzo dei lati del quadrato CHC_1H_1.

534. Due circoli variabili O e O′ ortogonali s'incontrano in due punti A e B fissi. Una delle tangenti comuni tocca i due circoli nei punti T e T′.

1°. Il luogo del punto comune alle rette OT′ e O′T è una retta.

2°. Il luogo del punto comune alle rette AT e BT′ è un'ellisse.

3°. La differenza delle aree dei triangoli ATT′ e BTT′ è costante.

4°. Il luogo dell'ortocentro del triangolo ATT′ è una quartica.

535. Dimostrare che

$$\int_0^{\frac{\pi}{2}} \frac{\operatorname{sen}^4\theta \cos^4\theta \, d\theta}{(a^2 \operatorname{sen}^2\theta + b^2 \cos^2\theta)^4} = \frac{1}{a^3 b^3} \int_0^{\frac{\pi}{2}} \frac{\operatorname{sen}^4\theta \cos^4\theta \, d\theta}{a^4 \operatorname{sen}^2\theta + b^4 \cos^2\theta}.$$

536. Dimostrare che

$$2 \int_0^{\frac{\pi}{2}} d\varphi \sqrt{a^2 \operatorname{sen}^2\varphi + b^2 \cos^2\varphi} =$$

$$= (a^2 + b^2) \int_0^{\frac{\pi}{2}} \frac{d\varphi}{\sqrt{a^2 \operatorname{sen}\varphi + b^2 \cos\varphi}} - (a^2 - b^2)^2 \int_0^{\frac{\pi}{2}} \frac{\operatorname{sen}^2\varphi \cos^2\varphi \, d\varphi}{(a^2 \operatorname{sen}\varphi + b^2 \cos\varphi)^{\frac{3}{2}}}.$$

537. Trovare l'area della curva inviluppo delle rette condotte per i punti di un asteroide in modo che la tagli negli stessi punti sotto un angolo costante. (Questa curva è la sviluppata obliqua dell'asteroide.)

538. Si considerino tutti i triangoli ABC, di cui la BC è fissa e di cui il vertice A si sposta sopra una retta parallela a BC. Dimostrare che

1° il luogo dell'ortocentro e quello del centro del circolo dei nove punti del triangolo ABC sono due parabole;

2° il luogo del punto di Lemoine del triangolo ABC è un'ellisse.

E.-N. Barisien.

539. Calcolare

$$\int \left[\left\{ 1 + n \operatorname{sen}^{n-1} x \right\} \operatorname{sen}(n+1)\, x \, dx \right].$$

G. Giovanetti.

540. Risolvere le equazioni

$$\frac{1}{x} + \frac{1}{x-1} + \frac{1}{x-2} + \frac{1}{x-3} = 0$$

$$\frac{1}{x} + \frac{1}{x-1} + \frac{1}{x-2} + \frac{1}{x-3} + \frac{1}{x-4} = 0$$

$$\frac{1}{x} + \frac{1}{x-1} + \frac{1}{x-2} + \frac{1}{x-3} + \frac{1}{x-4} + \frac{1}{x-5} = 0.$$

M. Chini.

BIBLIOGRAFIA

PINCHERLE. — *Introduzione al corso di algebra complementare e di geometria analitica.* Appunti redatti per uso degli studenti. Bologna, Zanichelli, 1901.

Riproduciamo la breve prefazione di questa utilissima operetta.

" Scopo di questa introduzione è di riassumere brevemente, nelle sue parti " essenziali, la genesi dei numeri reali, e di stabilire in modo preciso la corri" spondenza biunivoca fra i numeri reali ed i segmenti della retta: corrispondenza " che sta a fondamento della geometria analitica ".

Nei primi due capitoli dopo avere ricavato dall'operazione del contare il concetto di numeri interi e positivi ed avere esaminato rapidamente le loro proprietà formali, vengono dedotte con metodo chiaro e rigoroso tutte le successive generalizzazioni del concetto di numero per mezzo *del principio di permanenza* o *conservazione delle leggi formali.*

Nel terzo capitolo viene stabilita la corrispondenza fra i numeri reali ed i segmenti.

Troviamo molto lodevole lo scopo prefissosi, ed interamente raggiunto dal chiaro autore, di porre su basi solide e rigorose i fondamenti della geometria analitica.

K.

GIORLI. — *L'aritmetica e la geometria dell'operaio.* Manuali Höepli, 1900.

Come si vede dal titolo, questo libro non ha pretese scientifiche, ed ha per iscopo di raccogliere in piccolo volume un gran numero di nozioni pratiche relative all'aritmetica e alla geometria, ed è " compilato, come dice l'autore nella " prefazione, sulla base degli esami per Capi-tecnici ed Assistenti della R. Marina, " nonchè per l'ammissione dei giovani alla scuola macchinisti e fuochisti delle " ferrovie ".

La modestia degli intenti non ci sembra che giustifichi il sacrificio della chiarezza e della precisione che si nota in tutto il volume. — Senza dilungarci citeremo un solo esempio fra i moltissimi. A pag. 155: " Il prisma è un solido " che ha per basi due poligoni qualunque e per facce laterali tanti rettangoli, " parallelogrammi o trapezi, per quanti sono i lati del poligono base "!

K.

GHERSI. — *Conti e calcoli fatti.* Novantatre tabelle ed istruzioni pratiche sul modo di usarle. Manuali Höepli, 1901.

È un volumetto di molta utilità pratica poichè le novantatre tavole, che lo compongono, contengono i dati numerici relativi ad una quantità di cose svariatissime e di uso comune, e permettono quindi di risparmiare molti calcoli. — Riproduciamo sommariamente l'indice per dare un'idea dell'opera.

Misure, pesi e monete. — Misurazioni delle botti. — Termometri. — Pressioni dei gaz e vapori. — Areometri. — Miscele d'acqua e d'alcool. — Soluzioni zuccherine. — Soluzioni di glicerina. — Pesi specifici. — Legnami. — Carbone di legna. — Peso dei metalli. — Viti. — Dadi. — Divisione del tempo. — Paga giornaliera. — Prezzo del grano e del granturco. — Interessi ed annualità. — Rendita. — Potenze radici ed indici dei numeri. — Poligoni regolari. — Sfera. — Divisione della circonferenza. — Inclinazione e pendenza. K.

DA GIORNALI E RIVISTE

Annali di matematica pura ed applicata.

Serie III, tomo IV, fasc. 3° e 4°. — *De Sanctis*, Alcuni nuovi teoremi sulle funzioni armoniche a tre variabili. — *Timerding*, Sur les lignes osculatrices d'une cubique gauche. — *Pincherle*, Di alcune operazioni atte ad aggiungere o togliere singolarità in una funzione analitica. — *Lauricella*, Su di una classe di equazioni alle derivate parziali del secondo ordine.

Serie III, tomo V, fasc. 1°. — *Reye*, Lehrsätze über lineare Mannigfaltikeiten projectiver Kugelbüschel, Kugelbündel und Kugelbüsche. — *Niels Nielsen*, Sur une classe de polynômes qui se présentent dans la théorie des functions cylindriques. — *Ciani*, Contributo alla teoria del gruppo di 168 collineazioni piane. — *Hermite*, Extrait de quelques lettres de M. Ch. Hermite à M. S. Pincherle. — *Pirondini*, Risoluzione di due questioni geometriche.

Rendiconti del Circolo matematico di Palermo.

Tomo XIV (1900), fasc. 3° e 4°. — *Gerbaldi*, Sul gruppo semplice di 360 collineazioni piane. Parte II (continuaz.). — *Bucca*, Studii di analisi: I. Sullo sviluppo degli integrali di un'equazione differenziale lineare omogenea nell'intorno di un punto singolare. - II. Sulla riduzione del gruppo di Galois d'una equazione algebrica coll'aggiunzione di irrazionalità arbitrarie. - III. Sulle espressioni algebriche costruibili geometricamente colle sole coniche o con curve d'ordine superiore al secondo. - IV. Sulla irrazionalità icosaedrica. - V. Sulla reduttibilità delle equazioni binomie. — *Pincherle*, Sopra un problema d'interpolazione. — *Vivanti*, Sulla trasformazione di Laplace. — *Severini*, Sulla rappresentazione delle funzioni reali di variabili reali mediante serie di polinomi razionali interi. — *Burgatti*, Teoria dei sistemi articolati più semplici.

Fasc. 5°. — *Burgatti*, Teoria dei sistemi ecc. (continuaz. e fine). — *Vitali*, Sulle funzioni analitiche sopra le superficie di Riemann. — *Id.*, Sui limiti per $n=\infty$ delle derivate n^{esime} delle funzioni analitiche. — *Mittag-Leffler*, Sur la représentation analytique des functions d'une variable réelle. (Extrait d'une lettre a M. E. Picard.) — *Puglisi*, Sulle formule per la composizione di più movimenti finiti. — *Phragmèn*, Sur la représentation analytique de fonctions reélles, données sur un ensemble quelconque de points. (Extrait d'une lettre à M. G. B. Guccia.) — *Beltrami*, Commem. di Francesco Brioschi. (Dagli Atti della R. Acc. dei Lincei.) — *Cremona*, Commem. di Eugenio Beltrami. (Dagli Atti della R. Acc. dei Lincei.)

Il Bollettino di matematiche e di scienze fisiche e naturali diretto da *A. Conti.*

Fasc. 15-16. — *Ferrari*, Lunghezza, area, volume. — *Sforza*, Sopra una dimostrazione del principio di De Zolt relativamente all'equivalenza dei prismi. — *Scoto*, Rivista storica. — *Ciamberlini*, Didattica per le Scuole elementari. — Rivista bibliografica. — Cronaca: Nuovi programmi di matematica per la Scuola Complementare e per le Scuole Normali.

Fasc. 17-18-19-20. — *Del Pezzo, Gerbaldi, Guccia*, Perizia per la contraffazione di un'aritmetica. — *Conti*, Forme da evitarsi nell'insegnamento dell'Aritmetica e della Geometria (continuaz.) — *Cercignani*, Notizie storiche sulla misura del tempo. — *Dal Bo*, Per gli esercizi di applicazione del teorema di Pitagora. — *Magli*, Osservazioni intorno a una regola d'aritmetica elementare. — *Ciamberlini*, Gli esercizi di calcolo *semimentale*. — *Id.*, Un'osservazione sulla lettura delle misure del sistema metrico decimale. — *Scoto*, Rivista storica (continuaz.). — *Ciamberlini*, Didattica per le Scuole elementari. — Rivista bibliografica. — Cronaca.

Fasc. 21-22. — *Vanni*, Alcuni teoremi sulle proporzioni numeriche. — *Buzzi*, La genesi del calcolo numerale attraverso l'evoluzione (continuaz.). — *Genovesi*, La moltiplicazione con un fattore zero. — *Ciamberlini*, Didattica per le Scuole elementari. — Rivista bibliografica.

Fasc. 23-24. — *Nannei*, Alcuni teoremi sulle proporzioni numeriche (continuaz. e fine). — *Buzzi*, La Genesi del calcolo ecc. — *Ciamberlini*, Su alcuni problemi proposti ordinariamente come applicazione della teoria delle frazioni ordinarie. — Rivista bibliografica. — Corrispondenze.

I NUOVI PROGRAMMI DI MATEMATICA, CHIMICA E FISICA

NEI GINNASI E NEI LICEI

Da oltre trent'anni eravamo abituati a vedere i programmi di geometria nel Ginnasio e nel Liceo ridotti alla distribuzione dei libri di Euclide fra i vari corsi. Finalmente coi nuovi, pubblicati nel Bollettino della P. Istruzione del 15 nov. scorso, si è abbandonato questo brutto sistema, e si è adottata una divisione logica ed organica dei vari rami della matematica, indipendente dal vecchio codice Euclideo, e tenendo conto del sussidio che questa scienza deve dare allo studio della fisica.

Si potrà trovare a ridire su qualche particolare, ma complessivamente questi nuovi programmi sono un lavoro coscienzioso, maturamente ponderato, e degno dei maggiori encomi.

Non intendo qui di esaminarli partitamente, ma mi preme soltanto rilevare una cosa notevole e assolutamente nuova nel nostro paese.

Essi sono fatti accogliendo ed armonizzando le proposte degl'insegnanti di tutta Italia, tanto che possono dirsi il frutto della pratica, dell'esperienza di tutti; e con ciò non credo diminuire, ma anzi accrescere il merito degli egregi compilatori dei medesimi.

La pubblicazione di questi programmi è una bella vittoria della nostra Associazione " Mathesis „ e della Società italiana di Fisica, che, come è detto nella relazione, si *fecero organi autorevoli* delle osservazioni e dei desideri dalla maggioranza degl'insegnanti.

L'opera assidua compiuta dall'Associazione " Mathesis „ in quattro anni, le discussioni avvenute in varie città d'Italia, e specialmente nel congresso di Torino del 1898, hanno dunque recato un utile vero alla scuola; ed è da sperarsi che dopo quest'esempio tutti si persuadano della verità del vecchio proverbio l'*unione fa la forza*, e vogliano prender parte attiva ai lavori dell'Associazione, ed in particolare a quelli del secondo congresso, che, per iniziativa della medesima, avrà luogo a Livorno nella seconda quindicina del prossimo agosto.

Non posso infine tacere della soddisfazione che provo come vecchio e convinto fautore della fusione della geometria piana e solida.

Nella prima seduta del Congresso di Torino (9 settembre 1898) fu votato ad unanimità, meno un'astensione, il seguente ordine del giorno:

" È conveniente modificare possibilmente i programmi in modo che sia concessa " agl'insegnanti la libertà di scegliere fra il metodo separatista ed il fusionista „.

I nuovi programmi hanno resa possibile la libertà di scelta desiderata, esplicitamente ammessa nel n. 8 delle istruzioni, che è il seguente:

" Nella prima classe del Liceo v'è parte di geometria solida e parte di geo" metria piana. L'insegnante potrà svolgerle in quell'ordine che stimerà migliore „.

" Lo stesso è a dirsi del programma della seconda classe, che si chiude col " trattato della misura „.

Ma vi è di più. Nel n. 4 delle istruzioni medesime è detto: " l'insegnante " non mancherà di far notare agli allievi le analogie e le differenze, che passano " tra alcuni enti, a mano a mano che se ne svelano le proprietà, come, nella " geometria, tra la retta punteggiata, il fascio di raggi e gli archi di una circonfe" renza, tra i triangoli e i triedri, ecc. „ E questa, mi sembra, è fusione bella e buona.

D'altronde, dovendo fare in uno stesso anno argomenti affini di geometria piana e solida, anche i più ostinati antifusionisti si accorgeranno ben presto dell'utilità della fusione.

G. Lazzeri.

Giulio Lazzeri — *Direttore-responsabile*

Finito di stampare il 15 dicembre 1900.

MEMORIA BIBLIOGRAFICA
SULL' ULTIMO TEOREMA DI FERMAT

§ I.

Preliminari.

1. Ecco l'ultimo teorema di Pietro Fermat: (*)

" *Cubum in duos cubos, aut quadrato-quadratum in duos quadrato-quadratos et generaliter nullum in infinitum, ultra quadratum, potestatem in duos ejusdem nominis fas est dividere* ".

2. Principale scopo della presente memoria è di mettere sotto gli occhi degli studiosi delle discipline matematiche tutte le note e le memorie riguardanti un tal teorema, che hanno fin qui veduto la luce, e tra le quali una dimostrazione generale del prof. Calzolari di Ferrara; a proposito della quale però mi sorge il dubbio, che qualche inesattezza debba infirmarne la validità.

Questi lavori presentati direi quasi come in un quadro, chi sa che non facciano invogliare gli odierni matematici a riprendere dalle fondamenta tale questione, che ha per sì lungo ordine di anni affaticato indarno tante menti; e chi sa che essi più fortunati dei loro predecessori non riescano finalmente a darne una dimostrazione generale ed esauriente, tenuto anche conto degl'immensi progressi fatti in questi ultimi anni dalla matematica in ogni suo ramo; nello stesso modo che il Lindemann ha potuto mostrare la trascendenza di π. Io nutro ferma speranza che essi vinceranno anche questa battaglia e solo questa speranza e l'amore grande, che ho per la scienza, mi han consigliato a pubblicare la presente memoria.

3. Eulero, il Lejeune-Dirichlet, il Legendre, il Lamé, il Kummer, come vedremo in seguito, diedero la dimostrazione dell'ultimo teorema di Fermat per casi particolari, coll'intendimento forse, che, proseguendo nella via su cui si erano messi, sarebbero giunti a dimostrarlo nel caso generale; ma le loro dimostrazioni son troppo complicate ed artifiziose, e questa forse è l'unica ragione per cui gli autori di esse, ad onta del loro altissimo ingegno, non sono riusciti nello intento, che si eran prefisso. E tanto più queste dimostrazioni appaiono complicate ed artifiziose, quando si confrontano con alcune di quelle date dal Fermat, che furon per caso rinvenute in seguito, e che risplendono per chiarezza, per semplicità, per brevità e per eleganza; ed il Fermat stesso asserisce di aver trovato del suo ultimo teorema una dimostrazione molto elegante ed ammirabile.

(*) Vedi Diophanti Alexandrini Arithmeticorum Libri, sex, Tolosa 1670, Observatio Domini Petri de Fermat, pag. 61.

Probabilmente i matematici a lui posteriori non hanno fin qui battuto buona strada; e colla loro fantasia ingigantendo le difficoltà della dimostrazione, hanno voluto escogitare metodi assai difficili e complicati, i quali invece di condurli alla dimostrazione desiderata, li hanno sempre più allontanati da essa. E questa mia opinione viene in certo qual modo suffragata anche dal Legendre, il quale nella IV parte § VII, pag. 386 del suo " Essai sur la théorie des nombres ", a proposito della dimostrazione data da lui del teorema " Sulla reciprocità fra due numeri primi qualunque " così si esprime: " In tal guisa abbiamo dimostrato un teorema che si può riguardare come il più importante della teoria dei numeri e che sotto varie forme ha presentato difficoltà quasi insuperabili a chi voleva dimostrarlo seguendo altre vie. La dimostrazione che ne diamo, dopo Federico Gauss, è tanto più importante in quanto, che essa è fondata su principii elementarissimi e non occorre premettere ad essa teoria alcuna. Chi sa quanti teoremi come questo, reputati difficilissimi nella scienza de' numeri, non si possano dimostrare assai facilmente; e vi è sempre da sperare che si trovino dimostrazioni assai semplici anche per quelli, che sono stati fino ad ora dimostrati con metodi lunghi e complicati ".

4. Ognun sa con quale immenso successo il Fermat abbia coltivato la scienza de' numeri, in cui egli additò nuovi orizzonti e tracciò nuove vie; disgraziatamente però egli ha tramandato ai posteri senza dimostrazione un gran numero di teoremi interessantissimi, e le poche che rimangono fanno viepiù rimpiangere quelle che mancano e quelle che pur troppo sono andate perdute. Infatti dal seguente passo di una delle sue note su Diophanto pag. 187. (Vedi " Essai sur la théorie des nombres " del Legendre. Parte II, § IV, pag. 183.) " Imo propositionem pulcherrimam et maxime generalem nos primi deteximus. Nempe omnem numerum vel esse triangulum vel ex duobus aut tribus triangulis compositum, esse quadratum vel ex duobus aut tribus quadratis compositum; esse pentagonum vel ex duobus, tribus, quatuor aut quinque pentagonis compositum et sic deinceps in infinitum in hexagonis, heptagonis et polygonis quibuslibet, enuntianda videlicet pro numero angulorum generali et mirabili propositione. Eius autem demonstrationem quae ex multis variis et abstrusissimis numerorum mysteriis derivatur hic apponere non licet, opus enim et librum integrum huic operi destinare decrevimus et Arithmeticen hoc in parte ultra veteres et notos terminos mirum in modum promovere " risulta ben chiaramente che il Fermat stava scrivendo una grande opera, la quale come egli stesso asserisce doveva contenere molte e belle proprietà sui numeri; e, come giustamente dice il Legendre, i geometri dovranno ben dolersi per lungo tempo che questo illustre scienziato non abbia potuto condurre a compimento il suo disegno e che i suoi congiunti od amici, divenuti depositari dei suoi manoscritti, non li abbiano fatti conoscere al pubblico. In essi certamente si sarebbero trovati, oltre le dimostrazioni ancora ignorate di parecchi de' suoi teoremi, metodi degni della sagacia dell'autore, i quali accoppiati alle scoperte posteriori avrebbero di molto contribuito a perfezionare quella parte difficilissima delle discipline matematiche, che è la teoria dei numeri. Però è certo che anche il Fermat stesso, come parecchi matematici a lui contemporanei, molte volte si compiaceva di enunciare teoremi, che in gran parte egli aveva sicuramente prima dimostrati, senza renderne note le dimostrazioni trovate, come ad esempio questo. " Il numero $2^{31} - 1 = 2.147.483.647$ è un numero primo "; teorema che fu in appresso dimostrato dall'Eulero (Mém. de Berlin an. 1772, pag. 36). E come risulta anche dalla lettera seguente al padre Mersenne: " Vous demandez si le nombre 100. 895. 598. 169 est premier ou non, et une méthode pour découvrir dans l'espace d'un jour, s'il est premier ou composé. A cette

question, je réponds que ce nombre est composé et se fait du produit de ces deux: 898.423 e 112.303 qui sont premiers. Je suis toujours, mon révérend Père, votre très-humble et très-affectionné serviteur. FERMAT „.

Qui sorge spontanea la domanda: Quali le ragioni di questo fatto? Innanzi tutto ne abbiamo una nello spirito di que'tempi, in cui gli scienziati si proponevano a vicenda questioni da risolvere; ma il più delle volte essi nascondevano, invece di farli conoscere, i loro metodi, per riserbarsi nuovi trionfi in avvenire; ed a questo si aggiunga anche lo spirito di nazione; imperocchè vi era in quell'epoca una grande rivalità, sovrattutto fra i geometri di Francia e quelli d'Inghilterra. Potrebbe però anche darsi che il Fermat medesimo, riandando in seguito la dimostrazione del suo teorema, l'abbia trovata insufficiente od in qualche parte imperfetta. Ciò non deve punto recar meraviglia, quando si rifletta che anche la dimostrazione del teorema seguente: (*) Il sistema indeterminato di equazioni: $2y^2 - 1 = x$, $2z^2 - 1 = x^2$ ammette le sole due soluzioni:

1ª $\quad x = y = z = 1, \qquad$ 2ª $\quad x = 7, \quad y = 2, \quad z = 5,$

(dimostrazione che il Fermat ha inviato in una sua lettera al Frenicle) (**) non si è potuta rinvenire, perchè forse fu trovata insufficiente dal Frenicle stesso, non parendomi ammissibile che questi l'abbia, in caso contrario, tenuta nascosta; e quando per di più si pensi che talvolta il Fermat stesso cadde in errore, come ad esempio in questo teorema: " La formola $2^{2^n} + 1$ dà sempre numeri primi „; giacchè ognuno sa che Eulero dimostrò poi essere $2^{2^5} + 1 = 641 \times 6.700.417$.

§ II.

1. In questo paragrafo della presente memoria faccio conoscere alcuni miei risultati in parte nuovi ed in parte, benchè noti, ottenuti con metodi diversi ed assai più semplici di quelli seguiti dal Calzolari e da altri. Innanzi tutto espongo alcune considerazioni generali sull'equazione $x^n + y^n = z^n$; indi dimostro che " la differenza dei biquadrati di due numeri interi ed ineguali non è mai eguale al quadrato di un numero intero „ il qual teorema mi servirà per dimostrare quello di Fermat nel caso di $n = 4$; poi risolvo l'equazione $x^2 + y^2 = z^2$, esponendo indi le importanti proprietà dei numeri x, y, z che la verificano. Al § X poi dimostro l'impossibilità dell'equazione $x^5 + y^5 + z^5 = 0$ in numeri interi.

Per brevità, secondo la logica matematica, un numero intero positivo e diverso dallo zero lo indico con N_1; un numero intero e positivo che può essere anche zero lo indico con N_0; ed un multiplo di un N_1 qualunque a lo indico con $N_1 a$ o $a . N_1$, ed un numero primo con N_p. Il numero n significherà sempre un N_1.

2. Considerazioni generali sull'equazione $x^n + y^n = z^n$.

a) TEOREMA. — *Ammesso vero il teorema di Fermat per gli* N_1, *esso è vero anche per numeri fratti.*

(*) Vedi gli *Atti dell'Accademia pontificia dei nuovi Lincei*, Tomo XXXVI, Anno XXXVI, 1883 nota " sur un théorème de Fermat „ di M. TH. PEPIN.

(**) Vedi " Recherches sur les manoscrits de Fermat „ par M. HENRY, pubblicate nel *Bollettino di bibliografia e di storia delle scienze matematiche e fisiche* di B. Boncompagni, Tomo XXI, Roma, Luglio, Agosto, Settembre, Ottobre, 1879.

DIMOSTRAZIONE. — Infatti, se è possibile, poniamo che si abbia

$$(1) \qquad \left(\frac{a}{b}\right)^n + \left(\frac{c}{d}\right)^n = \left(\frac{e}{f}\right)^n,$$

ove a, b, c, d, e, f sono degli N_1; da essa si ha

$$(2) \qquad (adf)^n + (bef)^n = (bde)^n,$$

la quale pel teorema di Fermat non può verificarsi; dunque anche la (1) non può verificarsi ecc.

b) TEOREMA. (*) — *La somma delle potenze* n^{esime} *di due* N_p *non è mai eguale alla potenza* n^{esima} *di un* N_p, *se è* $n > 1$.

DIMOSTRAZIONE 1^a. — Sia $x < y < z$, dalla quale si vede che z supera x di non meno di 2; ora poniamo: $u = z - x$; allora dall'equazione $x^n + y^n = z^n$ si ha

$$y^n = (x+u)^n - x^n = n \, . \, u \, . \, x^{n-1} + \binom{n}{2} u^2 x^{n-2} + \ldots + u^n;$$

d'onde si ha che y^n è un $N_1 u$; ma y è per ipotesi un N_p; dunque essendo per ipotesi $u \geq 2$, ne consegue che u è uguale ad y o ad una sua potenza; se fosse $u = y$ si avrebbe: $x^n + y^n = (x+y)^n$, che è assurda; quindi deve essere $u < y$; dunque a fortiori è $u < y^s$, ove s è un N_1; ma y non ammette nessun divisore minore di esso; dunque ecc.

2^a. — Sia $x < y < z$; sarà $z - x \geq 2$; ora abbiamo

$$z^n - x^n = y^n:$$

e quindi y^n è divisibile per $z - x$; e perciò lo è y; poichè non può essere $z - x = y$, nè $z - x = 1$, perchè ciò sarebbe contro l'ipotesi; dunque ecc.

COROLLARIO. — *Se l'equazione* (1) $x^n + y^n = z^n$ *è soddisfatta in* N_1 *(se il valore di* $n > 1$ *permette che lo sia) il maggiore dei due numeri* x *ed* y, *è un numero composto, qualunque sia* x, *semplice o composto.*

c) TEOREMA. — *Allorchè l'equazione* (1) $x^n + y^n = z^n$ *è soddisfatta in* N_1 *(se il valore di* $n > 1$ *permette che lo sia):*

1^o *se* x *è un* N_p, *i due numeri* z *ed* y *differiscono tra loro di* 1;

2^o *se* y, *che è maggiore di* x, *è un* N_p, *l'equazione* (1) *non è soddisfatta in* N_1.

DIMOSTRAZIONE 1^a. — Si ponga $z = x + u = y + v$; si ha $x^n + y^n = (x+u)^n = (y+v)^n$; d'onde:

$$y^n = N_1 u, \qquad x^n = N_1 v;$$

ma x è un N_p, ed essendo $n > 1$, ne consegue che deve essere $v = 1$ e quindi $z - y = 1$.

2^a. — Si ha $z - x \geq 2$ e $z^n - x^n = y^n$; dalla quale si vede che y è divisibile per $z - x$; il che è assurdo; dunque ecc.

d) TEOREMA. — *Se l'esponente* n *dell'equazione* (1) $x^n + y^n = z^n$ *è un* $N_1 2 + 1$; *o se è un* $N_1 2$, *contenga almeno un fattore* $N_1 2 + 1$; *e si ammette che la* (1) *possa, se è possibile, essere soddisfatta in* N_1 *per* $n > 1$, *io dico che* z *non può essere un* N_p.

DIMOSTRAZIONE. — Supponiamo, se è possibile, che z sia un N_p; allora sapendosi che $x^n + y^n$ è divisibile per $x^{2^s} + y^{2^s}$, ove s può assumere i valori $0, 1, 2, 3, 4 \ldots$, ne viene che è $z = x^{2^s} + y^{2^s}$, il che è assurdo, essendo $z < x + y$; dunque ecc.

(*) Vedi negli *Atti dell'Accademia pontificia* ecc. t. XXXVII la nota „Sur le dernier théorème de Fermat par M. DE JONQUIÈRE, 1884 „.

e) Teorema. — *Supponiamo che l'esponente* n *della* (1) $x^n + y^n = z^n$ *sia un* $N_1 2 + 1$, *o se è un* $N_1 2$, *contenga almeno un fattore* $N_1 2 + 1$, *e supponiamo* $x < y < z$ *ed* x *sia un* N_p; *io dico che la* (1) *non può sussistere.*

Dimostrazione. — Infatti pel teorema *c)* si sa che è $z = y + 1$ e pel teorema *d)* si sa che z è un numero composto e divisibile per $x^{2^s} + y^{2^s}$, ove s può assumere i valori $0, 1, 2, 3 \ldots$; ma essendo $x \neq 1$, ne consegue che è sempre $x^{2^s} + y^{2^s} > y + 1$; quindi z non può essere divisibile per $x^{2^s} + y^{2^s}$; dunque ecc.

f) Teorema. — *Ammesso, se è possibile, che l'equazione* $x^n + y^n = z^n$ *per* $n > 1$ *possa esser soddisfatta in* N_1 *ed* x *ed* y *siano degli* N_1 *composti ed* n *sia un* $N_1 2 + 1$; *e se è un* $N_1 2$, *contenga almeno un divisore* $N_1 2 + 1$, *anche* z *è un* N_1 *composto.*

Dimostrazione. — Supponiamo, se è possibile, che z sia un N_p, dall'equazione $x^n + y^n = z^n$ si vede che z^n, e quindi z, è divisibile per $x^{2^s} + y^{2^s}$, ove s può prendere i valori $0, 1, 2, 3 \ldots$; e quindi dovrà essere $z = x^{2^s} + y^{2^s}$; ma si sa che è $z < x + y$; dunque z non può essere un N_p; perciò ecc.

g) Sia n un Np maggiore di 2, e sia $D(x, y) = 1$; poichè è

(1) $$x^n + y^n = (x + y)(x^{n-1} - x^{n-2}y + x^{n-3}y^2 - \ldots + y^{n-1}) = z^n,$$

sarà

$$D(x + y,\ x^{n-1} - x^{n-2}y + \ldots + y^{n-1}) = 1;$$

allora, posto

(2) $$x + y = a^\alpha b^\beta c^\gamma,$$

ove a, b, c sono degli N_1, deve essere

(3) $$z = a^{\alpha'} b^{\beta'} c^{\gamma'} \cdot z_1;$$

ed allora dalla (1), (2), (3), si deduce

(4) $$a^\alpha b^\beta c^\gamma = a^{n\alpha'} b^{n\beta'} c^{n\gamma'},$$

e

(5) $$x^{n-1} - x^{n-2}y + \ldots + y^{n-1} = z_1^n,$$

dalla (4) si ha

$$\frac{\alpha}{\alpha'} = \frac{\beta}{\beta'} = \frac{\gamma}{\gamma'} = n.$$

E allora abbiamo

$$x^{n-1} - x^{n-2}y + \ldots + y^{n-1} = z_1^n.$$

h) Ammesso vero il teorema di Fermat, ne consegue dal *g)* che i sistemi di equazioni della forma:

$$\begin{cases} x^n - x^{n-1}y + x^{n-2}y^2 - \ldots + y^n = z^{n+1} \\ \qquad\qquad x + y = u^{n+1}, \end{cases}$$

ove n è un N_p maggiore od eguale a 2, sono impossibili in N_1.

3. Risoluzione delle equazioni $x^4 - y^4 = z^2$ e $x^4 + y^4 = z^4$.

a) Teorema. — *L'equazione*: (1) $x^4 - y^4 = z^2$ *è impossibile in* N_1.

Dimostrazione. — Se la (1) è possibile in N_1, possiamo raggruppare tutte quelle soluzioni, in cui il prodotto xyz delle tre indeterminate ha lo stesso valore; è evidente che fra questi diversi gruppi ve ne ha uno, pel quale xyz ha il minimo valore possibile, senza essere nullo; suppongo che la soluzione considerata (x, y, z) appartenga a questo gruppo; e dimostrerò che si può sempre ottenere un'altra soluzione formata di tre numeri, il cui prodotto senza annullarsi, è minore del minimo prodotto xyz; questa conseguenza, a cui si arriva è assurda; dunque se ne inferisce che la (1) è impossibile in N_1. Dalla (1) si vede che, siccome i tre numeri x, y, z si possono supporre primi tra loro, due debbono essere degli $N_1 2 + 1$, ed uno di questi sicuramente è x. Infatti se x fosse un $N_1 2$, allora y e z sarebbero degli $N_1 2 + 1$; e dalla (1) si avrebbe $x^4 = z^2 + y^4$, la quale si mostra subito che è assurda, poichè essendo

$$x^4 = N_1 4; \qquad z^2 = N_1 4 + 1, \qquad y^4 = N_1 4 + 1$$

e quindi

$$N_1 4 = N_1 4 + 1 + N_1 4 + 1,$$

ne viene

$$N_1 2 = N_1 2 + 1,$$

che è assurda. Dunque x è un $N_1 2 + 1$; ma y può essere un $N_1 2$ o un $N_1 2 + 1$; consideriamo separatamente questi due casi.

1° Caso y è $N_1 2$.

Poniamo $y = 2\alpha . \beta$, ove α e β sono degli N_1; dalla (1) ho

$$x^2 \pm z = 2\alpha^4; \qquad x^2 \mp z = 8\beta^4; \quad \text{e quindi:} \quad x^2 = \alpha^4 + 4\beta^4;$$

dall'ultima ricavo

$$x^2 - \alpha^4 = (x + \alpha^2)(x - \alpha^2) = 4\beta^4;$$

ora ponendo $\beta = \delta . \gamma$, ove δ e γ sono degli N_1, si ha

$$x + \alpha^2 = 2\delta^4, \qquad x - \alpha^2 = 2\gamma^4;$$

e quindi $\alpha^2 = \delta^4 - \gamma^4$. In questo caso si avrà una seconda soluzione della (1) in δ, γ, α, il cui prodotto non solo è minore di xyz, ma anche di y.

2° Caso y è $N_1 2 + 1$.

In questo caso z è un $N_1 2$; poniamo $z = 2\alpha\beta$, ove α, β, sono degli N_1, si ha

$$x^2 + y^2 = 2\alpha^2, \qquad x^2 - y^2 = 2\beta^2;$$

d'onde

$$x^2 = \alpha^2 + \beta^2; \qquad y^2 = \alpha^2 - \beta^2; \qquad (xy)^2 = \alpha^4 - \beta^4;$$

e così la (1) sarà verificata da α, β, (xy), il cui prodotto $\alpha . \beta . (xy) = \frac{1}{2} xyz$, essendo $xyz = 2\alpha\beta\,(xy)$.

Da quanto precede si vede che supponendo y un $N_1 2$ o un $N_1 2 + 1$, si arriva all'assurdo, che la (1) sarebbe verificata da tre N_1, il cui prodotto sarebbe minore del minimo prodotto xyz; onde se ne inferisce che la (1) non ammette soluzione in N_1.

a) Teorema. — *L'equazione:* (1) $x^4 + y^4 = z^4$ *è impossibile in* N_1.

Dimostrazione 1ª. — Dalla (1) ho: $z^4 - y^4 = (x^2)^2$, la quale pel teorema *a)* è impossibile in N_1; dunque ecc.

2ª. — La (1) si può scrivere così

$$(2) \qquad (x^2)^2 + (y^2)^2 = (z^2)^2,$$

la quale, come può verificarsi, è soddisfatta da

$$(3) \qquad x^2 = p^2 - q^2, \qquad y^2 = 2pq, \qquad z^2 = p^2 + q^2;$$

da cui si ha moltiplicando la 1ª e la 3ª di queste fra loro: $p^4 - q^4 = (xz)^2$, la quale pel teorema *a)* si sa che è impossibile in N_1; dunque ecc.

Osservazione. — Ne consegue che l'equazione $x^2 + y^2 = z^2$ non può essere soddisfatta da tre $N_1{}^2$.

Corollario 1°. — *L'equazione:* $x^{2^n} + y^{2^n} = z^{2^n}$ *non può essere soddisfatta in* N_1; *perchè la si può scrivere così*

$$(x^{2^{n-2}})^4 + (y^{2^{n-2}})^4 = (z^{2^{n-2}})^4,$$

la quale, come si sa, non può essere soddisfatta in N_1.

2°. — *Per questo teorema e pel teorema* f) *del n. 2, possiamo ora asserire in generale che " se l'equazione* $x^n + y^n = z^n$, *è possibile di essere soddisfatta in* N_1 *per l'esponente* $n > 1$, *se* x *ed* y *sono degli* N_1 *composti, anche* z *è un* N_1 *composto ".*

4. Risoluzione dell'equazione pitagorica (1) $x^2 + y^2 = z^2$, e proprietà dei numeri x, y, z.

a) Teorema. — *Ponendo* (2) $z = x + u = y + v$; *far vedere che* x *ed* y *si scambiano fra loro, scambiando fra loro* u *e* v, *e che* z, $x + y = z$ *sono funzioni simmetriche di* u *e* v.

Dimostrazione. — Dalle (1) e (2) si ha:

$$z^2 - 2(u + v)z + (u^2 + v^2) = 0, \tag{3}$$

la quale rimane invariata scambiando u con v, cioè i valori di z sono funzioni simmetriche di u e v. Nelle (2) scambiando u con v e viceversa, la x si scambia con y e viceversa; ne consegue che anche $x + y - z$ è funzione simmetrica di u e v.

b) Teorema. — *Se* u *e* v *hanno un fattor comune, l'hanno pure* x, y, z, *e reciprocamente.*

Dimostrazione 1ª. — Si ha: (1) $z^2 - 2(u + v)z + (u^2 + v^2) = 0$; se u e v hanno a divisore comune d, ove d è un N_1, la $(u^2 + v^2)$ avrà a divisore comune d^2; onde dalla (1) si vede che z deve essere divisibile per d; ora essendo $x = z - u$, $y = z - v$, ne consegue che anche x ed y ammettono il divisore d.

2ª. — Se x, y hanno il divisor comune d, l'avranno pure z, u, v.

Infatti dall'equazione $x^2 + y^2 = z^2$ si vede che z ammette il divisore d; ora essendo $u = z - x$, $v = z - y$, ne viene che u e v sono divisibili per d.

Corollario. — *Se* u *e* v *sono primi fra loro, sono pure primi due a due fra loro* x, y, z; *e reciprocamente se* x *ed* y *sono primi fra loro, tali sono due a due fra loro* z, u, v.

Osservazione. — Si possono combinare nelle ipotesi due a due fra loro x, y, z, u, v, e si hanno altrettanti teoremi analoghi ai precedenti.

c) Teorema. — *L'equazione* (1) $x^2 + y^2 = z^2$ *è soddisfatta da*

$$z = u + v + w, \qquad x = v + w, \qquad y = u + w, \tag{2}$$

ove w *è* $N_1 2$ *e funzione simmetrica di* u *e* v.

Dimostrazione. — Dalla (1) si ha

$$z^2 - x^2 - y^2 = z^2 - x(z - u) - y(z - v) = 0;$$

d'onde

$$z - x - y + \frac{ux + vy}{z} = 0; \tag{3}$$

d'onde se ne inferisce che $ux + vy$ è divisibile per z e questo quoto è un $N_1 2$ e funzione simmetrica di u e v come $x + y - z$. Poniamo: (4) $\frac{ux + vy}{z} = w$; allora la (3) diviene: (5) $z - x - y + w = 0$; avendosi (6) $u = z - x$, $v = z - y$, e combinando le (5), (6) si hanno le (2).

OSSERVAZIONE 1ª. — Se nella $z^2 - x^2 - y^2 = 0$ si fa:

1°. $\quad z = x + u, \quad y = x + u - v;$

2°. $\quad z = y + v, \quad x = y - u + v,$

in uno dei due fattori eguali che formano $z \,.\, z$, $y \,.\, y$, $x \,.\, x$, e poi si dividono le equazioni così ottenute rispettivamente per x ed y, e si ottiene

$$z - x - y + \frac{uz + (v - u)\,y}{x} = 0,$$
$$z - x - y + \frac{vz + (u - v)\,x}{y} = 0;$$

e quindi da quanto si è veduto più sopra si ha:

$$\frac{ux + vy}{z} = \frac{uz + (v - u)\,y}{x} = \frac{vz + (u - v)\,x}{y} = w.$$

OSSERVAZIONE 2ª. — L'ammettere che sia possibile di risolvere in N_1 l'equazione (1), equivale ad ammettere la possibilità di poter determinare un $N_1 2$, che si è indicato con w, funzione simmetrica di u e v, tale che aggiunta ad $u + v$, a v e ad u dia rispettivamente i tre numeri z, x, y, che verificano l'equazione (1).

d) TEOREMA. — *Se l'equazione* (1) $x^2 + y^2 = z^2$ *è soddisfatta in* N_1, *le espressioni*

$$(2) \qquad \frac{u^2 + v^2}{z}, \quad \frac{u^2 - (v - u)^2}{x}, \quad \frac{v^2 - (v - u)^2}{y}$$

debbono essere degli N_1; *in altri termini* w *va determinato in modo, che* z, x, y *siano divisori rispettivamente di* $u^2 + v^2$, $u^2 - (v - u)^2$, $v^2 - (v - u)^2$.

DIMOSTRAZIONE. — Dall'equazione (3) $z^2 - 2(u + v)\,z + (u^2 + v^2) = 0$ dividendola per z si vede che $\frac{u^2 + v^2}{z}$ è un N_1. Essendo $z = x + u$; dalla (3) ho: (4) $x^2 - 2vx + (v - u)^2 - u^2 = 0$; dividendola per x si vede che $\frac{u^2 - (v - u)^2}{x}$ è un N_1. Analogamente facendo nella (3) $z = y + v$ ed operando come precedentemente, si vede che $\frac{v^2 - (v - u)^2}{y}$ è un N_1.

OSSERVAZIONE. — Facendo nelle espressioni

$$\frac{ux + vy}{z}, \; \frac{uz + (v - u)\,y}{x}, \; \frac{vz - (u - v)\,x}{y}$$

rispettivamente

$$x = z - u,\; y = z - v;\; z = x + u,\; y = x + u - v;\; z = y + v,\; x = y + v - u$$

si ottiene

$$\frac{ux + vy}{z} = u + v - \frac{u^2 + v^2}{z}; \quad \frac{uz + (v - u)\,y}{x} = v + \frac{u^2 - (v - u)^2}{x}$$

e

$$\frac{vz + (u - v)\,x}{y} = u + \frac{v^2 - (v - u)^2}{y};$$

sapendosi che

$$\frac{u^2 + v^2}{z}, \; \frac{u^2 - (v - u)^2}{x}, \; \frac{v^2 - (v - u)^2}{y}$$

sono degli N_1, ne consegue che anche le espressioni

$$\frac{ux + vy}{z}, \; \frac{uz + (v - u)\,y}{x}, \; \frac{vz + (u - v)\,x}{y}$$

sono degli N_1, i quali si è veduto (vedi Teor. *c)* Oss. 1ª) che son tutti eguali a w; e reciprocamente se ne dedurrebbe

$$\frac{u^2+v^2}{z}=u+v-w;\ \frac{u^2-(v-u)^2}{x}=-v+w;\ \frac{v^2-(v-u)^2}{y}=-u+w.$$

Il numero w lo chiameremo il *criterio di possibilità* dell'equazione (1), poichè dalla determinazione di w dipende precisamente la determinazione delle terne degli N_1, che soddisfano la (1).

e) TEOREMA. — *Per risolvere in* N_1 *l'equazione* (1) $x^2+y^2=z^2$ *la condizione* necessaria *e* sufficiente *è che il prodotto* $2uv$ *sia eguale al quadrato pari* w^2, *ossia abbiasi* (2) $w^2=2uv$, *per cui i numeri intieri* z, x, y *saranno dati da:*

$$(3)\qquad z=u+v+\sqrt{2uv},\qquad y=u+\sqrt{2uv},\qquad x=v+\sqrt{2uv}.$$

DIMOSTRAZIONE. — 1°. La condizione (2) è necessaria; infatti facendo nella (1)

$$z=u+v+w,\ y=u+w,\ x=v+w,$$

si ottiene la (2).

2°. La condizione (2) è sufficiente, poichè non solo la (1) è soddisfatta dalle (3); ma sono soddisfatte anche le condizioni richieste dal teorema 3; infatti si ha

$$(3)\qquad \begin{cases} \dfrac{u^2+v^2}{z}=\dfrac{(u+v+\sqrt{2uv})(u+v-\sqrt{2uv})}{u+v+w}; \\[2mm] \dfrac{u^2-(v-u)^2}{x}=-\dfrac{v^2-2uv}{x}=-\dfrac{(v+\sqrt{2uv})(v-\sqrt{2uv})}{v+w}; \\[2mm] \dfrac{v^2-(v-u)^2}{y}=-\dfrac{u^2-2uv}{y}=-\dfrac{(u+\sqrt{2uv})(u-\sqrt{2uv})}{u+w}; \end{cases}$$

ora ponendo $w=\sqrt{2uv}$, i primi membri delle (3) sono degli N_1, purchè bene inteso $2uv$ sia un quadrato pari, e così abbiamo

$$(4)\qquad \frac{u^2+v^2}{z}=u+v-\sqrt{2uv};\ \frac{u^2-(v-u)^2}{x}=-v+\sqrt{2uv};$$
$$\frac{v^2-(v-u)^2}{y}=-u+\sqrt{2uv}.$$

OSSERVAZIONE. — Sicchè abbiamo

$$\frac{ux+vy}{z}=\frac{uz+(v-u)\,y}{x}=\frac{vz-(u-v)\,x}{y}=\sqrt{2uv};$$

ciascuna delle quali conduce alla (1); infatti dall'equazione $\dfrac{ux+vy}{z}=\sqrt{2uv}$, essendo $u=z-x$, $v=z-y$, si ha

$$ux+vy=zx+zy-x^2-y^2=z\sqrt{2uv}=z\sqrt{2[z^2-(x+y)z+xy]};$$

d'onde

$$zx+zy-z^2=z\sqrt{2[z^2-(x+y)z+xy]};$$

dividendola per z ho

$$x+y-z=\sqrt{2[z^2-(x+y)z+xy]};$$

quadrandola ho, a fatte riduzioni, la (1) ecc.

f) Teorema. — *Le formule* (3) *della* e) *assumono le forme seguenti:*

$$(1) \qquad z = p^2 + q^2; \qquad y = 2pq; \qquad x = p^2 - q^2,$$

ove p *e* q *sono degli* N_1 *primi fra loro, se tali si suppongono nella* $x^2 + y^2 = z^2$ *i numeri intieri* z, y, x *due a due fra loro.*

Dimostrazione. — Infatti dalla nota equazione

$$z^2 - 2(u+v)z + (u^2+v^2) = 0,$$

ricavo $z = u + v \pm \sqrt{2uv}$; essendo $z = x + u = y + v$, avremo $x = v \pm \sqrt{2uv}$, $y = u \pm \sqrt{2uv}$. Dovendo essere $2uv$ un quadrato pari, potremo porre $u = 2\lambda^2$, $v = \mu^2$; e quindi avremo

$$(2) \quad z = (\lambda \pm \mu)^2 + \lambda^2; \; x = \mu^2 \pm 2\lambda\mu = (\lambda \pm \mu)^2 - \lambda^2; \; y = 2(\lambda^2 \pm \lambda\mu)^2 = 2\lambda(\lambda \pm \mu).$$

Ora facendo in queste formule $\lambda \pm \mu = p$, $\lambda = q$, le (*i*) divengono

$$(3) \qquad z = p^2 + q^2, \qquad x = p^2 - q^2, \qquad y = 2pq.$$

Osservazione 1ª. — Si è detto che se x, y, z sono primi due a due fra loro, tali son pure p e q; ciò discende dal corollario del teor. *b)*.

Osservazione 2ª. — Dalle (3) si vede che se p e q fossero entrambi degli $N_1 2 + 1$, allora x, y, z non sarebbero più primi due a due fra loro. Dunque p e q dovranno essere l'uno un $N_1 2$, l'altro un $N_1 2 + 1$.

g) Alcune proprietà dei numeri x, y, z.

1ª. Da quanto si è detto più sopra e dalle (3) se ne inferisce che dei tre numeri interi x, y, z due sono degli $N_1 2 + 1$ ed uno dei due x ed y è un $N_1 2$.

2ª. Essendo $x^2 + y^2 = z^2$, si avrà $(x+y)^2 - z^2 = 2xy$; quindi la somma $x + y + z$ e la differenza $x + y - z$ divideranno il prodotto $2xy$; ed essendo $x + y - z$ un $N_1 2$, non potrà mai dividere x, che è un $N_1 2 + 1$; e quando $x + y - z$ sarà prima con x, esso dividerà y.

3ª. Il 3 è sempre divisore di uno dei due numeri x, y.

Se è $x = p^2 - q^2$; e p e q sono primi con 3, p^2 e q^2 saranno della forma $N_1 3 + 1$, e perciò si ha

$$x = p^2 - q^2 = N_1 3 + 1 - (N_1 3 + 1) = N_1 3.$$

4ª. Il 4 è sempre divisore di uno dei due numeri x ed y.

Infatti se è: $y = 2pq$, dovendo essere p o q. (Vedi Oss. 2ª di *f)*) un $N_1 2$, ne consegue che y è un $N_1 4$.

5ª. Il 5 è sempre divisore di uno dei tre numeri x, y, z.

Se p o q fosse un $N_1 5$, allora $y = 2pq$ sarebbe un $N_1 5$; quindi supponiamoli non divisibili per 5; ora si sa che un N_1^2 può mettersi sotto le forme: $N_1 5 \pm 1$; quindi:

$$x = p^2 - q^2 = (N_1 5 \pm 1) - (N_1 5 \pm 1) = N_1 5,$$

ovvero:

$$z = p^2 + q^2 = (N_1 5 \mp 1) + (N_1 5 \pm 1) = N_1 5;$$

6ª. Essendo 3, 4, 5 primi due a due fra loro, dalle proprietà 3ª, 4ª e 5ª ne consegue che xyz è divisibile per 60.

7ª. Il 7 è sempre divisore di uno dei quattro numeri $x, y, x - y, x + y$. Infatti avendosi $x = p^2 - q^2$, $y = 2pq$, si ottiene:

$$x \pm y = p^2 - q^2 \pm 2pq = (p \pm q)^2 - 2q^2.$$

Ora si sa che un N_1^2 può avere una delle forme seguenti: $N_1 7 + 1$, $N_1 7 + 2$,

$N_1 7 + 4$. Se p o q fosse un $N_1 7$, allora y sarebbe un $N_1 7$; quindi supponiamo che p e q non siano degli $N_1 7$. Se p^2 e q^2 sono entrambi di una delle tre forme suesposte, si ha:

$$x = p^2 - q^2 = (N_1 7 + \alpha) - (N_1 7 + \alpha) = N_1 7,$$

ove α può assumere i valori 1, 2, 4; e quindi x è un $N_1 7$.

Essendo p^2 e q^2 di forme diverse, possono verificarsi questi sei casi:

1°. $p^2 = N_1 7 + 1, \quad q^2 = N.7 + 2;$
2°. $p^2 = N_1 7 + 1, \quad q^2 = N_2 7 + 4;$
3°. $p^2 = N_1 7 + 2, \quad q^2 = N_1 7 + 4;$
4°. $p^2 = N_1 7 + 2, \quad q^2 = N_1 7 + 1;$
5°. $p^2 = N_1 7 + 4, \quad q^2 = N_1 7 + 1;$
6°. $p^2 = N_1 7 + 4, \quad q^2 = N_1 7 + 2;$

ed osservando che si ha:

$$x^2 - y^2 = (x + y)\,(x - y) = (p^2 - q^2)^2 - 4p^2q^2;$$

si verifica facilmente in tutti e sei i casi che è: $(x + y) . (x - y) = N_1 7$; quindi $x + y$ o $x - y$ è un $N_1 7$.

8ª. Sia n un N_p maggiore di 3, allora y è un $N_1 12$.

Essendo x un N_p pel teorema *c)* del n. 2 si ha: $z - y = 1$ ossia $p^2 + q^2 - 2pq = 1$; d'onde $p - q = 1$, cioè $p = q + 1$; e quindi:

$$x = 2q + 1, \qquad y = 2q\,(q + 1), \qquad z = 2q^2 + 2q + 1.$$

Essendo x un N_p maggiore di 3, dovrà essere della forma $N_1 6 + 1$, e quindi si avrà: $2q + 1 = N_1 6 + 1$; da cui si ricava:

1°. $q = N_1 3$; 2°. $q = N_1 3 - 1$.

Nel 1° caso si avrà: $y = N_1 3$; sicchè in questo caso y è un $N_1 3$. Nel 2° caso essendo $q = N_1 3 - 1$, sarà $p = q + 1 = N_1 3$; quindi avremo: $y = N_1 3$; quindi anche in questo caso y è un $N_1 3$. Ma si sa dalla 4ª proprietà che y è un $N_1 4$, quindi essendo anche un $N_1 3$, ne consegue che esso è un $N_1 12$.

§ III.

La memoria di L. Calzolari. (*)

1. Risoluzione dell'equazione $x^3 + y^3 = z^3$.

a) Si suppongono x, y, z primi fra loro due a due; ed anche in questo caso due di essi saranno degli $N_1 2 + 1$ ed il rimanente un $N_1 2$. Sia $z = x + u = y + v$; si osserva che anche in questo caso x ed y si scambiano fra loro, scambiando fra loro u e v, e che z, $x + y - z$, $x^2 + y^2 - z^2$ sono funzioni simmetriche di u e v, e valgono per u, v, x, y, z le proprietà del n. 4 teorema *b)* § II.

(*) Vedi L. Calzolari. " Tentativo per dimostrare il teorema di Fermat sull'equazione indeterminata $x^n + y^n = z^n$ ". Ferrara, 1855.

b) Teorema. — *Se l'equazione* (1) $x^3 + y^3 = z^3$ *è risolubile in* N_1, *i valori di* x, y, z *assumono anch'essi la forma:*

$$z = u + v + w; \qquad x = v + u; \qquad y = u + w, \tag{2}$$

nelle quali w *è un* N_1 *e funzione simmetrica di* u *e* v.

Dimostrazione. — Dall'equazione (1) sapendosi che è: $x = z - u$, $y = z - v$, si ha:

$$z^3 - x^2 . x - y^2 . y = z^3 - x^2 . (z - u) - y^2 . (z - u) = 0;$$

d'onde dividendole per z si ricava

$$z^2 - x^2 - y^2 + \frac{ux^2 + vy^2}{z} = 0. \tag{3}$$

Ora si ponga:

$$w_1 = \frac{ux^2 + vy^2}{z}, \tag{4}$$

che è un N_1 e funzione simmetrica di u e v come $x^2 + y^2 - z^2$, a cui esso è uguale; così la (3) diviene (5) $z^2 - x^2 - y^2 + w_1 = 0$. Facendo in questa come precedentemente (6) $x = z - u$, $y = z - v$, e poi dividendo l'equazione così ottenuta per z avremo:

$$z - x - y + \frac{ux + vy + w_1}{z} = 0; \tag{7}$$

ora si ponga

$$w = \frac{ux + vy + w_1}{z}, \tag{8}$$

che è pur esso un N_1 e funzione simmetrica di u e v come $x + y - z$, a cui esso è uguale. Si avrà (9) $z - x - y + w = 0$; dalla quale, combinata colle (6) si ricavano le (2).

Osservazione 1ª. — Se nell'equazione $z^3 - x^3 - y^3 = z^2 . z - x^2 . x - y^2 . y = 0$, si fa

$$1^0.\ z = x + u, \quad y = x + u - v; \qquad 2^0.\ z = y + v, \quad x = y + v - u$$

si ottiene

$$z^2 (x + u) = x^3 - y^2 (x + u - v) = 0.$$
$$z^2 (y + v) - x^2 (y + v - u) - y^3 = 0;$$

dividendola rispettivamente per x ed y si ha:

$$\frac{uz^2 - (u - v)\, y^2}{x} = \frac{vz^2 - (v - u)\, x^2}{y} = x^2 + y^2 - z^2 = w_1,$$

e quindi

$$\frac{ux^2 + vy^2}{z} = \frac{uz^2 - (u - v)\, y^2}{x} = \frac{vz^2 - (v - u)\, x^2}{y} = w_1. \tag{10}$$

Analogamente sostituendo nella $z^2 - x^2 - y^2 + w_1 = z . z - x . x - y . y + w_1 = 0$;

$$1^0.\ z = x + u, \quad y = x + u - v; \qquad 2^0.\ z = y + v, \quad x = y + v - u$$

si avrà:

$$z (x + u) - x^2 - y (x + u - v) + w_1 = 0.$$
$$z (y + v) - x (y + v - u) - y^2 + w_1 = 0;$$

dividendole rispettivamente per x ed y, si avrà:

$$\frac{uz-(u-v)y+w_1}{x}=\frac{vz-(v-u)x+w_1}{y}=x+y-z=w;$$

quindi avremo:

$$(11)\qquad \frac{ux+vy+w_1}{z}=\frac{uz-(u-v)y+w_1}{x}=\frac{vz-(v-u)x+w_1}{y}=w.$$

Osservazione 2ª. — Ammesso di poter risolvere in N_1 la (1), deve certamente esistere un N_1, che dico w, pari e funzione simmetrica di u e v tale che aggiunto ad $u+v$, a v, ad u dia i valori di z, x, y, che soddisfano l'equazione (1).

c) Teorema. — *Se l'equazione* (1) $x^3+y^3=z^3$ *è possibile in* N_1,

$$(2)\qquad \frac{u^3+v^3}{z},\quad \frac{u^3-(u-v)^3}{x},\quad \frac{v^3-(v-u)^3}{y}$$

debbono essere degli N_1; *in altri termini il numero intero* w *va determinato in modo che* z, x, y *siano rispettivamente divisori di* u^3+v^3, $u^3-(u-v)^3$, $v^3-(v-u)^3$.

Dimostrazione. — Avendo posto $u=z-x$, $v=z-y$, dalla (1) abbiamo subito

$$(3)\qquad z^3-3(u+v)z^2+3(u^2+v^2)z-(u^3+v^3)=0;$$

dividendola per z si vede che $\frac{u^3+v^3}{z}$ è un N_1.

Procedendo come nel n. 4, teorema *d)* § II si dimostra che

$$\frac{u^3-(u-v)^3}{x},\qquad \frac{v^3-(v-u)^3}{y}$$

sono pure degli N_1. Dunque ecc.

Osservazione 1ª. — Identica all'osservazione del teorema *d)* del n. 4, § II.

Osservazione 2ª. — Perciò il *criterio di possibilità* per risolvere in N_1 la (1) è dunque rappresentato dalle (2), che debbono essere ad un tempo eguali ad un N_1 per un sol valore di w intero, positivo, pari e funzione simmetrica di u e v.

d) Teorema. — *L'equazione* (1) $x^3+y^3=z^3$ *non può essere risolta in* N_1.

Dimostrazione. — Si ha

$$\frac{u^3+v^3}{z}=\frac{(u+v)(u^2-uv+v^2)}{z}=\frac{(u+v)\left(u+v+\sqrt{3uv}\right)\left(u+v-\sqrt{3uv}\right)}{u+v+w};$$

esclusi i valori zero e negativi di w, il solo valore di w, che possa rendere intera l'espressione precedente è (2) $w=\sqrt{3uv}$, purchè $3uv$ rappresenti un quadrato pari. Analogamente si ha

$$\frac{u^3-(u-v)^3}{x}=\frac{v\left[v+\sqrt{3u(v-u)}\right]\left[v-\sqrt{3u(v-u)}\right]}{v+w};$$

qui il valore di w non può essere che (3) $w=\sqrt{3u(v-u)}$.

E così si ha pure

$$\frac{v^3-(v-u)^3}{y}=\frac{u\left[u+\sqrt{3v(u-v)}\right]\left[u-\sqrt{3v(u-v)}\right]}{u+w};$$

e qui il valore di w sarà (4) $w=\sqrt{3v(u-v)}$.

Dalla (2), (3), (4) si ottiene

$$w^2 = 3uv = 3u(v-u) = 3v(u-v);$$

d'onde: (5) $u = v = 0$; il che è assurdo. Dunque ecc.

OSSERVAZIONE. — Dalle (3), (4) si vede anche che w è ad un tempo reale ed immaginario; il che è pure assurdo ecc.

2. Risoluzione dell'equazione $x^n + y^n = z^n$ per $n > 3$.

a) Anche in questo caso generale supponiamo x, y, z primi due a due fra loro e $u = z - x$, $u = z - y$. I numeri x, y, z saranno due dispari ed uno pari; il trinomio $(x^{n-s} + y^{n-s} - z^{n-s})$, ove s può assumere i valori $1, 2, 3, \ldots (n-1)$, è sempre un N_12; anche in questo caso si può mostrare che z e tutti i trinomi $(x^{n-s} + y^{n-s} - z^{n-s})$ son funzioni simmetriche di u e v, e che x ed y si scambian fra loro, scambiando fra loro u e v; ed anche in questo caso valgono per x, y, z le proprietà contenute nel teor. *b)* del n. 4, § II.

b) TEOREMA. — *Se l'equazione* (1) $x^n + y^n = z^n$ *per* $n > 3$ *è risolubile in* N_1, *come nei casi di* $n = 2, 3$ *si hanno le formole risolventi:*

$$\text{(2)} \qquad z = u + v + w, \qquad x = v + w, \qquad y = u + w;$$

dove w *mantiene sempre la proprietà di essere un* N_12 *e funzione simmetrica di* u *e* v.

DIMOSTRAZIONE. — La dimostrazione di questo teorema è identica a quella del teorema *b)* del n. 1, § III.

Nell'equazione $z^n - x^n - y^n = 0$ s'introducono i valori semplici di x ed y dati da $x = z - u$, $y = z - v$, così:

$$z^n - x^n - y^n = z^n - x^{n-1}.x - y^{n-1}.y = z^n - x^{n-1}(z-u) - y^{n-1}(z-v) =$$
$$= z^n - zx^{n-1} - zy^{n-1} + ux^{n-1} + vy^{n-1} = 0;$$

dividendola per z avremo:

$$\text{(3)} \qquad z^{n-1} - x^{n-1} - y^{n-1} + \frac{ux^{n-1} + vy^{n-1}}{z} = 0;$$

e ponendo:

$$\text{(4)} \qquad w_1 = \frac{ux^{n-1} + vy^{n-1}}{z},$$

la (3) diverrà:

$$\text{(5)} \qquad z^{n-1} - x^{n-1} - y^{n-1} + w_1 = 0,$$

ove w_1 è un N_12 e funzione simmetrica di u e v come il trinomio $x^{n-1} + y^{n-1} - z^{n-1}$, a cui esso è uguale. Ripetendo sull'equazione (5) la solita sostituzione per x ed y e la divisione per z, come si è fatto nella (1), e ponendo

$$\text{(6)} \qquad \frac{ux^{n-2} + vy^{n-2}}{z} = w_2;$$

la (5) diverrà:

$$\text{(7)} \qquad z^{n-2} - x^{n-2} - y^{n-2} + w_2 = 0,$$

ove w_2 è un N_12 e funzione simmetrica di u e v, come il trinomio $x^{n-2} + y^{n-2} - z^{n-2}$, a cui esso è uguale. Procedendo a questo modo si otterrà la serie di equazioni successive:

$$\text{(8)} \qquad z^{n-1} - x^{n-1} - y^{n-1} + w_1 = 0;\ z^{n-2} - x^{n-2} - y^{n-2} + w_2 = 0; \ldots;$$
$$z^{n-s} - x^{n-s} - y^{n-s} + w_s = 0; \ldots;\ z - x - y + w_{n-1} = 0;$$

e per semplicità di scrittura porremo: $w_{n-1} = w$, il quale conserva evidentemente le stesse proprietà di $w_1, w_2, w_3 \ldots, w_{n-2}$, cioè di significare un $N_1 2$ ed una funzione simmetrica di u e v. Combinando al solito le $u = z - x$, $v = z - y$ colla $z - x - y + w = 0$, si hanno le (2).

Osservazione 1ª. — La stessa Oss. 1ª fatta nel teor. *b)* del n. 1 di questo paragrafo; così si hanno le due nuove condizioni:

$$(9) \qquad \frac{uz^{n-1} - (u - v)\, y^{n-1}}{x} = \frac{uz^{n-1} - (v - u)\, x^{n-1}}{y} = w_1,$$

le quali unitamente alla (4) servono di fondamento a stabilire il *criterio di possibilità* per l'equazione (1).

Osservazione 2ª. — Se la (1) è possibile in N_1, deve di conseguenza potersi determinare un N_1 che sia un $N_1 2$ e funzione simmetrica di u e v tale che aggiunto successivamente ad $u + v$, a v, ad u dia le formole (2), che soddisfano la (1).

c) Teorema. — *Nella ipotesi che* (1) $x^n + y^n = z^n$ *sia risolubile in* N_1;

$$(2) \qquad \frac{u^n + v^n}{z}, \quad \frac{u^n - (u - v)^n}{x}, \quad \frac{v^n - (v - u)^n}{y}$$

saranno degli N_1; in altri termini conviene determinare w in modo da rendere z, x, y rispettivamente divisori di:

$$u^n + v^n, \qquad u^n - (u - v)^n, \qquad v^n - (v - u)^n.$$

Dimostrazione. — Essendo $u = z - x$, $v = z - y$, dalla (1) ricaviamo:

$$(3) \quad z^n - \binom{n}{1}(u + v)\, z^{n-1} + \binom{n}{2}(u^2 + v^2)\, z^{n-2} - \binom{n}{3}(u^3 + v^3)\, z^{n-3} + \ldots + \\ + (-1)^s \binom{n}{s}(u^s + v^s)\, z^{n-s} + \ldots + (-1)^n (u^n + v^n) = 0;$$

dividendola per z si vede che $\frac{u^n + v^n}{z}$ è un N_1. Sostituendo nella (3) per z una volta $z = x + u$ e poi $z = y + v$, e quindi dividendo rispettivamente le equazioni così ottenute per x ed y si avranno $\frac{u^n - (u - v)^n}{x}$, $\frac{v^n - (v - u)^n}{y}$, che sono degli N_1.

Osservazione 1ª. — Le (2) rappresentano *il criterio di possibilità* per l'equazione (1); un sol valore di w intero, positivo, pari e funzione simmetrica di u e v deve rendere le (2) uguali a tre N_1.

Osservazione 2ª. — Identica a quella del teorema *d)* del n. 4 del § II.

d) Teorema. — *L'equazione* (1) $x^n + y^n = z^n$ *è impossibile in* N_1 *per*

$$n = N_1 . 2 + 1 > 1.$$

Dimostrazione. — Vediamo quali valori dovrà assumere w, affinchè le espressioni (2) del teorema *c)* siano degli N_1; consideriamo la 1ª delle (2) del teorema *c)*; si ha pel teorema di Cotes per $n = N_1 2 + 1$:

$$u^n + v^n = (u + v)\left(u^2 - 2uv\cos\frac{\pi}{n} + v^2\right)\left(u^2 - 2uv\cos\frac{3\pi}{n} + v^2\right) \ldots \\ \left(u^2 - 2uv\cos\frac{n-4}{n}\pi + v^2\right)\left(u^2 - 2uv\cos\frac{n-2}{n}\pi + v^2\right) = 0;$$

e si sa che è

$$u^2-2uv\cos\frac{\lambda\pi}{n}+v^2=\left(u+v+\sqrt{2uv}\,.\sqrt{1+\cos\frac{\lambda\pi}{n}}\right)\left(u+v-\sqrt{2uv}\,.\sqrt{1+\cos\frac{\lambda\pi}{n}}\right)=$$

$$=\left(u+v+2\sqrt{uv}\,.\cos\frac{\lambda\pi}{n}\right)\left(u+v-2\sqrt{uv}\,.\cos\frac{\lambda\pi}{n}\right)=0,$$

ove λ è un N_1; dunque u^n+v^n sarà divisibile per $z=u+v+w$, se sarà

$$w=2\sqrt{uv}\cos\frac{\lambda\pi}{2n}\,; \tag{2}$$

ove qui λ è un $N_1 2+1$; e si vede che w è funzione simmetrica di u e v, e sarà un N_1, se tale potrà ridursi il 2° membro della (2).

Consideriamo la 2ª delle (2) del teorema *c)*; essendo n un $N_1 2+1$, il suo numeratore potrà scriversi così: $u^n+(v-u)^n$, e come precedentemente si avrà:

$$w=2\sqrt{u(v-u)}\cos\frac{\lambda'\pi}{2n}, \tag{3}$$

ove λ' è un $N_1 2+1$; da cui si vede che w non è più funzione simmetrica di u e v. Ora consideriamo la 3ª delle (2) del teorema *c)*; permutando gli elementi u e v, e ripetendo il calcolo precedente per $v^n-(v-u)^n=v^n+(u-v)^n$ si ottiene:

$$w=2\sqrt{v(u-v)}\,.\cos\frac{\lambda''\pi}{2n}, \tag{4}$$

ove λ'' è un $N_1 2+1$.

Dalle (3) e (4) si vede che w è ad un tempo un numero reale ed un numero immaginario; e dalle (2), (3), (4) che w è funzione simmetrica e non simmetrica di u e v; il che è assurdo.

Osservazione. — Le impossibilità trovate si possono giustificare in questo modo: i fattori di u^n+v^n, all'infuori di $u+v$, sono tutti degli $N_1 2+1$, poichè essendo: $u^n+v^n=(u+v)(u^{n-1}+u^{n-2}v+\ldots+uv^{n-2}+v^{n-1})$, si vede che l'$N_1$ dentro la 2ª parentesi è sempre un $N_1 2+1$, tanto se u e v sono degli $N_1 2+1$, quanto se l'uno è un $N_1 2$ e l'altro un $N_1 2+1$. In egual modo si vede che i due numeri $u^n+(v-u)^n$ e $v^n+(u-v)^n$, in cui u e $v-u$, v e $u-v$ si conservano primi fra loro, oltre i fattori $u+v-u=v$, $v+u-v=u$, ne contengono altri tutti della forma $N_1 2+1$; quindi si ha

$$\frac{u^n+v^n}{z}=\frac{(u+v).N_1 2+1}{z}\,;\quad \frac{u^n-(u-v)^n}{x}=\frac{v.N_1 2+1}{x}\,;\quad \frac{v^n-(v-u)^n}{y}=\frac{u.N_1 2+1}{y}\,;$$

ma z non può dividere $(u+v)$, x la v, y la u; onde z, x, y debbono ricercarsi fra i divisori degli $N_1 2+1$; così ne verrebbe che tre $N_1 2+1$ verificherebbero la (1); il che pel teorema *a)* è assurdo.

e) Teorema. — *L'equazione* (1) $x^n+y^n=z^n$ *è impossibile in* N_1 *per* n *della forma* $N_1 2>2$.

Dimostrazione. — Dal teorema di Cotes per n della forma $N_1 2$ si ha

$$u^n+v^n=\left(u^2-2uv\cos\frac{\pi}{n}+v^2\right)\left(u^2-2uv\cos\frac{3\pi}{n}+v^2\right)\ldots$$

$$\ldots\left(u^2-2uv\cos\frac{n-3}{n}\pi+v^2\right)\left(u^2-2uv\cos\frac{n-1}{n}\pi+v^2\right)=0;$$

e si sa che è:

$$u^2 - 2uv\cos\frac{\lambda\pi}{n} + v^2 = \left(u+v+2\sqrt{uv}\cos\frac{\lambda\pi}{2n}\right)\left(u+v-2\sqrt{uv}\cos\frac{\lambda\pi}{2n}\right),$$

ove λ è un $N_1 2+1$. Dunque $u^n + v^n$ sarà divisibile per $z = u + v + w$, se sarà

(2) $$w = 2\sqrt{uv}\,.\cos\frac{\lambda\pi}{2n},$$

il qual valore è funzione simmetrica di u e v e sarà un N_1, se lo sarà il 2° membro della (2).

Consideriamo il 2° binomio

$$u^n - (u-v)^n = u^n - (v-u)^n = v(2u-v)\left[u^2 - 2u(v-u)\cos\frac{2\pi}{n} + (v-u)^2\right].$$
$$\left[u^2 - 2u(v-u)\cos\frac{4\pi}{n} + (v-u)^2\right]\ldots\left[u^2 - 2u(v-u)\cos\frac{n-4}{n}\pi + (v-u)^2\right].$$
$$\left[u^2 - 2u(v-u)\cos\frac{n-2}{n}\pi + (v-u)^2\right],$$

e si sa che è

$$u^2 - 2u(u-v)\cos\frac{\lambda'\pi}{n} + (v-u)^2 = \left[v + 2\sqrt{u(v-u)}\cos\frac{\lambda'\pi}{2n}\right]\left[v - 2\sqrt{u(v-u)}\cos\frac{\lambda'\pi}{2n}\right],$$

ove λ' è un $N_1 2$ e che $v(2u-v) = -\left(v+\sqrt{2uv}\right)\left(v-\sqrt{2uv}\right)$; quindi affinchè sia $u^n - (u-v)^n$ divisibile per $x = v + w$ bisogna che si abbia:

(3) $$w = \sqrt{2uv} \qquad \text{ovvero} \qquad w = 2\sqrt{u(v-u)}\cos\frac{\lambda'\pi}{2n}.$$

Ora consideriamo il 3° binomio $v^n - (v-u)^n = v^n - (u-v)^n$; affinchè esso sia divisibile per $y = u + w$ si ha, permutando gli elementi u e v nelle (3), che dovrà essere

(4) $$w = \sqrt{2uv}, \qquad \text{ovvero} \qquad w = 2\sqrt{v(u-v)}\cos\frac{\lambda''\pi}{2n},$$

ove λ'' è un $N_1 2$.

Osservando le (3) e (4) si vede che i secondi valori di w sono ad un tempo reali ed immaginari, il che è assurdo. Quindi rimane da considerare i rimanenti; allora avremo

$$\cos\frac{\lambda\pi}{2n} = \frac{1}{\sqrt{2}} = \cos\frac{\pi}{4};$$

e quindi $n = 2\lambda$ con $\lambda = N_1 2 + 1$; ciò equivale a dire che la (1) è risolubile in N_1, supposto il suo grado un $N_1 2$ e tale, che diviso per 2 dia per quoto un $N_1 2+1$; e vedremo che è $\lambda = 1$. Supponiamo $\lambda > 1$; l'equazione $z^{2\lambda} = x^{2\lambda} + y^{2\lambda}$, se poniamo $z^2 = z'$, $x^2 = x'$, $y^2 = y'$, si trasforma nella $z'^\lambda = x'^\lambda + y'^\lambda$; ora questa pel teorema *d)* è insolubile in N_1 per $\lambda > 1$; quindi a fortiori lo sarà la (1); dunque $\lambda = 1$, $n = 2$; e già sappiamo che $w = \sqrt{2uv}$ soddisfa l'equazione $x^2 + y^2 = z^2$, come dovevasi dimostrare.

Osservazione 1ª. — Essendo $\cos\frac{\lambda\pi}{2n} = \frac{1}{\sqrt{2}}$, il valore di w della (2) è irrazionale, mentre si sa che deve essere un N_1.

OSSERVAZIONE 2ª. — Può essere $\cos\frac{\lambda\pi}{2n}=1$ ossia $\frac{\lambda\pi}{2n}=0$, da cui si ha $\lambda=0$, il che è assurdo; e $\frac{\lambda\pi}{2n}=\alpha\,.\,2\pi$, ove α è un N_1, da cui $2n=\frac{\lambda}{2\alpha}$; la quale è assurda, perchè l'esponente della (1) è essenzialmente un N_1.

§ IV.

Memoria 1ª di Legendre. (*)

1. *Quatrième partie. Metodes et recherches sur les puissances des nombres* (p. 361).

a) (324) TEOREMA 2°. — *La somma di due biquadrati non può essere eguale ad un quadrato, a meno che uno di essi non sia nullo.*

DIMOSTRAZIONE. — Sia, se è possibile, $a^4+b^4=c^2$; dapprima bisogna che sia: $a^2=p^2-q^2$, $b^2=2pq$, $c^2=p^2+q^2$. Si osserva poi che a e b potendo essere supposti primi fra loro, p e q saranno primi fra loro, ed anche che non possono essere entrambi degli N_12, poichè se lo fossero, a e b sarebbero tutti e due degli N_12. Non si potrà neanche supporre p pari e q dispari, perchè allora p^2-q^2 sarebbe della forma N_14-1, la quale non può convenire al quadrato a^2. Dunque p è un N_12; e così per soddisfare l'equazione $b^2=2pq$ si prenderà $p=m^2$, $q=2n^2$, valori che essendo sostituiti nell'altra equazione $a^2=p^2-q^2$, daranno $m^4-4n=a^2$. Questa ultima equazione esprimendo che il quadrato m^4 è eguale alla somma di due altri quadrati $4n^2$, a^2, il solo mezzo di soddisfarvi è di prendere: $m^2=f^2+g^2$, $2n^2=2fg$, $a=f^2-g^2$. Nell'equazione $n^2=fg$, f e g sono primi fra loro, dunque $f=\alpha^2$, $g=\beta^2$; e per questi valori l'equazione $m^2=f^2+g^2$ diviene $\alpha^4+\beta^4=m^2$. D'onde si vede che se esistono due biquadrati a^4, b^4, la cui somma sia eguale ad un quadrato c^2, esisteranno ad un tempo due altri biquadrati assai più piccoli α^2, β^2, la cui somma similmente sia eguale ad un quadrato. E per rendere sensibile la piccolezza di questi in confronto dei primi, si dedurrà dai valori precedenti

$$a=\alpha^4-\beta^4,\qquad b=2\alpha\beta\sqrt{\alpha^4+\beta^4},$$

ciò che dà:

$$\alpha^4+\beta^4=\sqrt{\frac{1}{2}\,a^2+\frac{1}{2}\sqrt{a^4+b^4}},$$

e per conseguenza

$$\alpha^4+\beta^4<\sqrt[4]{a^4+b^4}.$$

Si osserverà d'altronde che α e β non possono essere zero, poichè ne seguirebbe $b=0$, caso escluso. Se esiste dunque un quadrato c^2 eguale alla somma di due biquadrati, si conoscerà per suo mezzo un secondo quadrato c'^2 similmente eguale alla somma di due biquadrati, e di cui il lato c' sarà $<\sqrt[4]{c}$, senza esser nullo. Ma per la stessa ragione il quadrato c'^2 ne farà conoscere un terzo c''^2 godente la stessa proprietà, e di cui il lato sarà $c''<\sqrt[4]{c'}$, senza essere nullo e così di seguito. Ora implica

(*) Vedi *Essai sur la théorie des nombres* par A. M. LEGENDRE. Seconde édition. Paris, 1808.

contraddizione che una serie di N_1: $c, c', c'', \ldots$, di cui ciascuno è minore della radice biquadrata del precedente, senza essere nullo, possa essere prolungata all'infinito. Dunque è impossibile che un quadrato si decomponga in due biquadrati.

Corollario 1°. — *La stessa dimostrazione prova che la forma* $\mathrm{m}^4 - 4\mathrm{n}^4$ *non può essere eguale ad un quadrato, se non è* $\mathrm{n} = 0$.

Corollario 2°. — *La stessa dimostrazione prova che la forma* $\mathrm{x}^4 + \mathrm{y}^4$ *non può essere eguale a* $\mathrm{z}^4 = (\mathrm{z}^2)^2$ *ecc.*

b) Teorema 5°. — *La somma o la differenza di due cubi non può essere eguale ad un cubo.*

Dimostrazione. — Sia, se è possibile, $x^3 \pm y^3 = z^3$; si potrà supporre secondo il solito che x, y, z siano primi fra loro. Ciò premesso, tra i numeri x, y, z ve ne son sempre due dispari ed uno pari; siano x ed y i dispari, che si possono sempre porre nello stesso membro; se si fa: $x \pm y = 2p$, $x \mp y = 2q$, ovvero $x = p + q$, $x \pm y = -q$ si avrà colla sostituzione: $2p(p^2 + 3q^2) = z^3$; e si osserverà ulteriormente che, poichè $p + q$ e $p - q$ devono essere dispari, bisogna che p e q siano uno pari, l'altro dispari; di maniera che $p^2 + 3q^2$ sarà sempre dispari. Ma $2p(p^2 + 3q^2)$ dovendo essere un cubo, è chiaro che $2p$ sarà divisibile per 8, e così p sarà un $N_1 2$ e q un $N_1 2 + 1$. Ora vi sono due casi da distinguere, secondo che p è o non è divisibile per 3.

1° Caso. — Se p non è un $N_1 3$, i fattori $2p$, $p^2 + 3q^2$ saranno primi fra loro, e se il loro prodotto è un cubo, bisognerà che ciascun d'essi ne sia uno. Sia dunque $p^2 + 3d^2 = r^3$; allora r sarà della forma $m^2 + 3n^2$, e si potrà fare

$$p + q\sqrt{-3} = (m + n\sqrt{-3})^3,$$

ciò che darà: $p = m^3 - 9mn^2$, $q = 3m^2n - 3n^3$. Questi valori soddisfano l'equazione $p^2 + 3q^2 = r^3$; ma d'altronde essi hanno tutta la generalità necessaria, come uno se ne può assicurare colla risoluzione diretta di questa equazione. Non resta dunque più che fare in modo che $2p$ o $2m(m + 3n)(m - 3n)$ sia un cubo. Ora è facile vedere che i tre fattori di questa quantità sono primi fra loro, e così ciascuno di essi deve essere un cubo; sia conseguentemente

$$m + 3n = a^3, \quad m - 3n = b^3, \quad 2m = c^3,$$

si avrà: $a^3 + b^3 = c^3$. Di qui si vede che se l'equazione $x^3 \pm y^3 = z^3$ è possibile in N_1, l'equazione $a^3 + b^3 = c^3$, simile alla prima ed espressa in numeri assai più piccoli, sarà egualmente possibile. Sia ora

$$\mathrm{A} = x^3 \pm y^3 = 2p(p^2 + 3q^2) \qquad \text{e} \qquad \mathrm{A}' = a^3 + b^3;$$

si avrà colla sostituzione dei valori precedenti:

$$\mathrm{A} = (a^3 + b^3)\, a^3 b^3 \left(\frac{a^6 + a^3 b^3 + b^6}{3}\right)^3,$$

ed a causa di $a^6 + b^6 > 2a^3b^3$, questa formula darà: $\mathrm{A} > (a^3 + b^3)\, a^{12} b^{12}$. Ma (eccetto il caso di $a = b = 1$ che non può mai verificarsi) si ha sempre: $a^3b^3 > \frac{a^3 + b^3}{3}$; dunque $\frac{1}{2}\mathrm{A}$ è maggiore di $\left(\frac{a^3 + b^3}{2}\right)^5$ o $\left(\frac{\mathrm{A}'}{2}\right)^5$: dunque $\frac{1}{2}\mathrm{A}' < \sqrt[5]{\frac{\mathrm{A}}{2}}$. Ma collo stesso ragionamento si dedurrà dal cubo di A' un terzo cubo A'' tale che $\frac{1}{2}\mathrm{A}''$ sarà $< \sqrt{\frac{\mathrm{A}'}{2}}$, e così all'infinito; ora è impossibile che una serie di N_1: $\mathrm{A}, \mathrm{A}', \mathrm{A}'' \ldots$

sia decrescente e prolungata all'infinito; dunque è impossibile che la formola: $2p(p^2+3q^2)$ sia un cubo, almeno allorchè p non è divisibile per 3.

2° Caso. — Se p è divisibile per 3, si farà $p=3r$ e la formula $2p(p^2+3q^2)$ diverrà: $18r(q^2+3r^2)$. Ora siccome i fattori $18r, q^2+3r^2$ son primi fra loro, bisognerà che ciascuno di essi sia un cubo. Facendo dunque dapprima: $q^2+3r^2=(f^2+3g^2)^3$ o piuttosto $q+r\sqrt{-3}=(f+g\sqrt{-3})^3$, ciò che darà: $r=f^3-9fg^2, r=3f^2g-3g^3$, resterà da farsi in modo che $18r$ o $27 . 2g . (f+g) . (f-g)$ sia un cubo. D'onde si dedurrà come sopra $f+g=a^3, f-g=b^3, 2g=c^3$, e per conseguenza: $a^3-b^3=c^3$. Ora similmente si farà vedere che il cubo c^3, eguale ad a^3-b^3, è assai più piccolo del cubo z^3, eguale a $2p(p^2+3q^2)$, (poichè si ha $c<\sqrt[3]{\frac{8}{9}z}$); si ricadrà dunque ancora su di una serie di N_1, che deve essere decrescente e prolungata all'infinito; donde si concluderà che le equazioni $x^3 \pm y^3 = z^3$ sono impossibili, a meno che l'uno dei termini non sia nullo.

Osservazione. — Si è dimostrato che le equazioni: $x^3 \pm y^3 = z^3$ e $x^4 \pm y^4 = z^2$ ecc., sono impossibili in N_1; Fermat ha asserito di più (ediz. cit. Dioph. pag. 61) che l'equazione $x^n + y^n = z^n$ è generalmente impossibile per $n>2$. È facile vedere che la proposizione sarà dimostrata in generale, se la è pel caso che n sia un Np.

§ V.

Memoria di Lejeune-Dirichlet. (*)

1. Se esistono degli N_1: t, u, v, che soddisfano l'equazione

$$t^{14} = u^{14} + v^{14}, \tag{1}$$

è manifesto che un fattore comune δ a due di essi dovrà dividere necessariamente l'altro. Si potrà dividere ciascun d'essi per δ, ciò non cambierà punto la forma dell'equazione; d'onde se ne conclude che si può sempre considerare gli N_1: t, u, v primi due a due fra loro. Ciò posto questi N_1 debbono evidentemente essere supposti l'uno un $N_1 2$, gli altri degli $N_1 2+1$; e l'$N_1 2$ sarà uno di quelli che compariscono al 2° membro. Si vede pure che se fra questi N_1 avvene uno divisibile per 7, non potrebbe essere che t, poichè 7 non può mai dividere la somma di due quadrati primi fra loro. L'equazione (1) essendo simmetrica rispetto ad u e v, possiamo supporre che, se fra questi N_1 vi è un $N_1 7$, v si trova in questo caso. Trasportando il termine u, l'equazione cambierà in questa

$$t^{14} - u^{14} = v^{14}, \tag{2}$$

che si può mettere sotto questa forma

$$(t^2-u^2)\left[(t^2-u^2)^6 + 7t^2u^2(t^4-t^2u^2+u^4)^2\right] = v^{14}. \tag{3}$$

(*) Vedi *Journal* de Crelle-Neunten, Band, Berlin, 1832, pag. 390 " Démonstration du théorème de Fermat pour le cas des 14ièmes puissances " par M. Lejeune-Dirichlet, prof. de Math. à Berlin.

I t, u essendo stati supposti primi fra loro, $t^2 - u^2$, tu sono pure primi fra loro e così anche $t^2 - u^2$ e $t^4 - t^2u^2 + u^4$, poichè ogni N_p divisore comune di questi dividerà

$$t^4 - t^2u^2 + u^4 - (t^2 - u^2)^2 = t^2u^2,$$

e per conseguenza anche tu. I numeri tu e $t^2 - u^2$ avranno dunque questo stesso divisore comune, la qual cosa non concorda con ciò che si è mostrato. Da ciò risulta, se per brevità poniamo

$$t^2 - u^2 = \varphi, \qquad tu\,(t^4 - t^2u^2 + u^4) = \psi,$$

che φ e ψ, di cui evidentemente l'uno è un $N_1 2$, l'altro un $N_1 2 + 1$, non hanno lo stesso divisore comune; e si avrà

(4)
$$\varphi \cdot ((\varphi^3)^2 + 7\psi^2) = v^{14}.$$

Noi distingueremo ora due casi, secondo che v è o non è divisibile per 7. Se in primo luogo si suppone v non divisibile per 7, φ non lo sarà pure; e da ciò consegue, e dal fatto che φ e ψ sono primi fra loro, che i due fattori del primo membro sono anche primi fra loro, e per conseguenza uguali l'uno e l'altro a delle 14esime potenze. D'altra parte si può conchiudere da un teorema conosciuto che la radice della 14esima potenza dispari $(\varphi^3)^2 + 7\psi^2$ ha la stessa forma $g^2 + 7h^2$, e si prova facilmente che gl'interi g ed h soddisfano all'equazione

$$\varphi^3 + \psi\sqrt{-7} = (g + h\sqrt{-7})^{14},$$

in cui bisogna eguagliare separatamente le parti reali ed i coefficienti di $\sqrt{-7}$. Senza sviluppare questa espressione è evidente che il valore che essa dà per ψ è divisibile per 7; ma essendo $\psi = tu\,(t^4 - t^2u^2 + v^4) = tu\,[(t^2 - u^2)^2 + t^2u^2]$ non può essere divisibile per 7, a meno che non lo sia t od u; il che sarebbe contrario all'ipotesi fatta più sopra. È adunque provato che il caso che si suppone di v non divisibile per 7, nello stesso tempo che t ed u, non potrebbe aver luogo.

Resta a far vedere che l'equazione (2) non può sussistere neppure se considerasi v come un $N_1 7$. Facendovi $v = 7w$, essa diverrà

$$t^{14} - u^{14} = 7^{14} \cdot w^{14};$$

questa è l'equazione di cui proveremo l'impossibilità. Senza complicare la via della dimostrazione, noi possiamo invece dell'equazione precedente, trattare l'equazione più generale

(5)
$$t^{14} - u^{14} = 2^m \cdot 7^{1+n} \cdot w^{14};$$

i numeri t, u essendo supposti sempre primi fra loro ed m ed n designando degli N_0. Conservando tutte le denominazioni precedenti, l'equazione (5) potrà essere messa sotto questa forma

$$\varphi\,[(\varphi^3)^2 + 7\psi^2] = 2^m \cdot 7^{1+n} \cdot w^{14}.$$

Siccome essa richiede evidentemente che φ sia un $N_1 7$, facciamo $\varphi = 7\chi$, noi così avremo

$$7^2\chi \cdot [\psi^2 + 7\,(7^2\chi^3)^2] = 2^m \cdot 7^{1+n} \cdot w^{14}.$$

È facile vedere che i due fattori $7^2\chi$ e $\psi^2 + 7\,(7^2\chi^3)^2$, di cui il 2° è impari, sono primi fra loro. Da ciò risulta che l'equazione precedente non può sussistere, a meno che $\psi^2 + 7(7^2\chi^3)^2$ e $7^2\varphi$ non siano il 1° una 14^{esima} potenza, il 2° il prodotto di una potenza eguale per $2^m . 7^{1+n}$. Per quanto concerne la 1ª di queste condizioni essa richiede, dopo quanto si è detto, che si abbia

$$\psi \pm 7^2\chi^3\sqrt{-7} = (r \pm s\sqrt{-7})^{14},$$

cioè

$$7^2 \cdot \chi^3 = \frac{(r + s\sqrt{-7})^{14} - (r - s\sqrt{-7})^{14}}{2\sqrt{-7}},$$

nella quale gl'interi r ed s son primi fra loro, l'uno pari e l'altro dispari, ed inoltre il 1° non divisibile per 7.

Possiamo far subire a questa espressione una trasformazione simile a quella che si è fatta sul 1° membro dell'equazione (2). A tal uopo basta sostituire nel 1° membro dell'equazione (3) a t ed u rispettivamente $r + s\sqrt{-7}$ e $r - s\sqrt{-7}$; operando in tal modo e facendo per abbreviare

$$(r^2 + 7s^2)(r^4 - 2 . 7^2 r^2 s^2 + 7^2 s^4) = \mathrm{R},$$

si ottiene

$$7^2\chi^3 = 2 . 7 . r . s[\mathrm{R}^2 - (7 . 4^3 . r^3 . s^3)^2],$$

o ciò che è lo stesso, moltiplicando i due membri per 7^4,

$$7^6\chi^3 = 2 . 7^5 . r . s[(\mathrm{R} + 7(4rs)^3)(\mathrm{R} - 7(4rs)^3)].$$

È facile mostrare che i tre fattori $2 . 7^5 . r . s$, $\mathrm{R} + 7(4rs)^3$, $\mathrm{R} - 7(4rs)^3$ sono due a due primi fra loro: è d'altra parte evidente che se vi è un divisore comune, questo non può essere nè 2, nè 7, giacchè i due ultimi N_1 in questione son dispari e non divisibili per 7. Sia in secondo luogo p un N_p impari e diverso da 7; supponiamo che esso sia un divisor comune di due delle espressioni, di cui trattiamo; si vede che esso sarà fattor comune di rs ed R; e facendo di poi attenzione al modo, con cui l'espressione R è composta con r ed s, è evidente che è necessario che p divida alla sua volta r ed s: il che è assurdo, essendo r ed s primi fra fra loro. Noi abbiam visto che $7^2\chi$ doveva essere una 14^{esima} potenza moltiplicata per $2^m . 7^{1+n}$; il 1° membro dell'ultima equazione sarà quindi il prodotto di una potenza del medesimo grado e di $2^{3m} . 7^{3+3n}$. Risulta da ciò e dal fatto che i tre fattori del 2° membro sono primi fra loro, che i due ultimi sono 14^{esime} potenze, e che il primo è il prodotto per una potenza eguale e di $2^{3m} . 7^{3+3n}$. Si avrà dunque

$$2 . 7^5 . r . s = 2^{3m} . 7^{3+3n} . v'^{14}; \qquad \mathrm{R} + 7(4rs)^3 = t'^{14}; \qquad \mathrm{R} - 7(4rs)^3 = u'^{14}.$$

È facile vedere che si può mettere il secondo membro della 1ª di queste equazioni sotto la forma $2^{3m} . 7^{5+n'} . v'^{14}$, dove n' è un N_1. Quando n' è differente da zero, la cosa è evidente; nel caso che n' è eguale a zero, bisogna che affinchè il secondo membro possa essere eguale al primo membro, divisibile per 7^5, che v' sia un $\mathrm{N}_1 7$. Mettendo quindi $7v'$ in luogo di v', il secondo membro prenderà ancora la forma supposta. Noi possiamo quindi alla 1ª delle equazioni precedenti sostituire questa:

$$4rs = 2^{3m+1} . 7^{1+n} . v'^{14}.$$

Prendendo in seguito la differenza delle due ultime, confrontandole e ponendo per brevità $v'^2 = w'$, si avrà

$$t'^{14} - u'^{14} = 2^{9m+6} . 7^{3n'+6} . w'^{14}.$$

Questa equazione, in cui t' ed u' sono primi fra loro, è interamente simile all'equazione (5), da cui essa deriva; solamente i numeri interi t', u', che vi entrano, sono molto più piccoli dei loro analoghi t ed u della (5).

Possiamo quindi concludere nel modo solito che l'equazione (5), e per conseguenza l'equazione (1), non può essere risoluta in N_1.

Berlino, Ottobre 1832.

DIRICHLET.

§ VI.

Memoria di Lamé. (*)

1. *Memoires présentés. — Analyse mathématique. — Memoire sur le dernier théorème de Fermat par* M. G. LAMÉ, pag. 45.

2. Di tutti i teoremi enunciati dal Fermat uno solo resta ancora dimostrato incompletamente. Questo teorema dice " l'equazione $x^n + y^n = z^n$ è impossibile in N_1 per $n > 2$ ". Questa memoria stabilisce la stessa impossibilità per $n = 7$ e per conseguenza per tutti gli $N_1 7$ dispari e non divisibili per 3 o per 5, i soli che non rientrano nei casi precedentemente trattati.

" Nella equazione $x^7 + y^7 + z^7 = 0$, essendo supposta risolta per N_1, dei quali uno almeno sia negativo, e che son primi fra loro, si dimostra dapprima che una delle incognite è necessariamente divisibile per 7, come Legendre l'aveva stabilito nella sua teoria dei numeri. L'equazione essendo decomposta in tre maniere diverse, si stabilisce facilmente la relazione:

$$x + y + z = 7A\mu\eta\rho = 7AP,$$

ove $7, \mu, \eta, \rho$ sono degli N_1 primi fra loro e tali che:

$$z + y = 7^6\mu^7 = a, \qquad z + x = \eta^7 = b, \qquad x + y = \rho^7 = c,$$

supponendo che x sia l'indeterminata divisibile per 7, A è primo con x, y, z ". Si dimostra che A è un quadrato B^2. Questa dimostrazione conduce alle 4 equazioni simmetriche:

$$a + b + c = 27B^2 . P,$$
$$abc = 7^6 . P^7,$$
$$a^2 + b^2 + c^2 + bc + ca + ab = BD,$$
$$3(a^4 + b^4 + c^4) + 10(b^2c^2 + c^2a^2 + a^2b^2) = 2^4 . B^{14};$$

da cui si eliminano a, b, c, per ottenere un'equazione non contenente che i numeri B, D, P. Questa equazione finale coll'aiuto di parecchie decomposizioni successive, è ricondotta alla risoluzione dell'equazione:

$$U^8 - 3 . 7^4 . V^4 . U^4 + 2^4 . 7^7 . V^8 = W^4,$$

di cui si dimostra l'impossibilità in N_1 finiti.

3. Vedi *Compt. rendus.* pag. 359 citato precedentemente *Rapport sur un Mèmoire de M.* LAMÉ *relatif au dérnier théorème de Fermat. (Commissaires M. M. Liouville, Cauchy rapporteur).*

(*) Vedi *Comptes Rendus Hebdomadaires des séances de l'académie des sciences*, t. IX, Paris, 1839.

Le dimostrazioni date per i vari casi particolari si fondano sulla teoria delle forme quadratiche dei N_p; ma le difficoltà incontrate da Legendre su questa via provano che àvvi poca speranza di applicare con esito favorevole gli stessi principi ai casi, in cui l'esponente n prenda valori maggiori.

Il Lamé dimostrò l'impossibilità dell'equazione $x^7 + y^7 + z^7 = 0$ senza battere la stessa via seguita da altri. M. Lamé mostrato che x, y, z possono supporsi primi fra loro, dimostra un lemma importante, e cioè che il rapporto fra la somma $x + y + z$ e la radice 7^{ma} del prodotto $(x + y)(x + z)(y + z)$ o di esso moltiplicato per 7 è un quadrato perfetto; poi mediante questo lemma dimostra facilmente che è impossibile di supporre le tre incognite non divisibili per 7, ciò che si sapeva già; ed infine supponendo una delle incognite divisibili per 7, e fondandosi sul lemma, di cui si tratta, egli rimpiazza l'equazione proposta del 7^{mo} grado con un'altra equazione, di cui il 1° membro è del 4° grado, il 2° membro essendo dell'8^{vo}, e che può essere presentata sotto la forma:

$$z^4 = x^8 - 3x^4y^4 + \frac{16}{7}y^8;$$

poi egli dimostra l'impossibilità di risolvere quest'ultima equazione, col sussidio di una serie di operazioni simili a quella, che fornisce la risoluzione dell'equazione della forma: $x^2 - y^2 = A$.

Osservano Liouville e Cauchy che il lemma del Lamé è una conseguenza necessaria di questo importante teorema di analisi. " Se si sottrae la somma delle potenze n^{esime} di due incognite x, y dalla potenza n^{esima} della loro somma $x + y$, il resto sarà divisibile algebricamente non solamente pel prodotto $nxy\,(x + y)$, come lo si riconosce facilmente; ma ancora per i valori di $n > 3$ per il trinomio: $x^2 + xy + y^2 = \frac{x^3 - y^3}{x - y}$, ed anche pel quadrato di questo trinomio, allorchè $n = N_1 6 + 1$ ". Applicando questo teorema al caso, in cui si ha: $n = 3$, $n = 5$, $n = 7$, si ottengono successivamente le formole:

$$\begin{aligned}
&(x + y)^3 - x^3 - y^3 = 3xy\,(x + y),\\
&(x + y)^5 - x^5 - y^5 = 5xy\,(x + y)\,.\,(x^2 + xy + y^2),\\
&(x + y)^7 - x^7 - y^7 = 7xy\,(x + y)\,(x^2 + y^2 + xy)^2,
\end{aligned}$$

di cui l'ultima conduce subito al lemma di Lamé.

Si può abbreviare la dimostrazione del Lamé, quando si cominci a stabilire l'impossibilità di risolvere l'equazione: $z^2 = x^4 - \frac{3}{4}x^2y^2 + \frac{1}{7}y^4$, prendendo per x, y, z degli N_1 primi due a due fra loro e per y un quadrato pari. Del resto il metodo col quale ci si arriva non differisce in fondo da quello che serve a dimostrare l'impossibilità di risolvere in N_1 l'equazione $z^2 = x^4 + y^4$; e servirebbe egualmente a stabilire l'impossibilità di risolvere in N_1 un'infinità di equazioni della forma:

$$z^2 = x^4 - Ax^2y^2 + By^4.$$

Quantunque il Lamé non abbia potuto dimostrare il teorema di Fermat, che l'Accademia aveva messo al concorso del premio, tuttavia fu trovato il lavoro del Lamé buono ecc.

Post-scriptum. — Si dimostra facilmente il nuovo teorema enunciato in questo supposto, così:

Siano 1, α, β le tre radici dell'equazione $x^3 = 1$; si avrà non solo $1 + \alpha + \beta = 0$, ma ancora, supponendo n non divisibile per 3

$$1 + \alpha^n + \beta^n = 0, \tag{1}$$

e di più

$$x^2 + xy + y^2 = (x - \alpha y)(x - \beta y).$$

Ciò posto io dico che se si prende per n un Np impari e maggiore di 3, l'espressione

$$(x + y)^n - x^n - y^n \tag{2}$$

sarà divisibile pel trinomio $x^2 + xy + y^2$, ed anche pel quadrato di questo trinomio, allorchè è $n = \mathrm{N}_1 3 + 1$. Infatti per stabilire questa proposizione bisognerà far vedere che supponendo $x = \alpha y$ o $x = \beta y$ si riduce a zero l'espressione (2), e di più la sua derivata relativa ad x sarà

$$n\,[(x + y)^{n-1} - x^{n-1}], \tag{3}$$

allorchè è $n = \mathrm{N}_1 6 + 1$. Ora allorchè si suppone $x = \alpha y$, le espressioni (2) e (3) divengono

$$(1 + \alpha)^n - 1 - \alpha^n = 1 - \alpha^n + (-\beta)^n,$$
$$n\,[(1 + \alpha)^{n-1} - \alpha^{n-1}] = n\,[(-\beta)^{n-1} - \alpha^{n-1}];$$

ed è chiaro che esse si annullano: la 1ª in virtù della formula (1) per i valori dispari di n non divisibile per 3; la 2ª in virtù delle formule $\alpha^3 = 1$, $\beta^3 = 1$ per i valori dispari di n, che, divisi per 3, dànno 1 per resto.

§ VII.

Memoria di Kummer. (*)

Dimostrazione generale del teorema di Fermat, che l'equazione $x^\lambda + y^\lambda = z^\lambda$, *è irresolubile per mezzo di numeri interi, per tutte quelle potenze coll'esponente* λ, *le quali sono numeri primi dispari e non compariscono come fattori nei numeratori dei primi numeri bernoulliani* $\frac{1}{2}(\lambda - 3)$.

1. Nella memoria precedente abbiamo condotta la teoria dei numeri complessi fino al punto, che coll'aiuto di essa la dimostrazione del teorema di Fermat, sebbene non ancora perfetta in generale, pure per tutte quelle potenze, i cui esponenti soddisfano alla condizione indicata nell'enunciato, può essere fatta con facilità e sicurezza. Imperocchè arreca poca differenza che si prendano x, y, z soltanto come numeri complessi formati dalle λ^{esime} radici dell'unità; noi subito daremo la dimostrazione per i numeri complessi.

(*) V. *Journal für die reine und angewandte mathematik.* In Zwanglosen Heften-Herausgegeben von A. L. Crelle-Vierzigster Band, Berlin, 1850 (t. 20).

„ Allgemeiner Beweis des Fermatschen Satzes, dafs die Gleichung $x^\lambda + y^\lambda = z^\lambda$ durch ganze Zahlen unlösbar ist, für alle diejenigen Potenz Exponenten λ, welche ungerade Primzahlen sind und in der Zählern der ersten $\frac{1}{2}(\lambda - 3)$ Bernoullischen Zahlen als Factoren nicht vorkommen „. (Von Herrn. E. E. Kummer Professor in Breslau) pag. 130.

2. L'equazione che tratteremo sia questa

$$u^\lambda + v^\lambda + w^\lambda = 0, \tag{1}$$

dove u, v, w rappresentano veri numeri complessi. Oltre a ciò sia λ un N_p, il quale non comparisca come fattore in nessuno dei primi numeri bernoulliani $\frac{1}{2}(\lambda - 3)$.

In questa supposizione i qui citati numeri complessi hanno, secondo il teorema dimostrato nella precedente memoria: (*)

1°. La proprietà che il numero di ogni classe non equivalente non è divisibile per λ; da cui noi ricaviamo subito per la seguente dimostrazione questa notevole conclusione, che qui mai una potenza λ^{esima} di un numero complesso è uguale ad un *reale*, questo stesso numero complesso deve essere un numero reale. (Si veda la Memoria n. 16, volume 35 di questo Giornale.)

2°. In questa supposizione, conforme all'ultimo teorema della precedente memoria, ogni unità complessa, la quale per il modulo λ diventa congruente di un numero complesso reale, non è mai potenza λ^{esima} di un'altra unità.

Inoltre i numeri complessi u, v, w vengono supposti primi due a due fra loro.

3. La dimostrazione della impossibilità dell'equazione (1) si scinde ora in due parti, di cui la 1ª considera il caso, in cui dei tre numeri complessi u, v, w nessuno ha il fattore $1 - \alpha$, l'altra considera il caso in cui uno di essi è divisibile per $1 - \alpha$.

4. Sia primieramente nell'equazione

$$u^\lambda + v^\lambda + w^\lambda = 0$$

nessuno dei numeri complessi u, v, w divisibile per $1 - \alpha$.

Poichè nella data equazione compariscono soltanto le λ^{esime} potenze di u, v, w, così si può moltiplicare questi numeri complessi per arbitrarie λ^{esime} potenze dell'unità; si può così porre $\alpha^h u$ in luogo di u, dove h è un N_1, il quale, come è facile mostrare, sempre si può determinare in modo che $\alpha^h u$ assuma la forma

$$a + (1 - \alpha)^2 . P,$$

dove a è un numero intero reale e P un numero intero complesso. La stessa forma può darsi anche a v e w. Perciò qui per u, v, w debbono essere prese le seguenti forme:

$$\begin{cases} u = a + (1 - \alpha)^2 . P \\ v = b + (1 - \alpha)^2 . Q \\ w = c + (1 - \alpha^2) . R. \end{cases} \tag{2}$$

I numeri interi reali a, b, c sono in causa della supposizione, che u, v e w non debbono essere divisibili per $1 - \alpha$, non divisibili per λ. Ora scompongo la forma $u^\lambda + v^\lambda$ nei suoi fattori ed ottengo così dall'eguaglianza (1) la seguente:

$$(u + v)(u + \alpha v)(u + \alpha^2 v) \ldots (u + \alpha^{\lambda - 1} v) = - w^\lambda . \tag{3}$$

Questi λ fattori non hanno alcun divisore comune; poichè se $u + \alpha^r v$ e $u + \alpha^s v$ ne avessero uno, dovrebbero $(\alpha^r - \alpha^s) u$ e $(\alpha^r - \alpha^s) v$ avere lo stesso divisore, e poichè u e v sono numeri primi fra loro, così il divisore comune non potrebbe essere che $\alpha^r - \alpha^s$. Ma $\alpha^r - \alpha^s$ è uguale ad $(1 - \alpha)$ moltiplicato per un'unità com-

(*) Vedi § XI della presente memoria.

plessa, e questo non può essere divisore di uno di quelli λ fattori, perchè altrimenti anche w^λ e conseguentemente anche w dovrebbe essere divisibile per $1-a$.

Poichè ora tutti questi λ fattori, che compariscono al 1° membro dell'equazione (3), sono numeri primi due a due fra loro, ed il loro prodotto è eguale ad una λ^{esima} potenza, così essi debbono essere tutti eguali a λ^{esime} potenze di numeri complessi ideali, moltiplicati per alcune unità complesse. Segue così immediatamente, come per i numeri interi ordinari, dal teorema dimostrato nella Memoria n. 16, volume 35, pag. 348, che considerato nelle unità, le quali possono entrare come fattori, ogni numero complesso come prodotto dei suoi fattori primi ideali, si rappresenta in un solo unico e determinato modo. Si ottiene dunque per tutti i valori $r = 0, 1, 2 \ldots (\lambda - 1)$:

(4)
$$u + a^r v = a^q E_r(a) \,.\, t_r^\lambda\,;$$

dove t_r è un numero complesso fattore di w e $a^q E_r(a)$ un'unità della specie tale che $E_r(a) = E_r(a^{-1})$.

Ora si osserva che si scompone lo stesso, come è noto, ogni unità complessa in due fattori a^q ed $E_r(a)$, di cui soltanto uno è la λ^{esima} potenza dell'unità, l'altro ha la proprietà di rimanere invariato alla trasformazione di a in a^{-1}.

Poichè secondo l'equazione (4) t_r^λ è uguale ad un reale numero complesso, così concludiamo, secondo quello che si è sopra dimostrato, che anche t_r deve essere un numero reale complesso; e poichè ogni λ^{esima} potenza di un reale numero complesso, come si sa, è congruente ad un numero intero reale per il modulo λ, così pongo

$$t_r^\lambda \equiv m \pmod{\lambda},$$

dove m è un N_1. L'equazione (4) si muta perciò nella congruenza:

(5)
$$u + a^r v \equiv a^q \,.\, E_r(a)\, m \pmod{\lambda}.$$

Ora si muti a in a^{-1}, onde u si trasforma in u', v in v', w in w', così è:

(6)
$$u' + a^{-r} v' \equiv a^{-q} E_r(a)\, m \pmod{\lambda};$$

eliminando dalle congruenze (5) e (6) la m si ha:

(7)
$$a^{-q}(u + a^r v) \equiv a^q (u' + a^{-r} v') \pmod{\lambda}.$$

Se si prende ora invece del modulo λ il modulo $(1-a)^2$, il quale è un divisore di λ, e si osserva che secondo le equazioni (2):

$$u \equiv a \quad , \quad v \equiv b \quad , \quad u' \equiv a \quad , \quad v' \equiv b \quad [\text{mod. } (1-a)^2],$$

si ottiene:

(8)
$$a^{-q}(a + a^r b) \equiv a^q (a + a^{-r} b) \pmod{(1-a)^2};$$

e poichè generalmente $a^h \equiv 1 - h(1-a) \pmod{(1-a)^2}$, così questa congruenza si muta nella seguente:

$$2(a+b)\, q \equiv 2br \pmod{(1-a)}.$$

Poichè ora i numeri reali interi che sono divisibili per $1-a$ devono anche essere divisibili per λ, così ne viene:

(9)
$$(a+b)\, q \equiv br \pmod{\lambda}.$$

Se ora si chiama con k quell'N_1, che basta alla congruenza:

(10) $$(a+b)k \equiv b \pmod{\lambda}:$$

k è indipendente da r e $q \equiv k.r$, così dà la congruenza:

(11) $$a^{-kr}(u + a^r v) \equiv a^{+kr}(u' + a^{-r} v') \pmod{\lambda}.$$

Pel caso speciale di $r = 0$, poichè non può essere
$$a + b \equiv 0 \pmod{\lambda},$$
dalla congruenza (9) si ha:
$$q \equiv 0 \pmod{\lambda};$$
così:

(12) $$u + v \equiv u' + v' \pmod{\lambda};$$

e poichè u, v, w della data equazione
$$u^\lambda + v^\lambda + w^\lambda = 0$$
possono essere arbitrariamente trasformati, così è anche:

(13) $$\left\{\begin{array}{l} u + w \equiv u' + w' \\ v + w \equiv v' + w' \end{array}\right\} \pmod{\lambda};$$

dalle quali si hanno le tre più semplici:

(14) $$\left\{\begin{array}{l} u \equiv u' \\ v \equiv v' \\ w \equiv w' \end{array}\right\} \pmod{\lambda}.$$

Perciò la congruenza (11) per ogni valore arbitrario di r si trasforma nella seguente:

(15) $$a^{kr}(u + a^r v) \equiv a^{kr}(u + a^{-r} v) \pmod{\lambda},$$

o in:

(15)' $$u(a^{kr} + a^{-kr}) + v(a^{(k-1)r} - a^{-(k-1)r}) \equiv 0 \pmod{\lambda}.$$

Faccio in quest'ultimo $r = 1$ e $r = 2$, ed ottengo:

(16) $$\left\{\begin{array}{l} u(a^k - a^{-k}) + v(a^{(k-1)} - a^{-(k-1)}) \equiv 0 \\ u(a^{2k} - a^{-2k}) + v(a^{2(k-1)} - a^{-2(k-1)}) \equiv 0 \end{array}\right\} \pmod{\lambda}.$$

E se si moltiplica la 1ª di queste congruenze per $a^k + a^{-k}$ e da essa poi si sottrae la 2ª, e quindi la ottenuta si divide per v, il quale non è divisibile per $1 - a$, pure primo con λ, si ottiene:
$$(a^k + a^{-k})[a^{(k-1)} - a^{-(k-1)}] + a^{2(k-1)} - a^{-2(k-1)} \equiv 0 \pmod{\lambda};$$
ossia:
$$(a^{k-1} - a^{-(k-1)})(a^{+k} + a^{-k} - a^{k-1} - a^{-(k-1)}) \equiv 0 \pmod{\lambda};$$
e quindi:

(17) $$(a^{k-1} - a^{-(k-1)})(a^{-k} - a^{k-1})(1-a) \equiv 0 \pmod{\lambda}.$$

Se ora nessuno di questi tre fattori:
$$a^{k-1} - a^{-(k-1)}\ , \quad a^{-k} - a^{k-1}\ , \quad 1 - a$$

per sè è uguale a zero, il prodotto di essi contiene tre volte il fattore $(1-a)$; ma esso dovrebbe contenerlo tante volte, quante sono le λ, così $\lambda-1$ volte, affinchè la congruenza realmente abbia luogo. Coll'esclusione del caso unico $\lambda=3$, questa congruenza non può aver luogo, se non è:

$$(18) \qquad \begin{cases} a^{k-1} - a^{-(k-1)} = 0 \text{ oppure} \\ a^{-k} - a^{k-1} \quad = 0. \end{cases}$$

Così deve essere o $k \equiv 1$ o $2k \equiv 1 \pmod{\lambda}$.

Ma il primo caso $k \equiv 1$ darebbe per conseguenza la congruenza:

$$(10) \qquad a \equiv 0 \pmod{\lambda};$$

e perciò non può aver luogo. Il secondo caso $2k \equiv 1$ darebbe luogo alla congruenza:

$$(10) \qquad a \equiv b \pmod{\lambda};$$

da cui segue, mercè semplice sostituzione di lettere, che deve essere anche:

$$a \equiv c \quad \text{e} \quad b \equiv c \pmod{\lambda}.$$

Ma dall'equazione:

$$u^\lambda + v^\lambda + w^\lambda = 0$$

segue, secondo le (2) accettate espressioni di u, v, w, che deve essere anche:

$$a^\lambda + b^\lambda + c^\lambda \equiv 0 \pmod{\lambda};$$

così anche:

$$a + b + c \equiv 0 \pmod{\lambda};$$

e poichè a, b, c sono congruenti, si ha infine $3a \equiv 0 \pmod{\lambda}$, il quale con eccezione del già escluso caso $\lambda=3$, è pure impossibile, poichè secondo la supposizione u non contiene il fattore $1-a$, e così anche a non può essere divisibile per λ.

Con ciò la prima parte della dimostrazione è data compiutamente, colla quale viene provato che l'equazione:

$$u^\lambda + v^\lambda + w^\lambda = 0,$$

se nessuno dei numeri complessi u, v, w contiene il fattore $1-a$, trae seco pel modulo λ una congruenza impossibile, con eccezione del caso di $\lambda=3$, che qui non vogliamo particolarmente considerare.

5. Sia secondariamente nell'equazione:

$$u^\lambda + v^\lambda + w^\lambda = 0$$

uno dei tre numeri u, v, w divisibile per $1-a$; e sia il numero w; questo può contenere il fattore $(1-a)$ anche parecchie volte; allora si pone $(1-a)^m w$ in luogo di w, così che ora w non può più contenere il fattore $1-a$; così si è condotti a studiare l'equazione:

$$u^\lambda + v^\lambda + (1-a)^{m\lambda} . w^\lambda = 0.$$

In luogo di questa io considero quest'altra un po' più generale:

$$(19) \qquad u^\lambda + v^\lambda = \mathrm{E}(a) . (1-a)^{m\lambda} . w^\lambda,$$

nella quale $\mathrm{E}(a)$ è un'unità complessa arbitraria. Scomponendo in fattori l'espressione $u^\lambda + v^\lambda$ si ottiene:

$$(20) \qquad (u+v)(u+av)(u+a^2v)\ldots(u+a^{\lambda-1}v) = \mathrm{E}(a)(1-a)^{m\lambda} . w^\lambda.$$

I l'λ fattori $u+v, u+av \dots u+a^{\lambda-1}v$, hanno tutti il maggior divisore comune $1-a$; all'infuori di questo, due di essi non hanno forse nessun divisore comune. Parimente, se si prende per u e v di nuovo, come sopra, le forme:

$$u = a + (1-a)^2 . \mathrm{P} \quad \text{e} \quad v = t + (1-a)^2 . \mathrm{Q},$$

si ottiene:

(21) $$u + a^r . v \equiv a + b - r\,b\,(1-a) \ (\text{mod. } (1-a)^2);$$

ma $u + a^r v$ per un valore almeno di r deve essere divisibile per $1-a$, perchè il prodotto di tutti questi fattori è divisibile per $(1-a)^{m\lambda}$; per conseguenza anche per λ, e la congruenza (21) diviene

(22) $$u + a^r v \equiv r . b\,(1-a) \ (\text{mod. } (1-a)^2);$$

da cui innanzi tutto segue che per ogni valore di r la $u+a^r v$ deve contenere il fattore $1-a$, in luogo del quale anche il fattore $1-a^r$, che differisce da questo solo per un'unità complessa, la quale vi entra come fattore; inoltre che $u+a^r v$ può contenere questo fattore $1-a^r$ oppure $1-a$ soltanto una volta con eccezione del caso $r=0$. Ma la quantità $u+v$ contiene veramente il fattore $1-a$ parecchie volte; ma in virtù dell'equazione (20) lo contiene esattamente $m\nu - \lambda + 1$ volte, mentre i rimanenti $\lambda - 1$ fattori lo contengono ciascuno una volta, ed il prodotto di tutti questi fattori $m\lambda$ volte.

Ora si pone:

(23) $$u + v = (1-a)^{m\lambda-\lambda+1} . \varphi$$

e

(24) $$u + a^r v = (1-a^r) . \varphi_r;$$

così l'equazione (20) si trasforma nella seguente

(25) $$\varphi . \varphi_1 . \varphi . \varphi_2 . - \varphi_{n-1} = \mathrm{E}(a) . w^\lambda;$$

e i fattori $\varphi, \varphi_1, \varphi_2 \dots \varphi_{n-1}$, i quali sono primi due a due fra loro, ed il cui prodotto è uguale ad una λ^{esima} potenza moltiplicata per un'unità, devono essere tutti le stesse λ^{esime} potenze moltiplicate per un'unità. Secondo ciò si può porre

$$\varphi = e(a)\, w_1^\lambda \quad \text{e} \quad \varphi_r = e_r(a)\, t_r^\lambda;$$

da cui:

(26) $$u + v = e(a)\,(1-a)^{m\lambda-\lambda+1} . w_1^\lambda$$

e

(27) $$u + a^r . v = e_r(a) . (1-a^r)\, t_r^\lambda$$

per tutti i valori $r = 1, 2, 3 \dots \lambda - 1$.

I numeri complessi w_1 e t_r sono qui parimente soltanto numeri reali complessi, perchè le λ^{esime} potenze di essi sono reali numeri complessi. Se si dà alla r un altro valore s, si ottiene

(28) $$u + a^s v = e_s(a) . (1-a^s) . t_s^\lambda;$$

e se dalle equazioni (26), (27), (28) si eliminano u e v si ottiene

(29) $$e_r(a) . t_r^\lambda - e_s(a)\, t_s^\lambda = \frac{e(a^s - a^r)(1-a)}{(1-a^r)(1-a^s)} . (1-a)^{(m-1)\lambda} . w_1^\lambda .$$

Se si divide per $e_r(a)$ e si pone

$$\frac{-e_s(a)}{e_r(a)} = \varepsilon(a), \quad \frac{e(a).(a^r - a^s)(1-a)}{e_r(a)(1-a^r)(1-a^s)} = E_1(a)$$

e dove $\varepsilon(a)$ ed $E_1(a)$ sono parimente unità complesse, così si ottiene

$$t_r^\lambda + \varepsilon(a)\, t_s^\lambda = E_1(a)(1-a)^{(m-1)\lambda} \,.\, w_1^\lambda \,. \tag{30}$$

Se ora $m > 1$, come è noto, è $(1-a)^{(m-1)\lambda} \equiv 0 \pmod{\lambda}$.

Oltre a ciò poichè t_r e t_s sono reali numeri complessi, le λ^{esime} potenze degli stessi numeri reali interi debbono essere congruenti rispetto al modulo λ, così deve essere

$$t_r^\lambda \equiv c \quad \text{e} \quad t_s^\lambda \equiv k \pmod{\lambda}.$$

L'equazione (30) dà quindi la congruenza seguente

$$c + \varepsilon(a) \,.\, k \equiv 0 \pmod{\lambda};$$

dalla quale segue che l'unità $\varepsilon(a)$ è congruente ad un numero intero reale rispetto al modulo λ; e così $\varepsilon(a)$ deve essere una λ^{esima} potenza di un'altra unità; perciò $\varepsilon(a) = \varepsilon_1(a)^\lambda$.

Se ora si pone $\varepsilon_1(a) \,.\, t_s = v_1$ ed in luogo di t_r il segno u_1, l'equazione (30) si muta nella seguente

$$u_1^\lambda + v_1^\lambda = E_1(a) \,.\, (1-a)^{(m-1)\lambda} \,.\, w_1^\lambda \,. \tag{31}$$

Ma questa equazione è per la forma perfettamente eguale all'equazione (19), dalla quale è derivata, e differisce da essa soltanto perciò che m è diminuita di un'unità. Se si adopera lo stesso metodo sull'equazione (31) si ottiene di nuovo da essa un'equazione della stessa forma, nella quale m è minore di due unità, che nell'equazione (19), e così via. Colla ripetizione di questo procedimento si giunge sempre ad un'equazione della stessa forma della (19), nella quale è $m=1$; ma arrivati a quest'ultima, poi il metodo che richiede, come sopra si è detto, $m > 1$, non è più servibile. Si ottiene così un'equazione dalla forma

$$u^\lambda + v^\lambda = E(a)(1-a)^\lambda \,.\, w^\lambda \,. \tag{32}$$

L'impossibilità di questa equazione si dimostra facilmente, se verrà dimostrato questo: se la forma $u^\lambda + v^\lambda$ contiene sovratutto il fattore $1-a$, essa lo deve contenere almeno $(\lambda + 1)$ volte. Per dimostrare ciò pongo per u e v, come sopra, di nuovo le forme

$$u = a + (1-a)^2 \,.\, P \quad , \quad v = b + (1-a)^2 \,.\, Q;$$

così si ottiene di nuovo

$$u + a^r v \equiv a + b - rb(1-a) \pmod{(1-a)^2}. \tag{33}$$

Poichè ora $u^\lambda + v^\lambda$ è divisibile per $1-a$, e perciò anche uno almeno dei fattori di questa espressione, i quali tutti hanno la forma: $u + a^r v$, deve essere divisibile per $1-a$, così ne segue che $a+b$ è divisibile per $1-a$, e quindi anche per λ. Allora la congruenza (33) si trasforma come sopra nella seguente

$$u + a^r v \equiv rt(1-a) \pmod{(1-a)^2}. \tag{34}$$

Così tutti i fattori della forma

$$u^\lambda + v^\lambda = (u+v)(u+\alpha v)(u+\alpha^2 v)\dots(u+\alpha^{\lambda-1} v)$$

sono divisibili per $1-\alpha$; ma il fattore $u+v$ è divisibile per $(1-\alpha)^2$; perciò il numero di tutti i fattori $1-\alpha$ contenuti in $u^\lambda + v^\lambda$ è almeno uguale a $\lambda+1$, ciò che dovevasi dimostrare.

Così l'equazione (32), nella quale w non è divisibile per $1-\alpha$, contiene in sè la contraddizione, che il primo membro di essa è divisibile per $(1-\alpha)^{\lambda+1}$, mentre il 2° membro non lo è. Quindi l'equazione (32) è impossibile, e perciò anche l'equazione (19), dalla quale essa è derivata, è impossibile; in questo modo chiamasi un'equazione, la quale non si possa in alcun modo soddisfare mediante numeri interi complessi

6. L'equazione

$$u^\lambda + v^\lambda + w^\lambda = 0$$

è dunque impossibile in entrambi i casi, tanto se nessuno dei numeri complessi u, v, w è divisibile per $1-\alpha$, quanto se anche uno di essi viene preso divisibile per $1-\alpha$. Perciò il teorema di Fermat è dimostrato non solo per numeri reali interi, ma altresì per numeri interi complessi, formati da λ^{esime} radici delle unità, per tutte quelle potenze, i cui esponenti λ sono degli N_p, ed i quali soddisfano alla condizione, che non compariscono in nessuno dei primi numeri bernoulliani $\frac{1}{2}(\lambda-3)$ come fattori del numeratore.

Poichè $\lambda = 5, 7, 11, 13, 17, 19, 23, 29, 31, 41, 43$ adempiono a questa condizione, così il teorema di Fermat è dimostrato per tutti questi esponenti. Ma per $\lambda = 37$ la data condizione non è soddisfatta: e quindi il teorema di Fermat non è dimostrato per l'esponente 37 e per gli esponenti $37 . n$.

Le mie presenti cognizioni sulla teoria dei numeri complessi non mi hanno ancora fornito il mezzo di poter dimostrare la non solubilità o la solubilità dell'equazione di Fermat per i rimanenti numeri primi, i quali non soddisfano alla data condizione.

§ VIII.

Memorie di Eulero. (*)

1. Al capitolo XIII dell'algebra di Eulero pag. 242 si ha:

" De quelques expressions de la forme $ax^4 + by^4$, qui ne sont pas réductibles à des carrés ".

In questo capitolo Eulero incomincia a dimostrare che $x^4 + y^4$ non può essere eguale ad un quadrato z^2 e poi dimostra che è pure impossibile che $x^4 - y^4$ sia eguale ad un quadrato z^2; siccome le dimostrazioni che egli ne dà sono in sostanza le stesse di quelle che abbiamo vedute più innanzi, crediamo conveniente di ometterle.

(*) Vedi *Éléments d'algèbre* par M. LÉONARD EULER, traduits de l'allemand, tome second. Lyon et Paris, 1774.

2. Nello stesso capitolo XIII a pag. 243 Eulero dimostra questo teorema:

" Il n'est pas possible de trouver deux cubes, dont la somme ou bien la différence soit une cube ".

La dimostrazione di questo teorema è identica a quella data dal Legendre, che noi abbiamo riportata nel § IX della presente memoria, quindi è inutile di qui riportarla.

§ IX.

Memoria 2ª di Legendre. (*)

" *Recherches sur quelques objets d'analyse indéterminée et particulièrement sur le théorème de Fermat* ".

1. Qui non riporteremo di questa memoria che la parte, la quale ha stretta attinenza coll'ultimo teorema di Fermat.

2. Quantunque la teoria dei numeri sia ora di molto progredita rispetto ai tempi di Fermat, tuttavia ancora rimane da dimostrare una proposizione scoperta da questo scienziato e cioè:

" Cubum autem in duos cubos, aut quadrato-quadratum in duos quadratos, et generaliter nullam in infinitum ultra quadratum, potestatem in duos ejusdem nominis fas est dividere, cujus rei demostrationem mirabilem sane detexi. Hanc marginis exiguitas non caperet ". FERMAT, *Notes sur Diophante,* pag. 61. Queste ultime parole autorizzano a credere che la dimostrazione, di cui parla il Fermat, non avrebbe occupato che un picciol numero di pagine, se la si avesse a nostra disposizione. Questa dimostrazione era dunque assai più semplice di quella, di cui noi ci serviamo in questo scritto per dimostrare solamente che la soluzione, se ve ne è una nei casi non risolti, non potrebbe essere data che per numeri di una grandezza prodigiosa.

Il caso delle terze potenze è stato dimostrato da Eulero e quello delle quarte lo è stato dimostrato egualmente con un metodo, che Fermat stesso aveva sufficientemente indicato; ma non si è andati al di là; e quantunque l'Accademia delle Scienze di Francia, a fine di onorare la memoria di Fermat, avesse proposto per soggetto di uno dei suoi premi di Matematiche, la dimostrazione del teorema suddetto, e quantunque avesse prorogato il limite di questo concorso al di là del termine ordinario, pur tuttavia non si ottenne lo scopo che l'Accademia si riprometteva.

Adunque sembra che una difficoltà particolare sia inerente a tale quistione e che non si conosca ancora il principio speciale, che sarebbe necessario per risolverla. Aspettando che un caso fortunato faccia ritrovare questo principio, tale quale Fermat lo aveva conosciuto, i cultori della teoria dei numeri vedranno forse con piacere che il caso delle quinte potenze può essere rigorosamente dimostrato. Ora esporremo questa dimostrazione, facendola precedere da alcune considerazioni generali intorno alle condizioni, alle quali dovrebbero soddisfare le tre incognite, se la soluzione fosse possibile. Una di queste condizioni è che l'esponente della potenza, od anche il suo quadrato, sia divisore di una delle incognite; e si osser-

(*) *Mémoires de l'académie royale des sciences de l'institut de France,* tome VI. Paris, 1823.

verà che questa semplice condizione, facile a dimostrarsi per piccoli valori dell'esponente, diviene un problema difficile e non risolto, allorchè si vuole estenderlo ad un esponente qualunque.

3. Ora si tratta di dimostrare che l'equazione

$$x^n + y^n + z^n = 0,$$

ove n è un Np maggiore di 2, è impossibile in N_1, salvo il caso evidente in cui uno qualunque dei numeri x, y, z fosse nullo. Per semplicità si suppongono i numeri x, y, z, i cui valori ed i cui segni sono indeterminati, primi due a due fra loro; e perciò due di essi saranno degli $N_1 2 + 1$ ed il terzo un $N_1 2$.

4. Teorema. — *Sia* $x + y + z = p$, *io dico che* p *è un* $N_1 n$.

Dimostrazione. — Infatti essendo n un Np, la quantità $x^n - x$ è un $N_1 n$, e così $y^n - y$, $z^n - z$ sono degli $N_1 n$; dunque la loro somma

$$(x^n - x) + (y^n - y) + (z^n - z) = x^n + y^n + z^n - (x + y + z) = -p$$

è un $N_1 n$.

5. Teorema. — *Io dico ora che* p^n *è divisibile pel prodotto* $(x+y)(y+z)(z+x)$, *sicchè si potrà porre*

$$p^n = (x + y)(y + z)(z + x) . P,$$

ove P *è un polinomio in* x, y, z *omogeneo del* $(n-3)^{mo}$ *grado.*

Dimostrazione. — Essendo n un $N_1 2 + 1$ qualunque, $p^n - z^n$ è sempre divisibile per $p - z$ ossia per $x + y$; e così pure $x^n + y^n$ è divisibile per $x + y$; dunque $p^n - z^n - x^n - y^n$ o semplicemente p^n è divisibile per $x + y$. Analogamente si dimostra che p^n è divisibile per $y + z$ e per $z + x$. Dunque se n è un $N_1 2 + 1$ qualunque, p^n è divisibile pel prodotto $(x + y)(y + z)(z + x)$ ecc.

6. Se si suppone che uno dei numeri x, y, z non sia un $N_1 n$, bisognerà pure che nessuna delle $x + y$, $y + z$, $z + x$ non sia un $N_1 n$, poichè se per es. $x + y$ fosse un $N_1 n$, la differenza $p - (x + y) = z$ sarebbe un $N_1 n$; il che è contro l'Hp.

7. Supponiamo che uno dei numeri x, y, z, per es. x, sia un $N_1 n$, allora $y + z$ non solo è un $N_1 n$ ma è un $N_1 n^{n-1}$. Infatti poichè si ha $x^n + y^n + z^n = 0$, bisogna che $y^n + z^n$ sia un $N_1 n^n$; ma $y^n + z^n$ è il prodotto di $y + z$ pel polinomio $y^{n-1} - zy^{n-2} + z^2 y^{n-3} - \ldots$; e se si fa in questo polinomio $y + z = 0$ ossia $z = -y$, esso diviene ny^{n-1}; dunque, siccome y non è un $N_1 n$, poichè x ed y son primi fra loro, il polinomio sarà divisibile per n semplicemente e non per una potenza più elevata di n. Dunque $y + z$ sarà divisibile per n^{n-1}. In generale se x fosse divisibile per n^a, e $y + z$ sarebbe divisibile per n^{na-1} e P semplicemente per n.

Osservazione. — Da ciò risulta che facendo $y^n + z^n = (y + z)\varphi(y, z)$, i fattori $y + z$ e $\varphi(y, z)$ avranno n per divisor comune o non ne avranno nessuno, secondo che x è o non è un $N_1 n$.

8. Consideriamo dapprima il caso, in cui l'uno dei tre numeri x, y, z sia un $N_1 n$, e sia x questo numero; allora facendo $y^n + z^n = (y + z)\varphi(y, z) = (-x)^n$; e siccome questi due fattori $y + z$, $\varphi(y, z)$ non possono avere che n per divisore, come risulta dall'Oss. del n. 7, bisognerà che $n(y + z)$ e $\frac{1}{n}\varphi(y, z)$ siano l'uno e l'altro delle potenze n^{esime}, il cui prodotto sarà eguale a $(-x)^n$; perciò faremo in generale $y + z = \frac{1}{n}a^n$, a essendo un $N_1 n$ o un $N_1 n^a$ e $\varphi(y, z) = n\alpha^n$, ciò che suppone $x = -a\alpha$, e di più α primo con $n\alpha$.

Analogamente si avrà, non essendo y e z degli $N_1 n$:

$$z + x = b^n,\ \varphi(z, x) = \beta^n,\ y = -b\beta \quad \text{e} \quad x + y = c^n,\ \varphi(x, y) = -\gamma^n,\ z = -c\gamma.$$

Si avrà dunque ad un tempo le nove equazioni:

$$\begin{cases} y + z = \frac{1}{n} a^n, & \varphi(y, z) = n\alpha^n, & x = -a\alpha, \\ z + x = b^n, & \varphi(z, x) = \beta^n, & y = -b\beta, \\ x + y = c^n, & \varphi(x, y) = \gamma^n, & z = -c\gamma. \end{cases}$$

E si ha

$$2p = \frac{1}{n} a^n + b^n + c^n;$$

e si avrà quindi

$$x = p - \frac{1}{n} a^n = \frac{1}{2}\left(b^n + c^n - \frac{1}{n} a^n\right);$$
$$y = p - b^n = \frac{1}{2}\left(c^n + \frac{1}{n} a^n - b^n\right);$$
$$z = p - c^n = \frac{1}{2}\left(\frac{1}{n} a^n + b^n - c^n\right).$$

9. Esiste pure una relazione fra a, b, c, la quale si dedurrà dall'equazione

$$2p = \frac{1}{n} a^n + b^n + + c^n,$$

combinata colla equazione

$$0 = \left(p - \frac{1}{n} a^n\right)^n + (p - b^n)^n + (p - c^n)^n.$$

Si sa d'altra parte che p^n è un $N_1 n (y + z)(z + x)(x + y)$ o un $N_1 abc$; dunque si può porre $p = abcD$; quindi si avrà

$$2abcD = \frac{1}{n} a^n + b^n + c^n.$$

E collo sviluppo dell'equazione precedente si otterrà in ciascun caso particolare un'altra equazione fra a, b, c, D ecc.

10. Se supponiamo ora che nessuno dei numeri x, y, z sia un $N_1 n$; allora il solo cambiamento da farsi nelle nove equazioni del n. 8 sarà di $\frac{1}{n} a^n$ in a^n e $n\alpha^n$ in α^n; ma si vedrà che questo caso non può aver luogo.

11. Se una delle indeterminate x, y, z è un $N_1 n$, io dico che è necessariamente anche un $N_1 n^2$, e così pure p sarà un $N_1 n^2$.

Infatti essendo x la indeterminata che è un $N_1 n$, ed avendosi

$$2p = \frac{1}{n} a^n + b^n + c^n,$$

in cui $2p$ e $\frac{1}{n} a^n$ sono degli $N_1 n$, occorre che $b^n + c^n$ sia un $N_1 n$. D'altra parte $b^n - b$, $c^n - c$ essendo sempre degli $N_1 n$, la loro somma $b^n + c^n - (b + c)$ è un $N_1 n$; dunque $b + c$ è pure un $N_1 n$. Sia $b + c = n$A, si avrà

$$b^n = (-c + nA)^n,$$

e

$$b^n + c^n = nc^{n-1} . nA - \frac{n(n-1)}{1} c^{n-1} . n^2A^2 + \text{etc.};$$

da cui si vede che $b^n + c^n$ è sempre un $N_1 n^2$. Ma la parte $\frac{1}{n} a^n$ è pure un $N_1 n^2$ nel caso di $n = 3$ e per una potenza più elevata di n, allorchè è $n > 3$. Dunque sarà sempre $p - \frac{1}{n} a^n$ un $N_1 n^2$ ossia x sarà un $N n^2$.

12. Ora mostreremo che una delle incognite x, y, z è necessariamente un $N_1 n$. (*)

Avendo già posto $p = x + y + z$, facciamo ora $q = xy + yz + zx$, $r = xyz$, di maniera che le incognite x, y, z sono le radici dell'equazione

$$V^3 - pV^2 + qV - r = 0;$$

ora si ha

$$S_1 = p; \qquad S_2 = p^2 - 2q; \qquad S_3 = p^3 + 3(r - pq),$$

ed in generale

$$S_m = p^m - mqp^{m-2} + mrp^{m-3} + \frac{m(m-3)}{2} q^2p^{m-4} - \frac{m(m-4)}{2} . 2qrp^{m-5}$$
$$+ \frac{m(m-5)}{2} r^2p^{m-6} - \frac{m(m-4)(m-5)}{2.3} q^3p^{m-6} + \frac{m(m-5)(m-6)}{2.3} . 3q^2rp^{m-7}$$
$$- \frac{m(m-6)(m-7)}{2.3} . 3qr^2p^{m-8} + \frac{m(m-7)(m-8)}{2.3} r^3p^{m-9} + \text{etc.},$$

questa serie dovendo essere prolungata sino alle potenze negative di p esclusivamente.

1°. Sia $n = 3$; si ha $S_3 = 0$, quindi si ha

$$p^3 = 3(pq - r) = 3(x + y)(y + z)(z + x);$$

dunque p è divisibile per 3, e di più uno dei fattori $x + y$, $y + z$, $z + x$ sarà un $N_1 9$; sia questo $y + z$, allora $p - (y + z) = x$ è un $N_1 3$; di più si può concludere, pel n. 11, che x è un $N_1 9$ come p.

2°. Sia $n = 5$; si ha $S_5 = 0$, la quale dà

$$p^5 = 5(pq - r)(p^2 - q),$$

ovvero

$$p^5 = 5(x + y)(y + z)(z + x)\frac{p^2 + x^2 + y^2 + z^2}{2}.$$

Se nessuno dei fattori $x+y$, $y+z$, $z+x$ è un $N_1 5$, bisognerà che $p^2+x^2+y^2+z^2$ o la parte $x^2 + y^2 + z^2$ sia un $N_1 5$. Ma ogni numero non un $N_1 5$ è delle forme $5m \pm 1$, $5m \pm 2$, ed il suo quadrato della forma $5m \pm 1$; ora tre N_1 della forma $5m \pm 1$ avranno la somma delle forme $5m \pm 1$, $5m \pm 3$; dunque è impossibile che $x^2 + y^2 + z^2$ sia un $N_1 5$, se non lo è nessuno delle x, y, z. Dunque in questo caso una delle indeterminate è un $N_1 5$, ed è ad un tempo un $N_1 25$ come p.

Questi due ultimi casi possono essere dimostrati anche così:

1°. Un cubo non un $N_1 3$ è delle forme $9m \pm 1$; ora tre dei resti ± 1, non possono fare nè la somma zero, nè la somma 9; dunque se si può soddisfare in N_1 all'equazione $x^3+y^3+z^3=0$, una delle tre indeterminate sarà necessariamente un $N_1 3$.

2°. La 5ª potenza di ogni N_1, che non è un $N_1 5$, ha necessariamente una delle quattro forme $25m \pm (1,7)$, ciò che si può verificare sulle quinte potenze dei

(*) Osservazione. — Se per es. x è un $N_1 n$ ed n è un Np, ne consegue che è $y \equiv z$ (mod. n).

D. Gambioli.

numeri 1, 2, 3, 4, che divise per 25, dànno gli stessi resti, che darebbero le quinte potenze dei numeri $5x+1$, $5x+2$, $5x+3$, $5x+4$. Ora tre dei quattro resti ± 1, ± 7 non possono fare nè la somma zero, nè la somma 25. Dunque se l'equazione $x^5+y^5+z^5=0$ è risolubile in N_1, bisognerà che una delle indeterminate sia un $N_1 5$ ecc.

In generale un tal principio si dimostra così:

Supponiamo che si abbia $x^n+y^n+z^n=0$ e θ sia un Np non divisore di xyz; poichè x e θ^n sono primi fra loro, si può supporre $y=fx+\theta^n y'$, $z=gx+\theta^n z'$; e facendo la sostituzione si vedrà che $1+f^n+g^n$ è divisibile per θ^n, o che sopprimendo i multipli di θ^n, si ha $(-g^n)=f^n+1$; dunque fra i resti delle potenze n^{esime} divise per θ^n, ve ne sarà sempre una, proveniente da $(\theta-g)^n$ o da $(-g)^n$, che supererà di un'unità il resto proveniente da f^n. Se questa condizione non si verifica nella serie dei resti, si deve concludere che vi è necessariamente uno dei numeri x, y, z divisibile per θ.

13. Dell'equazione $x^5+y^5+z^5=0$.

a) Poichè una delle indeterminate deve essere un $N_1 5$ ed un $N_1 25$, sia x questa indeterminata, e si troverà come al n. 8, che l'equazione $y^5+z^5=-x^5$ si scinde necessariamente in due altre di questa forma:

$$(1)\qquad \begin{cases} y+z=5^4 t^5 \\ y^4-y^3z+y^2z^2-yz^3+z^4=5r^5, \end{cases}$$

ciò che suppone $x=-5tr$, r essendo un $N_1 2+1$, positivo e primo con $5t$. Ciò posto, vi sono due casi da considerare: secondo che x è un $N_1 2$ o un $N_1 2+1$.

1° caso, in cui x è un $N_1 2$.

b) Allora t è un $N_1 2$, y e z sono degli $N_1 2+1$, e la 2ª dell'equazioni (1) si potrà mettere sotto la forma:

$$5\left(\frac{y^2+z^2}{2}\right)^2-\left(\frac{y^2+2yz+z^2}{2}\right)^2=5r^5.$$

Dividendo per 5 e mettendo in luogo di $y^2+2yz+z^2$ il suo valore $5^8 t^{10}$, si avrà:

$$\left(\frac{y^2+z^2}{2}\right)^2-5\left(\frac{5^7 t^{10}}{2}\right)^2=r^5.$$

Nella nostra Hp $\frac{1}{2}(y^2+z^2)$ e $\frac{1}{2}\cdot 5^7\cdot t^{10}$ sono degli N_1; d'altronde poichè il 1° membro è della forma p^2-5q^2, il suo divisore r dovrà essere della forma stessa, sicchè si potrà fare $r=f^2-5g^2$; poi facendo $(f+g\sqrt{5})^5=F+G\sqrt{5}$, ciò che dà:

$$F=f(f^4+50f^2g^2+125g^4)$$
$$G=5g(f^4+10f^2g^2+5g^4),$$

si avrà $r^5=F^2-5G^2$, e per conseguenza:

$$\left(\frac{y^2+z^2}{2}\right)^2-5\left(\frac{5^7 t^{10}}{2}\right)=F^2-5G^2.$$

Per ottenere una soluzione generale di questa equazione, bisognerà prendere due numeri m ed n tali che si abbia: $(y\pm 4\sqrt{5})^k=m+n\sqrt{5}$, k essendo un N_1;

questi N_1 soddisferanno in generale l'equazione $m^2 - 5n^2 = 1$; e si potrà supporre:

$$\frac{y^2+z^2}{2} + \frac{5^7 t^{10}}{2}\sqrt{5} = (F + G\sqrt{5})(m + n\sqrt{5});$$

ciò che darà:

$$\frac{1}{2}\cdot(y^2+z^2) = mF + 5nG,$$
$$\frac{1}{2}\cdot 5^7 t^{10} = mG + nF.$$

c) Queste formole contengono un'infinità di soluzioni, poichè si può prendere per k un N_1 qualunque; ma queste soluzioni in numero infinito sono solamente suscettibili di cinque forme diverse. Infatti, qualunque sia l'esponente k, sarà sempre di una delle cinque forme: $5i$, $5i \pm 1$, $5i \pm 2$. Ma osservasi che la parte indeterminata $5i$ può sopprimersi, essendo compresa nell'espressione di r^5; poichè si può fare: $(f + g\sqrt{5})(9 \pm 3\sqrt{5}) = f' + g'\sqrt{5}$, e si avrà di nuovo $r = f'^2 - 5g'^2$; sicchè basterà di mettere f' e g' in luogo di f e g nei valori di F e G. Quindi non resta che a considerare i cinque valori $k = 0, \pm 1, \pm 2$, ai quali corrispondono per m ed n i valori seguenti:

$$m = 1,\quad 9,\quad 161;\qquad n = 0,\quad \pm 4,\quad \pm 72.$$

d) Si osserva ancora che nell'equazione $\frac{1}{2}\cdot 5^7\cdot t^{10} = mG + nF$, ove G è sempre un $N_1 5$, il termine nF non può essere un $N_1 5$ se non lo è n; poiche r essendo primo con $5t$, ed il suo valore essendo $f^2 - 5g^2$, f non può essere un $N_1 5$, e per conseguenza F non può essere un $N_1 5$. Dunque dei cinque valori di n, non si può ammettere che il valore $n = 0$, che corrisponde ad $m = 1$; ciò che darà per sola soluzione ammissibile:

$$\frac{1}{2}\cdot 5^7\cdot t^{10} = G = 5g(f^4 + 10f^2 g^2 + 5g^4)$$

o

$$\frac{1}{2}\cdot 5^6\cdot t^{10} = g(f^4 + 10f^2 g^2 + 5g^4).$$

In questa equazione i due fattori del 2° membro sono primi fra loro, ed è necessario supporre g un $N_1 2$; poichè se g fosse un $N_1 2 + 1$, f dovrebbe essere un $N_1 2$, ed il 2° membro della nostra equazione sarebbe un $N_1 2 + 1$, mentre che il 1° è divisibile per 2^9, poichè t è un $N_1 2$; se ne concluderà che l'equazione precedente non può essere scomposta in due altre che nel modo seguente, in cui si suppone $t = 2ur'$; $g = 5^6 . 2^9 . u^{10}$, $f^4 + 10f^2 g^2 + 5g^4 = r'^{10}$. Nella 2ª equazione il 1° membro può mettersi sotto la forma: $(f^2 + 5g^2)^2 - 5(2g^2)^2$; dunque il suo divisore r' deve essere della forma $p^2 - 5q^2$; e lo stesso si ha per r'^2, e per conseguenza si potrà fare: $r'^2 = f'^2 - 5g'^2$; e quindi si avrà: $r^{10} = F'^2 - 5G'^2$, F' e G' essendo delle funzioni simili ad F e G; si avrà dunque l'equazione:

$$(f^2 + 5g^2)^2 - 5(2g^2)^2 = F'^2 - 5F'^2;$$

in cui $2g' = 5^{12} . 2^{19} . u^{20}$; e come sopra si troverà che la sola soluzione ammissibile è:

$$5^{11} . 2^{19} . u^{20} = g'(f'^4 + 10f'^2 g'^2 + 5g'^4).$$

Facendo ancora $u = u'r''$, r'' essendo primo con $10u'$, questa equazione non potrà scomporsi in altre due che così:

$$g' = 5^{11} \cdot 2^{19} u'^{20},$$
$$f^{14} + 10f^{12} g^{12} + 5g^{14} = (r'')^{20}.$$

e) Così si ricade sulle equazioni che son sempre della stessa forma e la cui serie può prolungarsi indefinitamente.

Ora avendo fatto successivamente $x = -5tr$, $t = 2ur'$, $u = u'r''$, $u' = u''r'''$ etc. ne segue che $t = 2ur' = 2u'r'r'' = 2u''r'r''r'''$ etc. sicchè il numero dei fattori r aumenta continuamente nell'espressione di t. Ciascuno di questi fattori determinati da un'equazione della forma: $r^{10m} = f^4 + 10f^2g^2 + 5g^4$, ove f e g sono degli N_1 sempre crescenti, poichè si ha: $g' = \frac{1}{2}(2g^2)^2$, $f^2 > 5g'^2$, è certamente maggiore di 1; e non può come un N_1 essere minore di 2. Dunque supponendo anche che la serie u, u', u'',... avrebbe per limite 1, il valore di t composto di un numero infinito di fattori 2, r', r'', r'''..., che non possono essere minori di 2, supererà tosto ogni quantità data, ciò che non può accordarsi colla supposizione fatta, che i valori primitivi di x, y, z siano dati in N_1 finiti. Dunque l'equazione proposta è impossibile nel 1° caso, in cui si suppone che una delle indeterminate sia ad un tempo un $N_1 2$ e un $N_1 5$.

2° caso, in cui x è un $N_1 2 + 1$.

f) Allora le due indeterminate y e z saranno l'una pari e l'altra dispari, e la 2ª dell'equazione (1) si potrà mettere sotto la forma

$$\left(y^2 - \frac{1}{2}yz + z^2\right)^2 - 5\left(\frac{1}{2}yz\right)^2 = 5r^5,$$

in cui si vede che $\frac{1}{2}yz$ è sempre un N_1 e che $y^2 - \frac{1}{2}yz + z^2$ deve essere un $N_1 5$; infatti si ha

$$y^2 - \frac{1}{2}yz + z^2 = (y+z)^2 - 5\left(\frac{1}{2}yz\right) = 5^8 t^{10} - 5\left(\frac{1}{2}yz\right).$$

L'equazione precedente può dunque scriversi così:

$$\left(\frac{1}{2}yz\right)^2 - 5\left(\frac{y^2 - \frac{1}{2}yz + z^2}{5}\right)^2 = -r^5;$$

e poichè il numero impari r è divisore di un numero della forma $p^2 - 5q^2$, in cui p e q son primi fra loro, sarà esso medesimo della stessa forma e così $-r$; poichè si ha che ogni N_1 della forma $p^2 - 5q^2$ è allo stesso tempo della forma $5a^2 - b^2$; si può quindi supporre $-r = f^2 - 5g^2$, e facendo come sopra,

$$(f + g\sqrt{5})^5 = F + G\sqrt{5},$$

si avrà $-r^5 = F^2 - 5G^2$, e l'equazione da risolvere sarà:

$$\left(\frac{1}{2}yz\right)^2 - 5\left(\frac{y^2 - \frac{1}{2}yz + z^2}{5}\right)^2 = F^2 - 5G^2.$$

Supponendo di nuovo $m+n\sqrt{5}=(9\pm4\sqrt{5})^k$, la risoluzione generale di questa equazione si otterrà facendo

$$\frac{1}{2}yz+\frac{y^2-\frac{1}{2}yz+z^2}{5}\cdot\sqrt{5}=(\mathrm{F}+\mathrm{G}\sqrt{5})(m+n\sqrt{5}),$$

ciò che dà:

$$\frac{1}{2}yz=m\mathrm{F}+5n\mathrm{G},$$

$$\frac{1}{5}(y^2-\frac{1}{2}yz+z^2)=m\mathrm{G}+n\mathrm{F}.$$

Da queste due equazioni si hanno:

$$\frac{1}{2}(y+z)^2=(m+n)\mathrm{F}+(m+5n)\mathrm{G},$$

ovvero

$$5^7t^{10}=(m+n)\mathrm{F}+(m+5n)\mathrm{G}.$$

g) Poichè G è sempre un N_15 e che F non lo è, questa equazione non può sussistere, a meno che $m+n$ non sia un N_15. Ora dai cinque valori di m ed n qui sopra riportati, si trova che questa condizione non può essere soddisfatta che supponendo $m=9$, $n=-4$, ciò che darà:

$$5^7t^{10}=5\mathrm{F}-11\mathrm{G},$$

o dividendo per 5 e sostituendo i valori di F e G:

$$5^6t^{10}=f^4(f-11g)+10f^2g^2(5f-11g)+5g^4(25f-21g).$$

Si vede da questa equazione che $(f-g)$ deve essere divisibile per 5; sia dunque $f=g+h$, h essendo un numero divisibile per 5; e si avrà

$$f+g\sqrt{5}=h+g(2+\sqrt{5}),$$

sicchè si potrà fare direttamente:

$$\mathrm{F}+\mathrm{G}\sqrt{5}=[h+g(1+\sqrt{5})]^5=h^5+5h^4g(1+\sqrt{5})+28h^3g^2(3+\sqrt{5})+80h^2g^3(2+\sqrt{5})$$
$$+40hg^4(7+3\sqrt{5})+16g^5(11+5\sqrt{5}).$$

D'onde si deducono i valori separati di F e G; ma siccome non si ha bisogno che della quantità $\mathrm{F}-\frac{11}{5}\mathrm{G}$, si potrà mettere in questa equazione $-\frac{11}{5}$ in luogo di $\sqrt{5}$, e quindi si avrà:

$$\mathrm{F}-\frac{11}{5}\mathrm{G}=h(h^4-6h^3g+16h^2g^2-16hg^3+16g^4),$$

e per conseguenza:

$$5^6t^{10}=h(h^4-6h^3g+16h^2g^2-16hg^3+16g^4).$$

h) Già si sa che h è un N_15 e che g non lo è, ed osservando di più che h deve essere un N_12+1, e che così i due fattori del 2º membro son primi fra loro, la sola maniera di soddisfare a questa equazione è di scinderla in altre due così:

$$h = 5^6 u^{10},$$
$$h^4 - 6h^3 g + 16h^2 g^2 - 16\,hg^3 + 16g^4 = r'^{10},$$

ciò che suppone $t = ur'$, r' essendo primo con $5u$.

La 2^a equazione può essere messa sotto la forma:

$$r'^{10} = (h^2 - 3\,gh + 6\,g^2)^2 - 5\,(gh - 2\,g^2)^2;$$

da cui si vede che r' deve essere della forma $p^2 - 5b^2$; e così r'^2 deve avere la stessa forma; si potrà dunque fare

$$r'^2 = f'^2 - 5\,g'^2;$$

ciò che darà $r'^{10} = \mathrm{F}'^2 - 5\,\mathrm{G}'^2$; e si soddisfarà generalmente all'equazione precedente facendo

$$h^2 - 3\,hg + 6\,g^2 = m\,\mathrm{F}' + 5n\,\mathrm{G}',$$
$$gh - 2g^2 = n\mathrm{F}' + m\mathrm{G}';$$

ciò che dà infine h^2 o:

$$5^{12}\,u^{20} = (m + 3n)\,\mathrm{F}' + (3m + 5n)\,\mathrm{G}'.$$

Poichè G' è un $\mathrm{N}_1 5$ e che F' non lo è, questa equazione non può sussistere a meno che $m + 3n$ non sia un $\mathrm{N}_1 5$. I soli valori di m ed n possibili per ciò sono $m = 161$, $n = -72$; ciò darà dividendo per 5:

$$5^{11}\,u^{20} = \frac{123}{5}\,\mathrm{G}' - 11\,\mathrm{F}',$$

o sostituendo i valori di F' e G':

$$5^{11}\,u^{20} = f'^{4}\,(123\,g' - 11f') + 10\,f'^2 g'^2\,(123\,g' - 55f') + 5\,g'^5\,(123\,g' - 275\,f').$$

i) Da questa equazione si vede che $3g' - f'$ è divisibile per 5; sia dunque $f' = 3g' - h'$, si avrà:

$$\mathrm{F}' + \mathrm{G}'\sqrt{5} = [-h' + g'\,(3 + \sqrt{5})]^5,$$

o facendo lo sviluppo

$$\mathrm{F}' + \mathrm{G}'\sqrt{5} = -h'^5 + 5\,h'^4 g'\,(3 + \sqrt{5}) - 20\,h'^3 g'^2\,(7 + 3\sqrt{5}) +$$
$$+ 80\,h'^2 g'^3\,(g + 4\sqrt{5}) - 40\,h' g'^4\,(47 + 21\sqrt{5}) +$$
$$+ 16\,g'^5\,(123 + 55\sqrt{5}).$$

Moltiplicando tutto per -11 e ponendo in luogo di $11\sqrt{5}$ il valore fittizio $-\frac{123}{5}$, si avrà $\frac{123}{5}\,\mathrm{G}' - 11\mathrm{F}'$, ovvero

$$5^{11}\,u^{20} = h'\,(11\,h'^4 - 42\,h'^3 g' + 64\,h'^2 g'^2 - 48\,h' g'^3 + 16\,g'^4).$$

Ora h' essendo un $\mathrm{N}_1 5$ e g' non essendolo, questa equazione non può scindersi in due altre che così:

$$h' = 5^{11}\,u'^{20}$$
$$11\,h'^4 - 42\,h'^3 g' + 64\,h'^2 g'^2 - 48\,h' g'^3 + 16\,g'^4 = r''^{20},$$

ciò che suppone $u = u'r''$ ed r'' primo con $5u'$.

Questa ultima equazione può essere messa sotto la forma:

$$4r''^{20} = (8g'^2 - 12g'h' + 7h'^2)^2 - 5h'^4;$$

d'onde ne consegue che r'' deve essere della forma $p^2 - 5q^2$, e così r''^4; dunque si può fare $r''^4 = f''^2 - 5g''^2$, ciò darà $r''^2 = F''^2 - 5G''^2$. Ora sia $4 = \mu^2 - 5\nu^2$, μ e ν essendo degli $N_1 2 + 1$, si potrà supporre:

$$8g'^2 - 12\,g'h' + 7h'^2 + h'^2\sqrt{5} = (F'' + G''\sqrt{5})(\mu + \nu\sqrt{5});$$

ciò darà:

$$h'^2 = \mu G'' + \nu F''.$$

Ma poichè h' e G'' sono degli $N_1 5$ e che F'' non lo è, questa equazione non può sussistere a meno che ν non sia un $N_1 5$. E siccome si ha in generale:

$$\mu + \nu\sqrt{5} = (3 + \sqrt{5})(m + n\sqrt{5}),$$

ciò che dà:

$$\mu = 3m + 5n \quad , \quad \nu = m + 3n,$$

non si potrà avere che $m = 161$, $n = -72$; da cui risulta $\mu = 123$, $\nu = -55$. di maniera che si avrà h^{12} o $5^{22}\,u''^{40} = 123\,G'' - 55\,F''$.

k) Così ricadiamo sopra una equazione simile all'equazione già considerata $5^{12}u^{20} = 123G' - 55F'$; d'onde ne consegue che le stesse trasformazioni potranno essere continuate all'infinito; ciò che supporrà infiniti i valori primitivi delle indeterminate. Poi avendo fatte successivamente:

$$x = -5tr, \qquad t = ur', \qquad u = u'r'', \qquad u' = u''r''' \ldots \text{etc.},$$

si avrà

$$t = ur' = u'r'r'' = u''r'r''r''' = \ldots \text{etc.};$$

sicchè il numero dei fattori r aumenta continuamente nell'espressione di t.

Questi fattori sono determinati da equazioni, che si possono ridurre alla stessa forma, e cioè

$$r'^{10} = r^2 + 5rh^2 + 5h^4, \qquad r''^{20} = r'^4 + 5r'^2h^2 + 5h'^4 \text{ etc.};$$

d'altra parte si ha

$$h = 5^6u^{10}, \qquad h' = 5^{11}u'^{20}, \qquad h'' = 5^{21}u''^{40} \text{ etc.};$$

sicchè la serie $h, h', h'' \ldots$ etc. è rapidamente crescente, anche supponendo che i numeri $u, u', u'' \ldots$ etc. abbiano 1 per limite. Dunque i numeri $r, r', r'' \ldots$ etc. sempre maggiori di 1, non potranno essere minori di 2; e da ciò ne consegue che t diverrà infinito.

Dunque l'equazione $x^5 + y^5 + z^5 = 0$ non ammette alcuna soluzione in N_1.

l) Ora è dimostrato che l'equazione $x^n + y^n + z^n = 0$ non può aver luogo per n, che è un $N_1 2 + 1$, delle forme $N_1 5$ e $N_1 3$. Rispetto agli altri casi del teorema di Fermat, non sembrano potersi dimostrare coi metodi impiegati per il 3° e 5° grado; si sa solamente che la soluzione, se ne avessimo una, non potrebbe essere data che per numeri grandissimi.

14. Nuova dimostrazione del teorema di Fermat nel caso del 3° grado.

a) Al solito supporremo che esistano tre N_1: x, y, z positivi o negativi, che soddisfano l'equazione:

$$x^3 + y^3 + z^3 = 0,$$

colla condizione che siano due a due primi fra loro, e quindi due sono degli $N_1 2 + 1$ ed il 3° è un $N_1 2$.

Ora vedremo quali consegnenze risultano da questa H_p; divideremo la dimostrazione in tre parti.

1ª. L'uno dei numeri x, y, z deve essere un $N_1 3$.

Infatti ogni numero non un $N_1 3$, positivo o negativo, è della forma $3m \pm 1$ ed il suo cubo $27m^3 \pm 27m^2 + 9m \pm 1$ è della forma $9n \pm 1$. Se dunque nessuno dei tre numeri x, y, z non è un $N_1 3$, la somma dei loro cubi $x^3 + y^3 + z^3$ dovrà essere di una delle quattro forme $9n \pm 1$, $9n \pm 3$ e non potrebbe per conseguenza ridursi a zero. Dunque uno dei tre numeri x, y, z è necessariamente un $N_1 3$.

2ª. Quella delle indeterminate che è un $N_1 2$, è ad un tempo un $N_1 3$.

Sia z un $N_1 2$ e sia $z = -2^m u$, u essendo un $N_1 2 + 1$; sicchè si ha l'equazione:

$$x^3 + y^3 = 2^{3m} u^3 ;$$

io dico che u è un $N_1 3$.

Infatti supponiamo, se è possibile, che u non sia un $N_1 3$; il 1° membro $x^3 + y^3$ è il prodotto di due fattori $x + y$ e $x^2 - xy + y^2$, il quale non può avere che 3 per divisore comune (vedi Oss. del n. 7); e poichè 3 non divide il 2° membro $2^{3m} u^3$, ne consegue che questi due fattori son primi fra loro. Il loro prodotto deve essere un cubo; se d'altra parte si osserva che $x^2 - xy + y^2$ è sempre un $N_1 2 + 1$, se ne concluderà che 2^{3m} deve essere fattore di $x + y$; così si dovrà porre:

$$x + y = 2^{3m} \alpha^3,$$
$$x^2 - xy + y^2 = \beta^3 ;$$

ciò che suppone $u = \alpha\beta$, β essendo un N_1 primo con α.

Ora se si mette la 2ª equazione sotto questa forma:

$$\beta^3 = \left(\frac{x+y}{2}\right)^2 + 3\left(\frac{x-y}{2}\right)^2 ;$$

si vede che il 2° membro essendo della forma $p^2 + 3q^2$; il suo divisore β, che è un $N_1 2 + 1$, dovrà essere della stessa forma. Facendo dunque $\beta = f^2 + 3g^2$, poi

$$(f + g\sqrt{-3})^3 = F + G\sqrt{-3},$$

ciò che dà

$$F = f(f^2 - 9g^2)$$
$$G = 3g(f^2 - g^2),$$

si avrà

$$\beta^3 = F^2 + 3G^2 ;$$

sicchè si soddisferà generalmente all'equazione precedente facendo:

$$\frac{x+y}{2} = F, \qquad \frac{x-y}{2} = G ;$$

ciò che darà:

$$x = f^3 + 3f^2 g - 9fg^2 - 3g^3,$$
$$y = f^3 - 3f^2 g - 9fg^2 + 3g^3.$$

Ora z essendo supposto non un $N_1 3$, bisognerà che uno dei numeri x ed y sia un $N_1 3$; ciò che esige che anche f sia un $N_1 3$. Ma allora i due numeri x ed y saranno divisibili per 3, come z; ciò che è contro l'H_p.

Dunque l'indeterminata z se è un $N_1 2$ sarà pure un $N_1 3$ e si dovrà fare in generale $z = -2^m \cdot 3^n \cdot u$, u essendo primo con 6; sicchè l'equazione proposta sarà sempre della forma $x^3 + y^3 = 2^{3m} \cdot 3^{3n} \cdot u^3$.

3ª. L'equazione $x^3 + y^3 = 2^{3m} \cdot 3^{3n} \cdot u^3$ è impossibile.

Infatti supponiamo per un momento che essa possa essere soddisfatta, senza che nessuna delle indeterminate sia nulla, i due fattori del 1º membro, cioè $x+y$ e $x^2 - xy + y^2$, hanno per divisor comune 3 e non una potenza più elevata di 3, come si è mostrato al n. 7; d'altra parte il 2º fattore è un $N_1 2 + 1$; sicchè la nostra equazione necessariamente si scinderà in altre due così:

$$x + y = 2^{3m} \cdot 3^{3n-1} \alpha^3$$
$$x^2 - xy + y^2 = 3\beta^3,$$

e si avrà ad un tempo $u = \alpha\beta$.

La 2ª di queste equazioni può scriversi così:

$$\beta^3 = \left(\frac{x-y}{2}\right)^2 + 3\left(\frac{x+y}{6}\right)^2;$$

d'onde ne consegue che β è ancora della forma $p^2 + 3q^2$. Facendo adunque come sopra:

$$\beta = f^2 + 3g^2 \quad \text{e} \quad \beta^3 = F^2 + 3G^2,$$

si avrà l'equazione

$$\left(\frac{x-y}{2}\right)^2 + 3\left(\frac{x+y}{6}\right)^2 = F^2 + 3G^2;$$

a cui si soddisferà generalmente prendendo

$$\frac{x-y}{2} = F, \qquad \frac{x+y}{6} = G.$$

Quest'ultima, facendo le sostituzioni, dà

$$2^{3m-1} \cdot 3^{3n-3} \cdot \alpha^3 = g(f^2 - g^2).$$

In questa equazione, in cui $f^2 - g^2$ è un $N_1 2 + 1$, poichè $f^2 + 3g^2$ è pure un $N_1 2 + 1$, bisogna che g sia un $N_1 2^{3m-1}$; sia dunque

$$g = 2^{3m-1}A, \qquad f + g = B, \qquad f - g = C;$$

si avrà

$$(3^{n-1}\alpha)^3 = ABC.$$

Ora perchè il prodotto ABC è un cubo ed i fattori A, B, C sono due a due primi fra loro, bisogna che ciascuno di essi sia un cubo; così dovrà farsi

$$A = \lambda^3, \qquad B = \mu^3, \qquad C = \nu^3;$$

ciò che darà

$$f + g = \mu^3, \qquad f - g = \nu^3, \qquad g = 2^{3m-1} \cdot \lambda^3,$$

e ad un tempo $\lambda\mu\nu = 3^{n-1}\alpha$. Da cui si ha l'equazione:

$$\mu^3 - \nu^3 = 2g = 2^{3m}\lambda^3,$$

simile alla proposta; in cui bisogna osservare che i tre numeri λ, μ, ν devono contenere il fattore 3^{n-1}. Ora da quello che si è mostrato nella seconda parte, il termine $2^m\lambda$ già divisibile per 2, è necessariamente anche divisibile per 3; dunque bisogna fare $\lambda = 3^{n-1}\theta$, ciò che darà

$$\mu^3 - \nu^3 = (2^m \cdot 3^{n-1}\theta)^3.$$

Così dall'equazione $x^3 + y^3 = (2^m . 3^n u)^3$, in cui una delle indeterminate è un $N_1 3^n$, si deduce una equazione simile, ove la indeterminata corrispondente è un $N_1 3^{n-1}$. Continuando dunque queste trasformazioni tante volte, quante sono le unità di n, si perverrà ad un'ultima trasformata $x'^3 + y'^3 = z'^3$, nella quale nessuno dei numeri x', y', z' non sarà un $N_1 3$. Questa equazione è impossibile in virtù della prima parte; dunque l'equazione proposta $x^3 + y^3 + z^3 = 0$ è similmente impossibile.

§ X.

Nota sulla impossibilità dell'equazione $x^5 + y^5 + z^5 = 0$.

1. In questa nota mi propongo di dare una dimostrazione semplice e breve della impossibilità di risolvere in N_1 l'equazione:

(1)
$$x^5 + y^5 + z^5 = 0.$$

2. Nella (1) uno dei tre numeri x, y, z lo supponiamo sempre negativo e per semplicità li supponiamo due a due primi fra loro; perciò due di essi saranno della forma $N_1 2 + 1$ ed il terzo un $N_1 2$; e sia z il $N_1 2$; allora possiamo porre

(2)
$$\begin{cases} x + y = 2p \\ x - y = 2q \,; \end{cases}$$

da cui si ha:

(3)
$$\begin{cases} x = p + q \\ y = p - q. \end{cases}$$

Dalle (3) si vede che anche p e q son primi fra loro e l'uno di essi è un $N_1 2$ e l'altro un $N_1 2 + 1$.

Sostituendo nella (1) i valori dati dalle (3) si ha:

(4)
$$2p\,[p^4 + 5q^2\,(q^2 + 2p^2)] + z^5 = 0.$$

3. Ora supponiamo che p sia un $N_1 2 + 1$; allora q è un $N_1 2$: ma anche $p^4 + 5q^2\,(q^2 + 2p^2)$ è un $N_1 2 + 1$; ma per ipotesi pure il prodotto

$$p\,[p^4 + 5q^2\,(q^2 + 2p^2)]$$

sarebbe un $N_1 2 + 1$; ma esso è uguale a $- z^5 : 2$, che è un $N_1 16$; dunque ne consegue che p non può essere un $N_1 2 + 1$; perciò p sarà un $N_1 2$, e quindi q sarà un $N_1 2 + 1$.

4. Ora possiamo porre

(5)
$$\alpha^2 = q^2 + 2p^2;$$

dalla quale si vede che α è un $N_1 2 + 1$, ed è soddisfatta da:

(6)
$$\begin{cases} p = 2ab, \\ q = 2a^2 - b^2, \\ \alpha = 2a^2 + b^2. \end{cases}$$

Allora la (4) prende la forma

$$2p\,[(p^2)^2 + 5\,(q\alpha)^2] + z^5 = 0. \tag{7}$$

Osservo che essendo p e q primi fra loro, ed essendo $\alpha^2 = q^2 + 2p^2$ e perciò α un $N_1 2 + 1$, ne consegue che p, q ed α sono primi due a due fra loro. Per potere poi stabilire quando anche $2p$ e $p^4 + 5\alpha^2 q^2$ siano primi fra loro, bisogna distinguere due casi.

5. 1° caso, p non è un $N_1 5$.

Allora $2p$ e $p^4 + 5\alpha^2 q^2$ son primi tra loro, ed affinchè il termine

$$2p\,[(p^2)^2 + 5\,(q\alpha)^2],$$

che comparisce nella equazione (7), sia una potenza quinta di un N_1, come lo è $-z^5$, a cui esso è uguale, è necessario e sufficiente che si abbia:

$$\begin{cases} 2p = s^5, \\ p^4 + 5\alpha^2 q^2 = r^5. \end{cases} \tag{8}$$

Ora faremo vedere che r è della forma $m^2 + 5n^2$; e perciò si potrà sempre porre:

$$p^2 + q\alpha\sqrt{-5} = (m + n\sqrt{-5})^5, \tag{9}$$

ove m ed n sono degli N_1 primi fra loro, essendolo p, q ed α. Sviluppando il 1° membro della (9) e poi eguagliando fra loro le parti reali e fra loro le parti immaginarie avremo:

$$\begin{cases} p^2 = m^5 - 50m^3n^2 + 125mn^4 = m\,(m^4 - 50m^2n^2 + 125n^4), \\ q\alpha = 5m^4n - 50m^2n^3 + 25n^5 = 5n\,(m^4 - 10m^2n^2 + 5n^4). \end{cases} \tag{10}$$

Da quest'ultima si vede che q od α è un $N_1 5$.

I valori dati per p^2 e $q\alpha$ dalle (10) insieme all'altro $r = m^2 + 5n^2$ soddisfano la 2ª dell'equazioni (8). Infatti facendovi la sostituzione abbiamo:

$$(m^5 - 50m^3n^2 + 125mn^4)^2 + 5\,(5m^4n - 50m^2n^3 + 25n^5)^2 = m^{10} +$$
$$+ 25m^8n^2 + 250m^6n^4 + 1250m^4n^6 + 3125n^8m^2 + 3125n^{10} = (m^2 + 5n^2)^5.$$

Dunque è vero che r è della forma $m^2 + 5n^2$.

Anche qui bisogna distinguere due casi: 1° m non è un $N_1 5$; 2° m è un $N_1 5$.

1° caso, m non è un $N_1 5$.

Allora m ed $m^4 - 50m^2n^2 + 125n^4$ son primi fra loro, e quindi affinchè sia possibile di risolvere in N_1 l'equazione:

$$p^2 = m\,(m^4 - 50m^2n^2 + 125n^4),$$

è necessario che sia:

$$\begin{cases} m = t^2, \\ m^4 - 50m^2n^2 + 125n^4 = u^2. \end{cases} \tag{13}$$

Ora si sa (*) che quest'ultima equazione non si può risolvere in N_1. Dunque in questo caso non essendo possibile di risolvere in N_1 la 2ª delle (13), che è conseguenza della (1), ne viene anche che la (1) non si potrà risolvere in N_1.

(*) Vedi *Comptes rendus des sciences de l'Academie des sciences*, t. 9. — 1839. " Mémoire de Mathématique sur le dernier théorème de Fermat " par M. Lamé etc.

2° caso, m è un $N_1 5$.

Allora dalle (10) ne viene che p ed α sono degli $N_1 5$; il che non può essere, essendo p, q ed α primi due a due fra loro. Dunque ecc.

6. 2° caso, p è un $N_1 5$.

Sapendosi che q od α è un $N_1 5$ e che p, q ed α sono primi due a due fra loro, ne consegue che p non può essere un $N_1 5$. Dunque ecc.

7. Da quanto precede risulta dimostrato che la equazione $x^5 + y^5 + z^5 = 0$ non può essere risolta in N_1; e da ciò ne consegue che non possono essere risolte in N_1 le equazioni della forma:

$$x^n + y^n + z^n = 0,$$

ove n è un $N_1 5$.

8. A me pare che si possa dimostrare l'impossibilità di risolvere in N_1 la 2ª dell'equazioni (13) in questo modo:

L'equazione:

$$(13)' \qquad m^4 - 50m^2n^2 + 125n^4 = u^2$$

si può scrivere così:

$$(14) \qquad (m^2 - 25n^2)^2 - (4n)^4 = u^2 + (12n^2)^2 + (10n^2)^2.$$

Ora si può sempre porre:

$$(15) \qquad m^2 - 25n^2 = \beta^2,$$

nella quale basta fare:

$$(16) \qquad \begin{cases} m = a^2 + b^2, \\ 5n = 2ab, \\ \beta = a^2 - b^2. \end{cases}$$

Di più si può sempre porre:

$$(17) \qquad u^2 + (12n^2)^2 + (10n^2)^2 = \gamma^2;$$

nella quale basta porre:

$$(18) \qquad \left\{\begin{array}{l} u = c^2 + d^2 - e^2 \\ 12n^2 = 2ce \\ 10n^2 = 2de \\ \gamma = c^2 + d^2 + e^2 \end{array}\right\} \quad \text{od anche} \quad \begin{cases} u = 61c^2 - d^2, \\ n^2 = cd, \\ \gamma = 61c^2 + d^2; \end{cases}$$

e così la (13) assume la forma:

$$\beta^4 - (3n)^4 = \gamma^2,$$

la quale come si sa (Vedi § I e IV) non può essere soddisfatta in N_1.

§ XI.

Per maggiore intelligenza della memoria del Kummer (§ VII) consultare:

1°. Pei numeri Bernoulliani:

a) L'opera recente Saalschütz (*Vorl. über die Bern. Zahlen.* Berlin, 1893).

b) Glaischer (*Mess. of Math.*, 1876).

c) Seidel (*Müch. Ak.* 1877).

d) Radicke (*Die Recursionsformeln für die Bern und Eul. Zahlen.* Halle 1880).

e) Haussner (*Gött. Nach.*, 1893; *Zeitschrift. f. Math*).

2°. Pei numeri ideali del Kummer:

a) KUMMER " Zur Theorie der complexen Zahlen „ e " Über die Zerlegung der aus Wurzeln der Einheit gebildeten complexen Zahlen in ihre Primfactoren „. Memorie 15 e 16 a pagg. 319 e 327 nel *Jornal* de CRELLE, Vol. 35. Berlin, 1847.

b) DIRICHLET (Acc. di Berlino, 1840, 1841, 1846).

c) DEDEKIND (*Ueber die Anzahlen der Ideal-Classen ecc.*, Braunschweig, 1877; *Ueber den Zusamm, ruischen der Theorie der Ideale* ecc. *Mem. di Göttingen*, t. XXIII; " Sur la th. des nombres alg. „ *Bull.* de DARBOUX, 1ª s., t. XI, e 2ª s., t. I, (1877).

d) FUCHS (*Crelle*, LXV).

e) SELLING (*Zeitsch. f. Math.* 1865).

f) ZOLOTAREFF *Liouville*, 1880).

g) Per una esposizione di tutta la teoria si può utilmente vedere l'ultima parte della 3ª edizione della *Teoria dei Numeri* di DIRICHLET-DEDEKIND tradotto in ital. dal *Faifofer*. Venezia 1881) ecc.

§ XII.

1°. Il Kummer oltre la memoria qui riportata al § VII, ha pubblicato le seguenti memorie, che hanno stretta attinenza coll'ultimo teorema di Fermat:

a) De æquatione: $x^{2\lambda} + y^{2\lambda} = z^{2\lambda}$ per numeros integros resolvenda. (Vedi *Journal de Crelle*, V, XVII, pp. 203-209, 1837).

b) Beweis des Fermatschen Zatzes der Unmöglichkit von $x^\lambda - y^\lambda = z^\lambda$ für eine ünendliche Anzahl Primzahlen λ. Berlin, Bericht, 1847; pp. 132, 139, 140, 141, 305, 319.

c) Théorème de Fermat et manuscrit Arabe. *Nouv. Ann. Math.* 1850, t. IV, pp. 386, 392.

2°. Il Legendre oltre le memorie dei §§ IV e IX ha pubblicato i seguenti lavori, che hanno pur essi stretta attinenza coll'ultimo teorema di Fermat:

A) Vedi *Essai sur la théorie des nombres,* second edition. Paris, 1808.

a) Quatrième partie.

Méthodes e recherches diverses. — § 1. Théoremès sur le puissances des nombres.

α) L'aire d'un triangle rectangle en nombres entiers ne pourrait être egale á un quarré.

β) La formule $x^4 + 2y^4$ ne peut être un quarré.

γ) Aucun nombre triangulaire, excepté 1, n'est égal à un biquarré, n'est égal à un cube.

δ) La somme ou la différence de deux cubes inegaux ne peut être double d'un cube.

B) Vedi " Mémoires de l'academie royale des sciences de l'institut de France „ année 1823, tome VI. Paris, 1827.

b) Recherches sur quelques objets d'analyse indéterminée et particulièrement sur le théorème de Fermat.

α) L'équation $x^3 + y^3 = 2^{3m} \,.\, 3^{3n}\, u^3$ est impossible.

β) De l'équation $x^3 + y^3 = 2^m z^3$.

γ) De l'équation $x^3 + y^3 = Az^3$.

δ) Théorèmes d'analyse.

Dott. DIONISIO GAMBIOLI.

Sul prodotto di due matrici rettangolari coniugate

---

1. Diremo *coniugate* due matrici rettangolari A e B, aventi rispettivamente m e p orizzontali ed n e q verticali ($m \leq n$, $p \leq q$), quando è soddisfatta la relazione

$$(1) \qquad n - m = q - p$$

ed inoltre, supposto $n \leq q$, le verticali di A corrispondono ordinatamente alle verticali di B rispettivamente di rango $s_1, s_2, \ldots, s_n$, intendendo questi numeri disposti in ordine crescente.

In particolare due matrici *simili* sono coniugate, giacchè per esse è $m = p$ ed $n = q$ e quindi la (1) è soddisfatta ed inoltre si corrispondono le verticali d'ugual rango.

Se con α indichiamo uno qualunque dei determinanti di ordine m appartenenti alla matrice A e con β la matrice formata colle verticali di B che corrispondono a quelle che entrano in α, assieme alle $q - n$ verticali che non hanno le corrispondenti in A, è facile vedere che β resulterà una matrice quadrata. Infatti l'ordine di α è m, quindi in β entrano $m + q - n$ verticali, numero che, per la (1), è uguale a p, cioè al numero delle orizzontali. Converremo che tanto le orizzontali quanto le verticali che entrano a formare i determinanti α e β conservino in questi lo stesso ordine di successione che hanno nelle matrici A e B.

Due tali determinanti li diremo *omologhi* e chiameremo *prodotto* delle due matrici rettangolari coniugate A e B la somma dei determinanti di ordine m di A moltiplicati rispettivamente per i loro omologhi in B, e scriveremo

$$(2) \qquad \mathrm{A} \,.\, \mathrm{B} = \Sigma \alpha \,.\, \beta.$$

Convenendo di indicare col medesimo numero (secondo indice) due verticali corrispondenti di due matrici coniugate, avremo per esempio

$$\begin{vmatrix} a_{12} & a_{14} & a_{15} \\ a_{22} & a_{24} & a_{25} \end{vmatrix} \cdot \begin{vmatrix} b_{11} & b_{12} & b_{13} & b_{14} & b_{15} \\ b_{21} & b_{22} & b_{23} & b_{24} & b_{25} \\ b_{31} & b_{32} & b_{33} & b_{34} & b_{35} \\ b_{41} & b_{42} & b_{43} & b_{44} & b_{45} \end{vmatrix} = \begin{vmatrix} a_{12} & a_{14} \\ a_{22} & a_{24} \end{vmatrix} \cdot \begin{vmatrix} b_{11} & b_{12} & b_{13} & b_{14} \\ b_{21} & b_{22} & b_{23} & b_{24} \\ b_{31} & b_{32} & b_{33} & b_{34} \\ b_{41} & b_{42} & b_{43} & b_{44} \end{vmatrix} +$$

$$+ \begin{vmatrix} a_{12} & a_{15} \\ a_{22} & a_{25} \end{vmatrix} \cdot \begin{vmatrix} b_{11} & b_{12} & b_{13} & b_{15} \\ b_{21} & b_{22} & b_{23} & b_{25} \\ b_{31} & b_{32} & b_{33} & b_{35} \\ b_{41} & b_{42} & b_{43} & b_{45} \end{vmatrix} + \begin{vmatrix} a_{14} & a_{15} \\ a_{24} & a_{25} \end{vmatrix} \cdot \begin{vmatrix} b_{11} & b_{13} & b_{14} & b_{15} \\ b_{21} & b_{23} & b_{24} & b_{25} \\ b_{31} & b_{33} & b_{34} & b_{35} \\ b_{41} & b_{43} & b_{44} & b_{45} \end{vmatrix} .$$

2. Il prodotto delle due matrici coniugate A e B può essere espresso anche mediante un unico determinante d'ordine p.

Siano infatti

$$\begin{vmatrix} a_{1s_1} \dots a_{1s_n} \\ \dots\dots\dots \\ a_{ms_1} \dots a_{ms_n} \end{vmatrix} \quad , \quad \begin{vmatrix} b_{11} \dots b_{1q} \\ \dots\dots \\ b_{p1} \dots b_{pq} \end{vmatrix}$$

le due matrici coniugate A e B e poniamo

$$(3) \qquad c_{ir_k} = a_{ks_1} b_{is_1} + a_{ks_2} b_{is_2} + \dots + a_{ks_n} b_{is_n}, \qquad \begin{pmatrix} k = 1, 2, \dots, m \\ i = 1, 2, \dots, p \end{pmatrix}.$$

Il determinante

$$P = \begin{vmatrix} c_{1r_1} c_{1r_2} \dots c_{1r_m} b_{1r_{m+1}} \dots b_{1r_p} \\ c_{2r_1} c_{2r_2} \dots c_{2r_m} b_{2r_{m+1}} \dots b_{2r_p} \\ \dots\dots\dots\dots\dots\dots \\ c_{pr_1} c_{pr_2} \dots c_{pr_m} b_{pr_{m+1}} \dots b_{pr_p} \end{vmatrix}$$

esprime, prescindendo dal segno, il prodotto delle matrici coniugate A e B.

Per ottenere esattamente detto prodotto basta permutare le verticali in modo che i secondi indici resultino disposti nell'ordine naturale.

Immaginando sostituite alle c le loro espressioni date dalla (3), possiamo decomporre il determinante P nella somma di determinanti del tipo

$$\begin{vmatrix} a_{1s_{j_1}} b_{1s_{j_1}} & a_{2s_{j_2}} b_{1s_{j_2}} \dots a_{ms_{j_m}} b_{1s_{j_m}} & b_{1r_{m+1}} \dots b_{1r_p} \\ a_{1s_{j_1}} b_{2s_{j_1}} & a_{2s_{j_2}} b_{2s_{j_2}} \dots a_{ms_{j_m}} b_{2s_{j_m}} & b_{2r_{m+1}} \dots b_{2r_p} \\ \dots\dots & \dots\dots\dots\dots & \dots\dots \\ a_{1s_{j_1}} b_{ps_{j_1}} & a_{2s_{j_2}} b_{ps_{j_2}} \dots a_{ms_{j_m}} b_{ps_{j_m}} & b_{pr_{m+1}} \dots b_{pr_p} \end{vmatrix}$$

e quindi in termini della forma

$$(4) \qquad a_{1s_{j_1}} a_{2s_{j_2}} \dots a_{ms_{j_m}} \begin{vmatrix} b_{1s_{j_1}} \dots b_{1s_{j_m}} b_{1r_{m+1}} \dots b_{1s_p} \\ \dots\dots\dots\dots\dots \\ b_{ps_{j_1}} \dots b_{ps_{j_m}} b_{pr_{m+1}} \dots b_{pr_p} \end{vmatrix}$$

in cui $j_1, j_2, \dots, j_m$ rappresentano una disposizione ad m ad m *senza ripetizione* degli n numeri $1, 2, \dots, n$. Facendo variare $j_1, j_2, \dots, j_m$ in tutti i modi possibili e sommando si otterrà il determinante P.

L'espressione (4) equivale evidentemente alla seguente:

$$(-1)^{\mu+\nu} a_{1s_{j_1}} a_{2s_{j_2}} \dots a_{ms_{j_m}} . \beta$$

in cui β rappresenta un determinante di ordine p appartenente alla matrice B, che si ottiene da quello che si trova nell'espressione (4) permutando opportunamente le verticali, μ indica il numero delle inversioni che presenta il gruppo $j_1, j_2, \ldots, j_m$, considerato quale una permutazione degli m numeri che vi figurano, e ν il numero delle inversioni che nella permutazione $s_{j_1}, s_{j_2}, \ldots, s_{j_m}, r_{m+1}, \ldots, r_p$ le s formano colle r.

Permutando in tutti i modi possibili i *medesimi* indici $j_1, j_2, \ldots, j_m$ otterremo $m!$ termini di P, la cui somma sarà

$$(-1)^\nu \alpha . \beta, \tag{5}$$

essendo α il determinante della matrice A omologo al determinante β.

Applicando il medesimo procedimento a tutte le espressioni che si ottengono dalla (4) e che corrispondono ai sistemi di m valori diversi delle j, otterremo altre espressioni analoghe alla (5), nelle quali il valore di ν è sempre il medesimo; avremo quindi

$$P = (-1)^\nu \Sigma \alpha . \beta$$

ossia, per la (2),

$$A . B = (-1)^\nu P$$

come avevamo asserito.

Abbiamo per es.:

$$\begin{vmatrix} a_{12} & a_{14} & a_{15} \\ a_{22} & a_{24} & a_{25} \end{vmatrix} . \begin{vmatrix} b_{11} & b_{12} & b_{13} & b_{14} & b_{15} \\ b_{21} & b_{22} & b_{23} & b_{24} & b_{25} \\ b_{31} & b_{32} & b_{33} & b_{34} & b_{35} \\ b_{41} & b_{42} & b_{43} & b_{44} & b_{45} \end{vmatrix} = (-1)^8 \begin{vmatrix} c_{12} & c_{14} & b_{11} & b_{13} \\ c_{22} & c_{24} & b_{21} & b_{23} \\ c_{32} & c_{34} & b_{31} & b_{33} \\ c_{42} & c_{44} & b_{41} & b_{43} \end{vmatrix} =$$

$$= \begin{vmatrix} b_{11} & a_{12}b_{12} + a_{14}b_{14} + a_{15}b_{15} & b_{13} & a_{22}b_{12} + a_{24}b_{14} + a_{25}b_{15} \\ b_{21} & a_{12}b_{22} + a_{14}b_{24} + a_{15}b_{25} & b_{23} & a_{22}b_{22} + a_{24}b_{24} + a_{25}b_{25} \\ b_{31} & a_{12}b_{32} + a_{14}b_{34} + a_{15}b_{35} & b_{33} & a_{22}b_{32} + a_{24}b_{34} + a_{25}b_{35} \\ b_{41} & a_{12}b_{42} + a_{14}b_{44} + a_{15}b_{45} & b_{43} & a_{22}b_{42} + a_{24}b_{44} + a_{25}b_{45} \end{vmatrix}.$$

3. Ogni minore di P, in cui figurano elementi composti, si può esprimere mediante il prodotto di due matrici coniugate che si deducono assai facilmente dalle due matrici date A e B. Un tale minore è, a meno del segno, anche minore del determinante che si ottiene moltiplicando le due matrici coniugate A e B.

Supponiamo che si tratti d'un minore M d'ordine h, nel quale gli elementi della diagonale principale siano

$$c_{\varrho_1 r_{\sigma_1}},\ c_{\varrho_2 r_{\sigma_2}}, \ldots, c_{\varrho_\lambda r_{\sigma_\lambda}},\ b_{\varrho_{\lambda+1} r_{\sigma_{\lambda+1}}}, \ldots, b_{\varrho_h r_{\sigma_h}}.$$

È facile verificare che questo minore, salvo il segno, si otterrà moltiplicando le matrici coniugate A′, B′ che si deducono rispettivamente da A e B, sopprimendo nella prima tutte le orizzontali di rango differente da $\sigma_1, \sigma_2, \ldots, \sigma_\lambda$ e nella seconda le orizzontali di rango differente da $\rho_1, \rho_2, \ldots, \rho_h$ e fra le verticali, che non hanno la corrispondente in A, quelle il cui rango è diverso da $r_{\sigma_{\lambda+1}}, r_{\sigma_{\lambda+2}}, \ldots, r_{\sigma_h}$.

Basterà poi disporre in M le verticali secondo l'ordine naturale per ottenere esattamente il prodotto delle due matrici coniugate A', B'.

Così, riferendoci all'esempio considerato nell'articolo precedente, abbiamo

$$\begin{vmatrix} b_{31} & a_{23}b_{32}+a_{24}b_{34}+a_{25}b_{35} \\ b_{41} & a_{22}b_{42}+a_{24}b_{44}+a_{25}b_{45} \end{vmatrix} = |a_{32}\, a_{34}\, a_{25}| \cdot \begin{vmatrix} b_{21} & b_{22} & b_{24} & b_{25} \\ b_{41} & b_{42} & b_{44} & b_{45} \end{vmatrix}.$$

4. Per mostrare un esempio in cui può intervenire utilmente la considerazione delle coppie di matrici rettangolari coniugate, proponiamoci il seguente problema:

Sia D *un determinante d'ordine* n *e da esso deduciamo il determinante* D_m *d'ordine* $\binom{n}{m}$, *i cui elementi siano i minori d'ordine* m *di* D, *disposti in modo che in una stessa orizzontale o verticale di* D_m *figurino tutti i minori ottenuti colle medesime orizzontali o verticali di* D *ed ordinati così che nella diagonale principale compariscano i minori principali d'ordine* m *del dato. Da un minore qualsivoglia d'ordine* h *di* D_m *deduciamo poi il determinante* $\delta^{(k)}$, *sostituendo agli elementi di* h — k *orizzontali i loro complementi algebrici in* D.

Vogliamo esprimere il valore del determinante $\delta^{(k)}$ *mediante il primitivo* D *ed i suoi minori d'ordine* m.

Indichiamo con $\Delta^{(k)}$ il determinante che si ottiene da D_m sostituendo a tutti gli elementi appartenenti alle $\binom{n}{m}-k$ orizzontali, che non hanno alcun elemento in $\delta^{(k)}$, i loro complementi algebrici in D. È chiaro allora che $\delta^{(k)}$ è un minore d'ordine h di $\Delta^{(k)}$.

Sostituiamo in questo determinante l'unità a tutti gli elementi della diagonale principale, situati sulle orizzontali non appartenenti alla matrice che comprende il minore $\delta^{(k)}$, e lo zero a tutti gli altri elementi di queste stesse orizzontali; inoltre poniamo zero al posto degli elementi che $\Delta^{(k)}$ ha in comune con D_m e che non appartengono a $\delta^{(k)}$.

Con ciò otteniamo un determinante $\Delta_1^{(k)}$ equivalente a $(-1)^{r+s}\delta^{(k)}$, in cui r ed s indicano rispettivamente la somma dei numeri che esprimono il rango delle verticali e delle orizzontali che figurano in $\delta^{(k)}$.

Moltiplichiamo questo determinante per D_m, dopo aver praticato in entrambi il medesimo spostamento di orizzontali in modo che in $\Delta_1^{(k)}$ figurino per prime quelle orizzontali che concorrono alla formazione di $\delta^{(k)}$; evidentemente il valore del prodotto non subisce alcuna alterazione ed è quindi uguale a

$$(-1)^{r+s}\delta^{(k)}D_m.$$

Eseguendo la moltiplicazione per orizzontali e scambiando nel determinante prodotto le orizzontali colle verticali, si ottiene un determinante nel quale $h-k$ verticali hanno gli elementi nulli ad eccezione dell'elemento che si trova sulla diagonale principale e che resulta uguale a D.

È quindi facile dedurre che, sviluppando il determinante ottenuto per prodotti di minori contenuti in quelle $h-k$ verticali, si otterrà

$$H'H \,.\, D^{h-k},$$

dove H' ed H sono due matrici rettangolari coniugate, di cui la prima è formata cogli elementi di D_m che figurano in $\delta^{(k)}$ e la seconda si ottiene sopprimendo in D_m tutte le orizzontali che contengono quegli elementi che in $\delta^{(k)}$ sono stati sostituiti coi loro complementi algebrici in D e disponendo in questa le orizzontali e le verticali in modo che la matrice comune alle prime k orizzontali ed alle prime h verticali sia identica ad H'.

Le due matrici ora menzionate sono coniugate perchè H' contiene h verticali e k orizzontali, H contiene $\binom{n}{m}$ verticali ed $\binom{n}{m}-h+k$ orizzontali e quindi la relazione (1) è soddisfatta; in esse sono poi corrispondenti quelle verticali i cui elementi appartengono ad una medesima verticale di D_m (cioè le verticali d'ugual rango).

Possiamo quindi scrivere

$$(-1)^{r+s}\delta^{(k)}D_m = H'H \,.\, D^{h-k},$$

e poichè è noto (teorema di Sylvester) (*) che $D_m = D^{\binom{n-1}{m-1}}$, deduciamo infine

$$\delta^{(k)} = (-1)^{r+s} H'H \,.\, D^{h-k-\binom{n-1}{m-1}}. \tag{6}$$

Abbiamo così provato che

Un determinante $\delta^{(k)}$ d'ordine h, *dedotto da D_m nel modo detto, è uguale (in valore assoluto) alla potenza $\left[h-k-\binom{n-1}{m-1}\right]^{ma}$ del determinante primitivo* D, *moltiplicata per il prodotto di due matrici rettangolari coniugate, di cui una è formata cogli elementi di D_m che figurano in $\delta^{(k)}$ e l'altra s'ottiene sopprimendo in D_m quelle orizzontali che contengono gli elementi i cui complementi algebrici in* D *entrano in $\delta^{(k)}$ e disponendo in questa le orizzontali e le verticali in modo che le prime* k *orizzontali e le prime* h *verticali formino una matrice identica ad* H'. *In queste due matrici coniugate sono poi corrispondenti le verticali d'ugual rango.*

Se supponiamo $h=\binom{n}{m}$, $\delta^{(k)}$ diventa il determinante $\Delta^{(k)}$, prima considerato, e quindi, osservando che in tal caso abbiamo $r=s$, e che inoltre la matrice H' diventa identica alla matrice H, dalla (6) otteniamo

$$\Delta^{(k)} = H^2 \,.\, D^{\binom{n-1}{m}-k}. \tag{7}$$

(*) E. PASCAL, *I determinanti*, § 22. Manuali Hoepli.

Resta così dimostrato che

Il determinante $\Delta^{(k)}$, che si deduce da D_m sostituendo agli elementi di $\binom{n}{m} - k$ orizzontali i loro complementi algebrici in D, è uguale al quadrato della matrice formata cogli elementi di D_m che figurano in $\Delta^{(k)}$, moltiplicato per la potenza $\left[\binom{n-1}{m} - k\right]^{ma}$ di D.

In particolare, per $m = 1$, resulta $D_1 = D = \Sigma \pm a_{11} a_{22} \ldots a_{nn}$; quindi $\delta^{(k)}$ è un determinante che si ottiene da un minore d'ordine h di D, sostituendo agli elementi di $h - k$ orizzontali i loro complementi algebrici in D, e $\Delta^{(k)}$ è un determinante che si deduce da D sostituendo agli elementi di $n - k$ orizzontali i loro complementi algebrici.

In tal caso abbiamo dunque, applicando le (6) e (7) e supponendo che in $\delta^{(k)}$ e $\Delta^{(k)}$ entrino gli elementi di D che appartengono alle orizzontali di rango $s_1, s_2, \ldots, s_k$,

$$\delta^{(k)} = (-1)^{r+s} \begin{vmatrix} a_{s_1 r_1} \ldots a_{s_1 r_h} \\ \ldots\ldots\ldots \\ a_{s_k r_1} \ldots a_{s_k r_h} \end{vmatrix} \begin{vmatrix} a_{\sigma_1 r_1} & \ldots a_{\sigma_1 r_h} \\ \ldots\ldots\ldots & \ldots\ldots\ldots \\ a_{\sigma_{n-h+k} r_1} & \ldots a_{\sigma_{n-h+k} r_h} \end{vmatrix} . D^{h-k-1}$$

in cui i numeri $\sigma_1, \sigma_2, \ldots, \sigma_{n-h+k}$ differiscono dai numeri che esprimono il rango delle orizzontali di D che contengono quegli elementi che in $\delta^{(k)}$ sono stati sostituiti coi loro complementi algebrici, e

$$\Delta^{(k)} = \begin{vmatrix} a_{s_1 1} \ldots a_{s_1 n} \\ \ldots\ldots\ldots \\ a_{s_k 1} \ldots a_{s_k n} \end{vmatrix}^2 . D^{n-k-1}.$$

Cuneo, dicembre 1900.

Dott. LUIGI CARLINI.

LA RISOLUZIONE COMPLETA DEL TETRAGONO PIANO

Dicesi *tetragono piano* il sistema di 4 punti e delle 6 congiungenti posti in un medesimo piano. In esso si distinguono i 6 *lati* concorrenti tre a tre nei 4 *vertici* ed i 6 *angoli principali* formati dalla loro mutua inclinazione.

I 12 elementi di misura per comodità di studio li supporremo sempre aggruppati nel modo seguente; tre lati formeranno il *triangolo* detto *di base* o la *base del tetragono* di cui a, b, c, sono i lati ed A, B, C, gli angoli opposti, gli altri tre lati saranno concorrenti nel quarto *vertice* D e li diremo a', b', c' e formano i tre angoli opposti α, β, γ.

Dalla geometria elementare e dalla trigonometria è noto come del triangolo, dati tre elementi, fra cui sia compreso almeno un lato, si possono determinare i tre incogniti mediante le tre relazioni

$$A + B + C = \pi, \tag{1}$$

$$\frac{a}{\operatorname{sen} A} = \frac{b}{\operatorname{sen} B} = \frac{c}{\operatorname{sen} C}, \tag{2}$$

oppure

$$a^2 = b^2 + c^2 - 2bc \cos A \tag{3}$$

e l'analoga.

È pure noto come fra gli elementi lineari del tetragono piano esiste la relazione (*)

$$\begin{vmatrix} 0, & c^2, & b^2, & a'^2, & 1 \\ c^2, & 0, & a^2, & b'^2, & 1 \\ b^2, & a^2, & 0, & c'^2, & 1 \\ a'^2, & b'^2, & c'^2, & 0 & 1 \\ 1, & 1, & 1, & 1, & 1 \end{vmatrix} = 0. \tag{4}$$

In altro nostro lavoro tuttora inedito (**) abbiamo trovato esistere fra gli elementi lineari ed angolari del tetragono piano le relazioni seguenti:

$$\alpha + \beta + \gamma = 2\pi, \tag{5}$$

$$\left\{\begin{aligned} a' &= \frac{bc}{q} \operatorname{sen}(\alpha - A) \\ b' &= \frac{ca}{q} \operatorname{sen}(\beta - B) \\ c' &= \frac{ab}{q} \operatorname{sen}(\gamma - C), \end{aligned}\right. \tag{6}$$

dove il valore di q è dato da una qualunque delle seguenti espressioni:

$$\left\{\begin{aligned} q^2 &= a^2 \operatorname{sen}^2 \beta + b^2 \operatorname{sen}^2 \alpha + 2ab \operatorname{sen} \alpha \operatorname{sen} \beta \cos(\gamma - C) \\ q^2 &= b^2 \operatorname{sen}^2 \gamma + c^2 \operatorname{sen}^2 \beta + 2bc \operatorname{sen} \beta \operatorname{sen} \gamma \cos(\alpha - A) \\ q^2 &= c^2 \operatorname{sen}^2 \alpha + a^2 \operatorname{sen}^2 \gamma + 2ca \operatorname{sen} \gamma \operatorname{sen} \alpha \cos(\beta - B). \end{aligned}\right. \tag{7}$$

In altro lavoro abbiamo pure ottenuto le seguenti relazioni fra gli elementi del tetragono piano:

$$\left\{\begin{aligned} a' &= \frac{b \operatorname{sen} C}{k} \operatorname{sen}(\alpha - A) = \frac{c \operatorname{sen} B}{k} \operatorname{sen}(\alpha - A) \\ b' &= \frac{c \operatorname{sen} A}{k} \operatorname{sen}(\beta - B) = \frac{a \operatorname{sen} C}{k} \operatorname{sen}(\beta - B) \\ c' &= \frac{a \operatorname{sen} B}{k} \operatorname{sen}(\gamma - C) = \frac{b \operatorname{sen} A}{k} \operatorname{sen}(\gamma - C), \end{aligned}\right. \tag{8}$$

dove il valore di k è dato da una qualunque delle seguenti espressioni:

$$\left\{\begin{aligned} K^2 &= \operatorname{sen}^2\alpha \operatorname{sen}^2(\beta - B) + \operatorname{sen}^2\beta \operatorname{sen}^2(\alpha - A) + 2 \operatorname{sen}\alpha \operatorname{sen}\beta \operatorname{sen}(\alpha - A) \operatorname{sen}(\beta - B) \cos C \\ K^2 &= \operatorname{sen}^2\beta \operatorname{sen}^2(\gamma - C) + \operatorname{sen}^2\gamma \operatorname{sen}^2(\beta - B) + 2 \operatorname{sen}\beta \operatorname{sen}\gamma \operatorname{sen}(\beta - B) \operatorname{sen}(\gamma - C) \cos R \\ K^2 &= \operatorname{sen}^2\gamma \operatorname{sen}^2(\alpha - A) + \operatorname{sen}^2\alpha \operatorname{sen}^2(\gamma - C) + 2 \operatorname{sen}\gamma \operatorname{sen}\alpha \operatorname{sen}(\gamma - C) \operatorname{sen}(\alpha - A) \cos B \end{aligned}\right. \tag{9}$$

(*) *Periodico di Matematica*, 1886, LORIA, "Intorno ad alcune relazioni fra distanze" p. 38

(**) *Atti R. Accademia dei Lincei*, fasc. giugno 1899. G. DELITALA, "Formole definitive di risoluzione del problema di Pothenot".

Fra le due incognite ausiliarie q e K si ha quindi la relazione

$$(10) \qquad \frac{q}{K}=\frac{a}{\operatorname{sen}A}=\frac{b}{\operatorname{sen}B}=\frac{c}{\operatorname{sen}C}.$$

Dalle precedenti formule si deducono facilmente le seguenti:

$$(11) \qquad \begin{cases} \dfrac{aa'}{bb'}=\dfrac{\operatorname{sen}(\alpha-A)}{\operatorname{sen}(\beta-B)} \\ \dfrac{bb'}{cc'}=\dfrac{\operatorname{sen}(\beta-B)}{\operatorname{sen}(\gamma-C)} \\ \dfrac{cc'}{aa'}=\dfrac{\operatorname{sen}(\gamma-C)}{\operatorname{sen}(\alpha-A)}; \end{cases}$$

e quindi la doppia eguaglianza

$$(12) \qquad \frac{aa'}{\operatorname{sen}(\alpha-A)}=\frac{bb'}{\operatorname{sen}(\beta-B)}=\frac{cc'}{\operatorname{sen}(\gamma-C)}=\frac{2\Omega}{K}.$$

Inoltre dalle (1) e (5) si deduce:

$$(13) \qquad (\alpha-A)+(\beta-B)+(\gamma-C)=\pi.$$

Si osserva che fra gli elementi del tetragono piano, oltre le tre relazioni del triangolo base esistono quattro relazioni distinte per es. le (5) e (6) oppure le (5) e (8); quindi dati cinque dei suoi elementi si possono in generale determinare gli altri sette incogniti.

È notevole l'analogia fra le formule di risoluzione del triangolo rettilineo e quelle del tetragono piano, inoltre i quattro casi di risoluzione del triangolo corrispondono ai quattro casi principali di risoluzione del tetragono.

Infatti nel triangolo sono dati:

1° Caso. — La base (lato) e due angoli (a, B, C).
2° „ „ „ un lato e un angolo opposto (a, b, B).
3° „ „ „ un lato e un angolo compreso (a, b, C).
4° „ „ „ e due lati (a, b, c).

Nel tetragono i dati sono:

1° Caso. — La base (triangolo) e due angoli (t, β, γ).
2° „ „ „ un lato e l'angolo opposto (t, b', β).
3° „ „ „ un lato e un angolo adiacente (t, b', γ).
4° „ „ „ e due lati (t, b', C').

Qualora i dati del problema fossero cinque lati, si potrebbe calcolare direttamente il sesto lato mediante la relazione (4), e quindi calcolare gli elementi angolari colle note formule di trigonometria.

Esaminiamo brevemente come l'uso delle nostre formule conduce alla risoluzione del tetragono piano nei quattro casi principali accennati:

1° Caso. — I dati sono: t (ossia tre elementi del triangolo basso) β e γ; e si devono trovare gli altri elementi incogniti del tetragono. Si ricava l'angolo α dalla (5); quindi si possono calcolare i tre lati a', b', c' applicando le formule (6), oppure la (8), previo il calcolo di q o di K.

2° Caso. — I dati sono: la base t, un lato b' e l'angolo opposto β. Si può far uso delle (6) e (7) oppure delle formule (8) e (9).