ARTICOLO DECIMO

Sui numeri primi e sui problemi dell'analisi indeterminata
di UMBERTO SCARPIS a Bologna.

CAPITOLO I.

NUMERI PRIMI

Introduzione. — Le proprietà inerenti ai numeri interi ed alla divisibilità che, nelle opere di LEGENDRE, GAUSS, DIRICHLET sono state raccolte a formare un corpo di dottrina « l'Aritmetica in senso stretto o teoria dei numeri », formarono oggetto di ricerca fino dai matematici più antichi.

Esse fermarono in ispecie l'attenzione dei pitagorici, che a talune curiose relazioni connettevano un carattere mistico, e nel successivo sviluppo delle Matematiche in Grecia, non furono mai totalmente neglette, sebbene la scoperta delle grandezze incommensurabili richiamasse di preferenza il pensiero greco sulla Geometria come su scienza *più generale.*

Così nei libri VII, VIII, IX degli *Elementi di Euclide*, vero codice della Matematica greca, sono contenute le principali proposizioni intorno ai divisori e ai multipli, e l'algoritmo delle divisioni successive per la ricerca del m. c. d. di due numeri che il DIRICHLET considera come la chiave di volta di tutto l'edificio della Teoria dei numeri; vi si trovano pure i teoremi sui numeri primi ed in particolare quello che « la serie dei numeri primi è illimitata ».

Oltre a ciò vi si trova trattata l'equazione pitagorica

$$x^2 + y^2 = z^2$$

alla cui risoluzione in numeri interi avevano contribuito quasi tutti i matematici, commentatori ed esplicatori del teorema

che fornisce la relazione fra i quadrati dei lati di un triangolo rettangolo, e tra questi PLATONE. Inoltre viene pur data la formula secondo cui, se $2^{n+1} - 1$ è un numero primo, il prodotto

$$2^n \cdot (2^{n+1} - 1)$$

è un numero *perfetto*, cioè eguale alla somma dei suoi divisori non esclusa l'unità.

Il teorema che la serie dei numeri primi è illimitata dava in qualche modo un'indicazione, se non una risposta, alla domanda che naturalmente dovette porsi già allo spirito dei matematici antichi di « assegnare tutti i numeri primi ».

Una risposta positiva a questa domanda essi cercarono solo attraverso metodi empirici come il *crivello* di ERATOSTENE che, com'è noto, consiste nel separare dalla successione degli interi protratta fino ad un certo limite n, da prima i numeri pari, quindi i multipli di 3 e così di seguito fino a quelli della radice quadrata intera di n, dopo di chè quelli che ancor rimangono sono manifestamente primi.

Nè DIOFANTO ALESSANDRINO (a cui si deve la trattazione dei problemi d'analisi indeterminata, v. Cap. II), nè i matematici del Rinascimento sembrano aver superato questo stadio del problema, non trovandovi invece altro contributo ad esso che la semplificazione del metodo primitivo di ERATOSTENE per la costruzione di « Tavole dei numeri primi » come risulta da alcuni lavori di PELL, LAMBERT, EULERO e da altri più recenti di GLAISHER e di BERTELSEN.

Solo con LEGENDRE il problema stesso viene posto come vero oggetto di ricerca matematica che viene tutt'ora continuata secondo due diversi indirizzi.

a) Valendosi della conoscenza di alcuni numeri primi di un dato intervallo, determinare il numero di tutti quelli contenuti nell'intervallo stesso (LEGENDRE, MEISSEL, ROGEL, TORELLI, CIPOLLA ecc.).

b) Dato un numero x reale e positivo, indipendentemente dalla conoscenza di numeri primi, costruire una funzione della x tale che, per ogni valore della variabile, dia il numero degli interi primi non superiori ad x (TCHEBYCHEFF, RIEMANN, LEVI-CIVITA ecc.).

In questo Capitolo riporteremo in primo luogo una soluzione del problema *a*), che si ottiene con metodi elementari e che, non richiedendo novità di concetti, si può considerare come una diretta derivazione dell'opera Euclidea; e successivamente, in modo compatibile coi limiti assegnati a questo lavoro, verranno riassunti alcuni dei più importanti lavori nei quali, col potente sussidio dell'Analisi, si giunse a risolvere la seconda e più difficile questione.

§ 1. **La serie dei numeri primi è illimitata. - Il teorema di Wilson.** — Essendo n un intero qualunque, indichiamo con π il prodotto dei numeri primi non superiori ad n.

Degli $(n-1)$ numeri

$$\pi+2;\quad \pi+3;\quad \pi+4;\ldots.\quad \pi+n$$

nessuno è primo poichè divisibile per qualcuno dei numeri primi inferiori ad n, e ne risulta che nella successione dei numeri naturali esistono degli intervalli di ampiezza arbitrariamente grande e tali che nessuno dei numeri che li compongono è primo.

Questo fatto può ingenerare il dubbio che la serie dei numeri primi sia limitata; ma come ha già dimostrato EUCLIDE si prova immediatamente che ciò non è.

Detti infatti:

$$p_1=2\quad p_2=3\ldots.\quad p_r$$

i primi r numeri primi consecutivi, consideriamo la

$$P=p_1\cdot p_2\ldots.p_r+1. \tag{1}$$

Se P non è primo deve tuttavia ammettere sempre un divisore primo, e siccome tale non può essere nè p_1, nè p_2,.... nè p_r, resta provata sempre l'esistenza di altri numeri primi oltre a quelli considerati.

Alla stessa conclusione si perviene sostituendo alla (1) l'espressione

$$P=1\cdot 2\ldots.n+1 \tag{2}$$

che, se non è un numero primo, non può essere multipla di alcuno dei numeri inferiori ad n e deve quindi possedere uno o più divisori primi maggiori di n.

Cercando appunto questi divisori si trova che, ogni qualvolta $n+1$ sia primo, uno di essi è il numero $(n+1)$ stesso; mentre che se $n+1$ non è primo, non può esser P multiplo nè di $(n+1)$ nè di alcuno dei suoi divisori.

Si ha con ciò una proprietà atta a definire i numeri primi ed a fornire un criterio per decidere se un dato numero è primo o no.

Tale proprietà venne enunciata per primo dal WILSON senza però farne conoscere la dimostrazione, e quella che qui riportiamo è dovuta ad EULERO.

Teorema di WILSON. « Se p è primo l'espressione:

$$1 \cdot 2 \cdot 3 \ldots (p-1)+1$$

è divisibile per p e reciprocamente ».

Detto r un intero qualunque compreso tra 0 e p (estremi esclusi), i termini della progressione

$$(1) \qquad 0, \quad r, \quad 2r, \ldots \quad (p-1)r$$

divisi per p danno resti disuguali; poichè se due di essi dessero resti eguali, per es. hr, kr, la loro differenza $r(k-h)$ dovrebbe esser multipla di p il quale, essendo primo con r, dovrebbe dividere la differenza $k-h$ evidentemente minore di p la qual cosa è assurda.

Segue che i numeri (1) divisi per p daranno per resti p numeri che coincideranno a meno dell'ordine con

$$0, \quad 1, \quad 2, \ldots \quad (p-1)$$

e si potrà affermare che tra di essi ve ne sarà uno, ma uno solo, il cui resto sia l'unità, e sia questo $s \cdot r$.

Seguendo EULERO gl'interi s ed r si diranno *coniugati* rispetto a p.

Ad ogni intero r tale che $0 < r < p$, corrisponderà un unico coniugato, e quindi a due numeri diversi r, r' verranno subordinati due coniugati s, s' pure tra loro diversi.

Segue che gli elementi

$$(1) \qquad 1, \quad 2, \quad 3, \ldots \quad (p-1)$$

si possono porre in corrispondenza biunivoca con se stessi, considerando come corrispondenti due coniugati.

Cerchiamo ora quali e quante sono le coppie ad elementi coniugati tra loro eguali.

Come si vede subito 1 e $(p-1)$ sono coniugati di se stessi; ma, oltre a questi, non ve ne sono altri dotati dell'istessa proprietà.

Ammesso infatti che $\alpha \cdot \alpha$ desse per resto 1, se ne dedurrebbe che

$$\alpha^2 - 1 = (\alpha + 1)(\alpha - 1)$$

dovrebbe esser multiplo di p, la qual cosa, per $\alpha < p$, può verificarsi solo se $\alpha = 1$, oppure $\alpha = p - 1$.

Consideriamo ora i prodotti dei termini di tutte le possibili coppie di numeri coniugati

$$(2) \qquad 1 \cdot 1; \quad (p-1)(p-1); \quad 2 \cdot \alpha_2; \quad 3 \cdot \alpha_3; \ldots \frac{p-3}{2} \cdot \alpha_{\frac{p-3}{2}}$$

il cui prodotto, diviso per p, darà pure per resto 1.

Ma essendo $\alpha_2, \alpha_3, \ldots \alpha_{\frac{p-3}{2}}$ tutti tra loro diversi e diversi da $1, 2, 3, \ldots \frac{p-3}{2}, (p-1)$ il prodotto dei numeri (2) si potrà indicare con:

$$1 \cdot 2 \cdot 3 \ldots (p-1) \cdot (p-1) = kp + 1$$

$$1 \cdot 2 \cdot 3 \ldots (p-1) \cdot p - 1 \cdot 2 \cdot 3 \ldots (p-1) = kp + 1$$

ed in fine:

$$(3) \qquad 1 \cdot 2 \cdot 3 \ldots (p-1) + 1 = k \cdot p$$

Per la reciproca, basta osservare che se sussiste la (3), p dev'essere primo: poichè, diversamente, ogni suo divisore primo compreso necessariamente tra i fattori

$$1, \quad 2, \quad 3, \ldots \quad (p-1)$$

dovrebbe dividere l'unità.

§ 2. **La funzione $E(x)$ di Legendre. - Definizione. - Proprietà. - Applicazioni.** — Indichiamo, secondo LEGENDRE, con $E\left(\frac{a}{b}\right)$ la parte intera del quoziente dei due interi positivi a, b. Sarà quindi:

$$E\left(\frac{a}{b}\right) \leq \frac{a}{b} \qquad a = E\left(\frac{a}{b}\right) \cdot b + r$$

dove r è il resto positivo della divisione di a per b.

Lemma 1°. « Se $n = a + b + \ldots$, si avrà:

$$E\left(\frac{n}{p}\right) \geq E\left(\frac{a}{p}\right) + E\left(\frac{b}{p}\right) + \ldots$$

essendo n, a, b.... p interi positivi ».

Dall'ipotesi segue:

$$\frac{n}{p} = \frac{a}{p} + \frac{b}{p} + \ldots$$

ed indicando rispettivamente con r, r', r'' i resti delle divisioni $\frac{n}{p}$, $\frac{a}{p}$, $\frac{b}{p}$....

$$\frac{n}{p} = E\left(\frac{n}{p}\right) + \frac{r}{p}$$

$$\frac{a}{p} = E\left(\frac{a}{p}\right) + \frac{r'}{p}$$

$$\frac{b}{p} = E\left(\frac{b}{p}\right) + \frac{r''}{p}$$

$$\ldots\ldots\ldots$$

e quindi:

$$E\left(\frac{n}{p}\right) + \frac{r}{p} = E\left(\frac{a}{p}\right) + \frac{r'}{p} + E\left(\frac{b}{p}\right) + \frac{r''}{p} + \ldots.$$

Se ora

$$\frac{r'}{p} + \frac{r''}{p} + \ldots < 1$$

perchè sussista la precedente eguaglianza dev'essere manifestamente essendo pure $\frac{r}{p} < 1$:

$$\frac{r'}{p} + \frac{r''}{p} + \ldots = \frac{r}{p}$$

ed in conseguenza

$$E\left(\frac{n}{p}\right) = E\left(\frac{a}{p}\right) + E\left(\frac{b}{p}\right) + \ldots.$$

Se invece

$$\frac{r'}{p} + \frac{r''}{p} + \ldots \geq 1$$

si deduce:

$$E\left(\frac{n}{p}\right) > E\left(\frac{a}{p}\right) + E\left(\frac{b}{p}\right) + \ldots.$$

Lemma 2°. « Se n, a, b sono interi positivi qualunque, sussiste la relazione:

$$E\left(\frac{n}{a \cdot b}\right) = E\left(\frac{E\left(\frac{n}{a}\right)}{b}\right) \text{».}$$

Se r è il resto di $\frac{n}{a}$ si ha:

$$n = E\left(\frac{n}{a}\right) \cdot a + r$$

e dividendo primo e secondo membro per $a \cdot b$:

$$\frac{n}{a \cdot b} = \frac{E\left(\frac{n}{a}\right)}{b} + \frac{r}{a \cdot b}$$

ed indicando con r' il resto di $\frac{E\left(\frac{n}{a}\right)}{b}$

$$\frac{n}{a \cdot b} = E\left(\frac{E\left(\frac{n}{a}\right)}{b}\right) + \frac{r'}{b} + \frac{r}{ab}.$$

I resti r, r' sono rispettivamente minori di a, b; ed anche attribuendo loro i massimi valori dei quali sono suscettibili, vale a dire $a - 1$, $b - 1$, la somma $\frac{r'}{b} + \frac{r}{a \cdot b}$ risulta sempre inferiore all'unità, per cui:

$$E\left(\frac{n}{a \cdot b}\right) = E\left(\frac{E\left(\frac{n}{a}\right)}{b}\right).$$

Osservazione. « Dalla dimostrazione stessa risulta che le divisioni per a e per b si possono invertire, ed è facile estendere questa proposizione ad un numero qualsiasi di divisori ».

Passiamo ora ad applicare i due lemmi precedenti alla risoluzione del seguente

Problema. « Determinare la più alta potenza del numero primo $p \leq n$ che divide il prodotto:

$$\pi(n) = 1 \cdot 2 \cdot 3 \ldots . n \text{ ».}$$

Si scorge intanto che tra i fattori di $\pi(n)$ sono divisibili per p solo i seguenti:

$$p,\quad 2p,\quad 3p,\ldots.E\left(\frac{n}{p}\right)\cdot p$$

e siccome i rimanenti non hanno alcuna influenza sul valore dell'esponente della più alta potenza di p che divide $\pi(n)$, la questione è così ridotta alla determinazione della massima potenza di p che divide il prodotto

$$(1)\qquad 1\cdot 2\cdot 3\ldots.E\left(\frac{n}{p}\right)\cdot p^{E\left(\frac{n}{p}\right)}.$$

Tra i fattori di (1) sono divisibili per p solo i seguenti:

$$p,\quad 2p,\quad 3p,\ldots.E\left(\frac{E\left(\frac{n}{p}\right)}{p}\right)\cdot p,\quad p^{E\left(\frac{n}{p}\right)}$$

per cui tenendo conto del *Lemma* 2° per il quale:

$$E\left(\frac{E\left(\frac{n}{p}\right)}{p}\right)=E\left(\frac{n}{p^2}\right)$$

risulta manifesto che la potenza della più alta potenza di p che divide (1) dipende dall'analoga determinazione pel prodotto:

$$1\cdot 2\cdot 3\ldots.E\left(\frac{n}{p^2}\right)\cdot p^{E\left(\frac{n}{p^2}\right)}\cdot p^{E\left(\frac{n}{p}\right)}.$$

Procedendo a questo modo e considerando che la successione:

$$E\left(\frac{n}{p}\right),\quad E\left(\frac{n}{p^2}\right),\quad E\left(\frac{n}{p^3}\right)\ldots.$$

è limitata, concluderemo che il più alto esponente della potenza di p che divida $\pi(n)$ vien dato dalla somma:

$$E\left(\frac{n}{p}\right)+E\left(\frac{n}{p^2}\right)+E\left(\frac{n}{p^3}\right)\ldots.$$

Applicando ora i risultati ottenuti, possiamo dimostrar il

Teorema. « Se n, a, b, c sono interi positivi ed $n = a + b + c ....$, l'espressione

$$\frac{\pi(n)}{\pi(a) \cdot \pi(b) \cdot \pi(c)}$$

è un numero intero ».

Cominciamo dall'osservare intanto che la proposizione sarà dimostrata qualora si possa provare che il numeratore contiene i fattori primi del denominatore con esponente non minore.

In fatti sia p un certo numero primo che divide il denominatore.

Allora:

$$E\left(\frac{a}{p}\right) + E\left(\frac{a}{p^2}\right) + ...$$

$$E\left(\frac{b}{p}\right) + E\left(\frac{b}{p^2}\right) + ...$$

$$E\left(\frac{c}{p}\right) + E\left(\frac{c}{p^2}\right) + ...$$

saranno rispettivamente gli esponenti delle più alte potenze di p che dividono i prodotti $\pi(a)$, $\pi(b)$, $\pi(c)$.... e quindi l'esponente della più alta potenza di p che divide il denominatore sarà dato dalla loro somma (1).

D'altra parte:

$$E\left(\frac{n}{p}\right) + E\left(\frac{n}{p^2}\right) + ...$$

è l'esponente della maggior potenza di p che divide il numeratore, per cui tutto si riduce a dimostrare che quest'ultima somma non è minore della precedente.

Poichè $n = a + b + c ....$, segue dal *Lemma 1°*

$$E\left(\frac{n}{p}\right) \geq E\left(\frac{a}{p}\right) + E\left(\frac{b}{p}\right) + E\left(\frac{c}{p}\right) ....$$

$$E\left(\frac{n}{p^2}\right) \geq E\left(\frac{a}{p^2}\right) + E\left(\frac{b}{p^2}\right) + E\left(\frac{c}{p^2}\right)$$

. . . . . .

(1) Se eventualmente $p > a ....$, sarebbe $E\left(\frac{a}{p}\right) = 0 ....$ ecc.

Sommando membro a membro si viene quindi a concludere che l'esponente della più alta potenza di p che divide il numeratore non è inferiore all'analogo per il denominatore, e siccome il dividendo viene così a contenere tutti i fattori primi del divisore con esponente non minore, si conclude che l'espressione proposta è un numero intero.

Corollario 1°. « La frazione

$$\frac{(n+1)(n+2)\ldots(n+r)}{1\cdot 2\ldots r} = \frac{\pi(n+r)}{\pi(r)\cdot\pi(n)}$$

è un intero ».

Corollario 2°. « Essendo p, r interi positivi ed $r \leq p$

$$\frac{p(p-1)\ldots(p-r+1)}{1\cdot 2\ldots r}$$

è un intero, e se p è primo, divisibile per p ».

La prima parte discende immediatamente dal *Corollario 1°* essendo:

$$\frac{p(p-1)(p-2)\ldots(p-r+1)}{1\cdot 2\ldots r} = \frac{\pi(p)}{\pi(r)\cdot\pi(p-r)}$$

e per la seconda osserviamo che per $r < p$ si ha:

$$E\left(\frac{p}{p}\right)=1, \quad E\left(\frac{r}{p}\right)=E\left(\frac{p-r}{p}\right)=0.$$

Allo stesso tipo delle proposizioni precedenti appartengono alcune altre di cui ci limitiamo a riportare l'enunciato.

« Se a, b sono interi positivi qualunque

$$\frac{\pi(2a)\cdot\pi(2b)}{\pi(a)\pi(a+b)\cdot\pi(b)}$$

è un numero intero: e parimenti

$$\frac{\pi(4a)\cdot\pi(4b)}{\pi(a)\pi(b)\pi(2a+b)\pi(2b+a)} \text{ ».}$$

la prima delle quali è dovuta a CATALAN e la seconda a LANDAU [1].

[1] Della proposizione di CATALAN si può leggere una dimostrazione semplice e del tutto elementare nei « Elemente der Zahlenteorie » del BACHMANN. Lipsia, 1892, pag. 37.

Del pari, merita di venir ricordato il *Teorema* dovuto contemporaneamente a TCHEBYCHEF e DE POLIGNAC, e la cui dimostrazione non esige cognizioni speciali bastando all'uopo quanto è stato esposto nei paragrafi precedenti (1).

« Convenendo di chiamare *fattoriale primitivo d'ordine* q il prodotto $\theta_q(n)$ dei numeri primi a partire da 2, le cui potenze q^{esime} non superino il numero positivo, intero o frazionario n, e ponendo pure per convenzione:

$$\theta_q(n) = 1 \quad \text{per} \quad n < 2^q$$

sussiste la relazione:

$$\pi(E(n)) = \Theta\left(\frac{n}{1}\right) \cdot \Theta\left(\frac{n}{2}\right) \cdot \Theta\left(\frac{n}{3}\right) \ldots \Theta\left(\frac{n}{n}\right)$$

avendo posto per semplicità:

$$\Theta\left(\frac{n}{i}\right) = \theta_1\left(\frac{n}{i}\right) + \theta_2\left(\frac{n}{i}\right) + \theta_3\left(\frac{n}{i}\right) \ldots$$

§ 3. **Definizione, proprietà e forma della funzione**

$$\Phi(n;\ a_1,\ a_2 \ldots a_i)$$

che dà il numero degli interi non superiori ad n e non divisibili per alcuno degli a, primi tra loro due a due - Funzione indicatrice di Gauss. — Indichiamo col simbolo

$$\Phi(n;\ a_1 a_2 \ldots a_i)$$

quanti sono i termini della successione

$$(1) \qquad 1,\ 2,\ 3, \ldots n$$

non divisibili per alcuno dei numeri $a_1, a_2, \ldots a_i$ che, al pari di n, supponiamo interi positivi e, per di più, primi tra loro due a due.

Ciò premesso, dimostriamo il seguente *Lemma*:

« $$\Phi(n;\ a_1 a_2 \ldots a_i) = \Phi(n,\ a_1 a_2 \ldots a_{i-1}) - \Phi\left(E\left(\frac{n}{a_i}\right);\ a_1 a_2 \ldots a_{i-1}\right)$$ ».

(1) E. LUCAS, *Theorie des nombres*, cap. XX, § 205.

Infatti l'insieme dei $\Phi(n, a_1 a_2 ..., a_{i-1})$ numeri della successione (1) non divisibili per a_1, a_2,.... a_{i-1} si compone dei termini di (1) non divisibili per a_1, a_2,.... a_{i-1}, a_i; e dell'insieme di quelli che non sono multipli di a_1, a_2,.... a_{i-1}, ma divisibili per a_i.

Ma in (1) gli elementi divisibili per a_i sono i seguenti

$$(2) \qquad a_i, \quad 2a_i, \quad 3a_i, \cdot ka_i .... E\left(\frac{n}{a_i}\right) \cdot a_i,$$

e siccome, per essere gli a primi tra loro due a due, un elemento di (2) può essere divisibile per a_1, a_2,.... a_{i-1} solo quando lo sia il suo coefficiente k, ne segue che i termini di (2) soddisfacenti alla condizione di non esser divisibile per a_1, a_2,.... a_{i-1} saranno tanti quanti quelli di

$$1, \quad 2, \quad 3 .... k .... E\left(\frac{n}{a_i}\right)$$

dotati della stessa proprietà cioè: $\Phi\left(E\left(\frac{n}{a_i}\right); a_1, a_2 .... a_{i-1}\right)$ e se ne deduce pure che altrettanti saranno gli elementi di (1) multipli di a_i e non di a_1, $a_2 .... a_{i-1}$, con che resta dimostrato il *Lemma* posposto.

Applicando ora il *Lemma* precedente possiamo determinare la forma della funzione Φ.

Per $i = 1$, abbiamo intanto

$$\Phi(n; a_1) = n - E\left(\frac{n}{a_1}\right).$$

Per $i = 2$

$$\Phi(n; a_1 a_2) = \Phi(n; a_1) - \Phi\left(E\left(\frac{n}{a_2}\right); a_1\right) =$$

$$= n - E\left(\frac{n}{a_1}\right) - E\left(\frac{n}{a_2}\right) + E\left(\frac{E\left(\frac{n}{a_2}\right)}{a_1}\right)$$

e pel § 2° *Lemma* 2°:

$$\Phi(n; a_1 a_2) = n - E\left(\frac{n}{a_1}\right) - E\left(\frac{n}{a_2}\right) + E\left(\frac{n}{a_1 a_2}\right)$$

che si può esprimere simbolicamente scrivendo:

$$\Phi(n; a_1 a_2) = n\left(1 - \frac{1}{a_1}\right)\left(1 - \frac{1}{a_2}\right)$$

qualora si convenga di sostituire alle frazioni che risultano dallo sviluppo del secondo membro, le loro parti intere.

Ammesso ora che per $i = 1, 2, \ldots (i-1)$ si sia trovato:

$$\Phi(n;\ a_1 a_2 \ldots a_{i-1}) = n\left(1-\frac{1}{a_1}\right)\left(1-\frac{1}{a_2}\right)\ldots\left(1-\frac{1}{a_{i-1}}\right)$$

si ottiene subito:

$$\Phi(n;\ a_1 a_2 \ldots a_i) = \Phi(n;\ a_1 \ldots a_{i-1}) - \Phi\left(E\left(\frac{n}{a_i}\right);\ a_1 \ldots a_{i-1}\right) =$$

$$= n\left(1-\frac{1}{a_1}\right)\ldots\left(1-\frac{1}{a_{i-1}}\right) - E\left(\frac{n}{a_i}\right)\left(1-\frac{1}{a_1}\right)\ldots\left(1-\frac{1}{a_{i-1}}\right) =$$

$$= n - \Sigma_r E\left(\frac{n}{a_r}\right) + \Sigma_{r,s} E\left(\frac{n}{a_r a_s}\right) \ldots + \ldots$$

$$\ldots + (-1)^{i-1} E\left(\frac{n}{a_1 a_2 a_{i-1}}\right) -$$

$$- \left(E\left(\frac{n}{a_i}\right) - \Sigma_r E\left(\frac{n}{a_i a_r}\right) + \Sigma_{rs} E\left(\frac{n}{a_i a_r a_s}\right) \ldots \right.$$

$$\left. + (-1)^{i-1} E\left(\frac{n}{a_i a_1 a_2 \ldots a_{i-1}}\right)\right)$$

dove le sommatorie rispetto agli indici r, s..., vanno estese da 1 ad $i-1$.

Togliendo poi le parentesi nel secondo membro e raggruppando i termini simili risulta:

$$\Phi(n;\ a_1 a_2 \ldots a_i) = n - \Sigma_r E\left(\frac{n}{a_r}\right) + \Sigma_{r,s} E\left(\frac{n}{a_r a_s}\right)$$

$$\ldots + (-1)^i E\left(\frac{n}{a_1 a_2 \ldots a_i}\right)$$

dove le sommatorie vanno estese da 1 ad i ed in fine:

$$\Phi(n;\ a_1 \cdot a_2 \ldots a_i) = n\left(1-\frac{1}{a_1}\right)\left(1-\frac{1}{a_2}\right)\ldots\left(1-\frac{1}{a_i}\right).$$

Se poi $a_1, a_2, \ldots a_i$ coincidono con i fattori primi dell'intero n, la $\Phi(n; a_1 a_2 \ldots a_i)$ ci dà manifestamente il numero degli interi non superiori ad n e primi con esso e coincide con la *funzione indicatrice* di GAUSS che brevemente si rappresenta con $\varphi(n)$.

§ 4. **Proprietà della funzione $\varphi(n)$. - Definizione di funzione aritmetica e d'integrale numerico.** — La grande importanza della funzione indicatrice, non solo nella Teoria dei numeri, ma anche in molte questioni di Algebra, c'inducono ad approfondirne la conoscenza studiando qualcuna delle principali sue proprietà ed accennando ad altre.

In primo luogo, posto che n, risolto nei suoi fattori primi abbia la forma:

$$n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \dots p_i^{\alpha_i}$$

ne viene:

$$\varphi(n) = n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\dots\left(1-\frac{1}{p_i}\right)$$

$$= p_1^{\alpha_1-1} \cdot p_2^{\alpha_2-1} \dots p_i^{\alpha_i-1}(p_1-1)(p_2-1)\dots(p_i-1).$$

Dalla forma di $\varphi(n)$ discende:

Corollario 1°. « Se $a, b, c\dots$ sono primi tra loro due a due:

$$\varphi(a \cdot b \cdot c\dots) = \varphi(a) \cdot \varphi(b) \cdot \varphi(c)\dots \text{ ».}$$

Corollario 2°. « Se $1, d, d', d''\dots n$ sono tutti i divisori di n

$$\varphi(1) + \varphi(d) + \varphi(d') + \dots + \varphi(n) = n \text{ ».}$$

Osservazione. « Facciamo notare, per di più, che una volta stabilito il Corollario 1° indipendentemente dalla forma di $\varphi(n)$, esso può servire alla determinazione della forma stessa osservando, com'è facile provare, che

$$\varphi(p^\nu) = p^{\nu-1} \cdot (p-1) \text{ ».}$$

Anche il Corollario 2° può venir dedotto dalla sola definizione di $\varphi(n)$, come segue.

Determiniamo, in primo luogo, quanti tra i numeri

$$(1) \qquad 1,\ 2,\ 3\dots n$$

abbiano con n per *m. c. d.* un certo numero δ.

Potranno intanto trovarsi in queste condizioni

$$\delta,\ 2\delta,\ 3\delta,\dots\ k\delta,\dots\ \frac{n}{\delta}\cdot\delta$$

ma per le note proprietà del *m. c. d.*, avranno con n per

m. c. d. δ, tutti e solo quei termini $k \cdot \delta$ pei quali k è primo con $\frac{n}{\delta}$, il cui numero sarà quindi $\varphi\left(\frac{n}{\delta}\right)$.

Se ora indichiamo con $\delta_1 \delta_2 \ldots \delta_\nu$ tutti i divisori di n da 1 ad n, estremi inclusi, tra i numeri (1) ve ne saranno

$$\varphi\left(\frac{n}{\delta_1}\right) \text{ a massimo comun divisore } \delta_1 = 1$$

$$\varphi\left(\frac{n}{\delta_2}\right) \quad \text{» } \quad \delta_2$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$\varphi\left(\frac{n}{\delta_\nu}\right) \quad \text{» } \quad \delta_\nu = n$$

e poichè così vengono completamente esauriti, segue che

$$\sum_{i=1}^{i=\nu} \varphi\left(\frac{n}{\delta_i}\right) = n.$$

Ma i numeri $\frac{n}{\delta_i}$ coincidono, ordine a parte, con i divisori δ_i, per cui si conclude che

$$\sum_{i=1}^{i=\nu} \varphi(\delta_i) = n. \tag{2}$$

La funzione indicatrice appartiene alla classe delle *funzioni aritmetiche* cioè funzioni che si suppongono date per valori interi della variabile, ed al primo membro di (2) per una qualsiasi funzione aritmetica si dà il nome di *integrale numerico*.

§ 5. **Problema d' inversione dell' integrale numerico. - Esempii notevoli di funzioni ed integrali.** — Passiamo ora allo studio di una questione più generale dalla quale dedurremo nuovamente come semplice corollario, la forma di $\varphi(n)$.

Lemma. « Se n è composto dei fattori primi $p_1 p_2 \ldots p_s$, i due sistemi di numeri:

$$\alpha) \qquad n, \quad \left[\frac{n}{p_i p_j}\right], \quad \left[\frac{n}{p_i p_j p_h p_k}\right], \ldots$$

$$\beta) \qquad \left[\frac{n}{p_i}\right], \quad \left[\frac{n}{p_i p_j p_h}\right], \ldots$$

il primo dei quali si compone di n e di tutti i quozienti che si ottengono dividendolo per tutti i possibili prodotti di fattori primi disuguali presi due a due, quattro a quattro, sei a sei e così di seguito per combinazioni pari; mentre il secondo contiene i quozienti corrispondenti a combinazioni dispari, comprendono lo stesso numero di termini divisibili per uno qualunque dei divisori δ di n, escluso n ».

Indichiamo con r il numero dei fattori p che in n hanno un esponente maggiore che in δ.

Nella serie α), δ divide intanto n: e dei numeri $\frac{n}{p_i p_j}$ ne dividerà tanti quante sono le combinazioni di r elementi due a due cioè $\binom{r}{2}$, e precisamente quelli che risultano dal dividere n per ciascuna coppia di fattori p che in n hanno un esponente maggiore che in δ.

Parimenti dei quozienti del tipo $\frac{n}{p_i p_j p_h p_k}$, δ ne dividerà $\binom{r}{4}$ e così di seguito per cui la quantità dei termini di α) divisibili per δ verrà espressa da:

$$S = 1 + \binom{r}{2} + \binom{r}{4} + \ldots + \binom{r}{r}$$

se r è pari o da

$$S' = 1 + \binom{r}{2} + \binom{r}{4} + \ldots + \binom{r}{r-1}$$

se r è dispari.

Parimenti i termini di β) dotati di analoga proprietà saranno rispettivamente:

$$R = \binom{r}{1} + \binom{r}{3} + \ldots + \binom{r}{r-1}$$

$$R' = \binom{r}{1} + \binom{r}{3} + \ldots + \binom{r}{r}$$

e siccome in ogni caso

$$S = R; \quad S' = R'$$

resta dimostrato il *Lemma*.

Teorema. « Se $\varphi(n)$ è una qualsiasi funzione aritmetica della variabile intera n, tale che si abbia

$$\Sigma\varphi(\delta) = f(n) \tag{1}$$

dove la sommatoria s'intende estesa a tutti i divisori di n da 1 ad n inclusivamente, ed $f(n)$ è simbolo di un'altra funzione aritmetica, sussiste la relazione:

$$\varphi(n) = \Sigma f(\delta_1) - \Sigma f(\delta_2) \tag{2}$$

dove le due sommatorie s'intendono estese rispettivamente a tutti i numeri dei sistemi α) e β) ».

Siano δ_1, δ_2 particolari elementi di α) e β) però diversi da n.

Per l'ipotesi (1), avremo:

$$\Sigma\varphi(\delta_1') = f(\delta_1); \quad \Sigma\varphi(\delta_2') = f(\delta_2)$$

intendendo estese le sommatorie a tutti indistintamente i divisori δ_1', δ_2' di δ_1 e di δ_2.

Ma in virtù del *Lemma* precedente si trovano in egual numero tanto in α) come in β) i termini divisibili per un qualsiasi divisore particolare Δ di δ_1 o δ_2; per cui, se si immagina che nel secondo membro di (2) si ponga per ogni $f(\delta_1)$ ed $f(\delta_2)$ le rispettive sommatorie $\Sigma\varphi(\delta_1')$, $\Sigma\varphi(\delta_2')$, i termini come $\varphi(\Delta)$ si troveranno ripetuti in egual numero nel minuendo e nel sottraendo, e l'unico che non venga distrutto dal suo contrario e quello che corrisponde a $\delta_1 = n$ e $\Delta = \delta_1 = n$. Resta così dimostrata la (2).

Corollario. « Posto $f(n) = n$ da (2) si ricava:

$$\varphi(n) = \Sigma\delta_1 - \Sigma\delta_2 = \left\{ n + \left[\frac{n}{p_i p_j}\right] + \left[\frac{n}{p_i p_j p_h p_k}\right] \dots \right\} -$$

$$- \left\{ \left[\frac{n}{p_i}\right] + \left[\frac{n}{p_i p_j p_h}\right] + \dots \right\} =$$

$$= n \cdot \left\{ 1 - \Sigma\frac{1}{p_i} + \Sigma\frac{1}{p_i p_h} - \Sigma\frac{1}{p_i p_h p_k} \dots \right\} =$$

$$= n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \dots$$

e risulta così per altra via la forma di $\varphi(n)$ come conseguenza della sua proprietà caratteristica espressa dalla $\Sigma\varphi(\delta) = n$.

Osservazione. Col medesimo procedimento seguito nella dimostrazione dell'ultimo *Teorema*, si ha che, partendo invece dall'ipotesi

$$(1)' \qquad \prod_{\delta=1}^{\delta=n} \varphi(\delta) = f(n)$$

si deduce

$$(2)' \qquad \varphi(n) = \frac{\Pi f(\delta_1)}{\Pi f(\delta_2)}.$$

Ne segue che se $\varphi(n)$ è una tale funzione aritmetica che abbia il valore p se n è potenza di un numero primo p, e sia eguale ad 1 in tutti gli altri casi, si ha:

$$\prod_{\delta=1}^{\delta=n} \varphi(\delta) = n$$

e quindi per la (2)':

$$\varphi(n) = \frac{\Pi \delta_1}{\Pi \delta_2}$$

da cui risulta che il quoziente del prodotto dei numeri α) per quello dei numeri β) ha il valore p se $n = p^\lambda$ ed in tutti gli altri casi è uguale all'unità (1).

Come esempio di altre funzioni aritmetiche citiamo le seguenti.

Il numero dei divisori di n che si rappresenta con $t(n)$ e che è uguale a

$$t(n) = (\alpha_1 + 1)(\alpha_2 + 1) \ldots (\alpha_s + 1)$$

essendo $\alpha_1, \alpha_2, \ldots \alpha_s$ gli esponenti dei fattori primi di n.

La somma dei divisori di n: $\sum_{\delta=1}^{\delta=n} \delta$ e che si suol indicare con $\int(n)$ per cui:

$$\int(n) = \frac{p_1^{\alpha_1+1} - 1}{p_1 - 1} \cdot \frac{p_2^{\alpha_2+1} - 1}{p_2 - 1} \ldots \frac{p_s^{\alpha_s+1} - 1}{p_s - 1}.$$

In una lunga serie di lavori il LIOUVILLE ha stabilito molte notevoli relazioni tra le funzioni $t(n)$, $\int(n)$, $\varphi(n)$ di cui

(1) DIRICHLET, *Vorlesungen über die zahlentheorie.* Supplemente, pagina 363.

le più semplici sono:

$$\sum_{\delta=1}^{\delta=n} \int(\delta) = \sum_{\delta=1}^{\delta=n} \frac{n}{\delta} \cdot t(\delta)$$

$$\sum_{\delta=1}^{\delta=n} \varphi(\delta)\, t\left(\frac{n}{\delta}\right) = \int(n)$$

$$\sum_{\delta=1}^{\delta=n} \int(\delta) \int\left(\frac{n}{\delta}\right) = \sum_{\delta=1}^{\delta=n} \delta \cdot t(\delta) \cdot t\left(\frac{n}{\delta}\right).$$

Altra funzione importante è quella che si rappresenta con $\mu(n)$ e viene definita come segue:

$\mu(1) = 1$

$\mu(n) = 0$ se n è divisibile per un quadrato diverso dall'unità, se cioè non tutti gli esponenti dei fattori p di n sono eguali ad uno.

$\mu(n) = (-1)^s$ se n si compone di s fattori primi tra loro differenti.

Non è difficile provare che l'integrale numerico di $\mu(n)$ è nullo cioè:

$$\sum_{\delta=1}^{\delta=n} \mu(\delta) = 0.$$

Facciamo ancora notare che il procedimento che conduce alla determinazione della forma di una funzione per mezzo del suo integrale numerico, costituisce un notevole esempio di « inversione ».

La funzione $\mu(n)$ facilita considerevolmente l'inversione dell'integrale numerico, e DEDEKIND e LIOUVILLE hanno dimostrato che posto:

$$f(n) = \sum_{\delta=1}^{\delta=n} \varphi(\delta)$$

risulta:

$$\varphi(n) = \sum_{\delta=1}^{\delta=n} \mu(\delta) \cdot f\left(\frac{n}{\delta}\right)$$

la qual ultima, come è facile constatare ricordando il significato di $\mu(n)$, coincide con la

$$\varphi(n) = \Sigma f(\delta_1) - \Sigma f(\delta_2)$$

dove le sommatorie s'intendono rispettivamente estese ai numeri α), β) (1).

§ 6. **Relazione di Legendre. - Teorema di Meissel.** — Passiamo ora ad applicare alcuni dei risultati precedenti alla dimostrazione di due importanti teoremi che servono alla determinazione della quantità dei numeri primi in un dato intervallo.

A tal uopo indicheremo con $\psi(n)$ il numero dei numeri primi non superiori ad n, e con $p_1, p_2, \ldots p_a$ i numeri primi consecutivi a partire da $p_1 = 2$ fino a quello di posto a.

Ciò premesso, detto a un numero soddisfacente alla condizione:

$$\psi(\sqrt{n}) \leq a < \psi(n) \tag{1}$$

e ricordando il significato della funzione

$$\Phi(n;\ p_1,\ p_2, \ldots\ p_a)$$

definita al § 2, tra le due funzioni Φ e ψ esiste la relazione

$$\Phi(n;\ p_1 p_2 \ldots p_a) = \psi(n) - a + 1. \tag{2}$$

Notiamo, in primo luogo, che esiste sempre un intero a soddisfacente ad (1).

Dopo ciò, dei numeri

$$1,\ 2,\ 3, \ldots n$$

saranno non divisibili per $p_1, p_2, \ldots p_a$, oltre all'unità, tutti i fattori semplici non superiori ad n e diversi da $p_1\ p_2 \ldots p_a$ in numero di $\psi(n) - a$: ed oltre a questi non ve ne saranno altri.

In fatti dalla prima parte di (1)

$$\psi(\sqrt{n}) \leq a$$

risulta

$$\sqrt{n} < p_{a+1}$$

(1) Intorno alle importanti e geniali questioni che si riferiscono all'integrale numerico di una funzione aritmetica ed alla sua inversione, si possono consultare i lavori di E. Cesàro nelle « Memorie della Società scientifica di Liegi », 1883. Merita pure di esser ricordata un'estensione della funzione indicatrice dovuta al prof. L. Carlini e che servì di spunto al Cesàro per una interessante memoria sull'inversione. « Periodico di Matematica ». Anno VII, 1892, Fasc. 1°.

e quindi qualunque intero $x < n$ e non primo, non potendo risultare dal prodotto di fattori maggiori di p_a e quindi di $\sqrt{n}$ dovrà esser divisibile per uno o più dei $p_1, p_2 \ldots p_a$.

Resta così provata la (2).

Se poi si pone $a = \psi(\sqrt{n})$ la (2) si cambia nella formula di LEGENDRE

$$\psi(n) = \Phi(n;\ p_1 p_2 \ldots p_{\psi(\sqrt{n})}) + \psi(\sqrt{n}) - 1 \tag{3}$$

mediante la quale ove si conoscano i numeri primi successivi da 2 fino al massimo non superiore a $\sqrt{n}$, si potrà determinare il numero di quelli non superiori ad n.

Il calcolo della funzione

$$\Phi(n;\ p_1,\ p_2, \ldots\ p_{\psi(\sqrt{n})})$$

risulta piuttosto laborioso, e si deve a MEISSEL una trasformazione della formula di LEGENDRE in cui la Φ viene sostituita con altre di più facile determinazione.

Sia n un intero qualunque, e *fatta l'ipotesi che tra* $\sqrt[3]{n}$ *e* $\sqrt{n}$ *esista per lo meno un numero primo,* si ponga:

$$m = \psi(\sqrt[3]{n}) \quad m + \mu = \psi(\sqrt{n})$$

da cui $\mu \geq 1$; e detto quindi s un intero tale che

$$1 \leq s \leq \mu \tag{4}$$

dimostriamo intanto che si ha:

$$\psi\left(\frac{n}{p_{m+s}}\right) \geq m + s - 1 \geq \psi\left(\sqrt{\frac{n}{p_{m+s}}}\right). \tag{5}$$

Essendo $m + s \leq m + \mu$, ne discende $p_{m+s} \leq p_{m+\mu}$ e quindi $p_{m+s} \leq \sqrt{n}$ e di conseguenza:

$$\frac{n}{p_{m+s}} \geq \frac{n}{\sqrt{n}} \quad \text{cioè:} \quad \psi\left(\frac{n}{p_{m+s}}\right) \geq \psi(\sqrt{n}) = m + \mu$$

ed essendo per (1) $s \leq \mu$, si avrà *a fortiori*:

$$\psi\left(\frac{n}{p_{m+s}}\right) \geq m + s - 1$$

e resta così dimostrata la prima parte di (5).

Parimenti per (4) $m+s>m$ e quindi $p_{m+s}>\sqrt[3]{n}$ da cui:

$$\frac{n}{p_{m+s}}<\frac{n}{\sqrt[3]{n}};\quad \sqrt{\frac{n}{p_{m+s}}}<\sqrt[3]{n}$$

e quindi:

$$\psi\left(\sqrt{\frac{n}{p_{m+s}}}\right)\leq\psi(\sqrt[3]{n})=m$$

e per (4)

$$\psi\left(\sqrt{\frac{n}{p_{m+s}}}\right)\leq m+s-1$$

con che resta dimostrata la seconda parte della (5).

Notando ora che ove si ponga

$$E\left(\frac{n}{p_{m+s}}\right)=n,\quad m+s-1=a$$

la (5) viene a coincidere con la (1), segue che potremo applicare agli interi $E\left(\frac{n}{p_{m+s}}\right)$, $m+s-1$ la relazione (2) ivi dimostrata, che ponendo per brevità

$$\Phi\left(E\left(\frac{n}{p_{m+s}}\right);\quad m+s-1\right)$$

in luogo di

$$\Phi\left(E\left(\frac{n}{p_{m+s}}\right);\quad p_1,\ p_2\ldots\ldots p_{m+s-1}\right)$$

assume la forma:

$$(6)\quad \psi\left(E\left(\frac{n}{p_{m+s}}\right)\right)=\Phi\left(E\left(\frac{n}{p_{m+s}}\right);\quad m+s-1\right)+(m+s-1)-1.$$

Ma per il *Lemma* del § 2 si ha:

$$\Phi(n;\ m+s)=\Phi(n;\ m+s-1)-\Phi\left(E\left(\frac{n}{p_{m+s}}\right),\ m+s-1\right).$$

e mediante questa la (6) si cambia nella

$$(7)\quad \begin{aligned}&\Phi(n;\quad m+s-1)-\Phi(n;\quad m+s)=\\&=\psi\left(E\left(\frac{n}{p_{m+s}}\right)\right)-(m+s-1)+1.\end{aligned}$$

Facendo ora in (7) successivamente $s=1,\ 2,\ldots.\mu$ e som-

mando membro a membro, si ricava:

$$\Phi(n,\ m)-\Phi(n,\ m+\mu)=\Sigma\psi\left(E\left(\frac{n}{p_{m+s}}\right)\right)-\mu\frac{2m+\mu-1}{2}+\mu. \tag{8}$$

Ma, essendo $m+\mu=\psi(\sqrt{n})$, dalla relazione (3) di LEGENDRE si ottiene:

$$\Phi\left(n;\ \psi(\sqrt{n})\right)=\psi(n)-\psi(\sqrt{n})+1\ (^1)$$

e sostituendo in (8):

$$\psi(n)=\Phi(n;\ m)+\psi(\sqrt{n})-\sum_{s=1}^{s=\mu}\psi\left(E\frac{n}{p_{m+s}}\right)+\mu\frac{2m+\mu-1}{2}-\mu-1 \tag{9}$$

la qual ultima è l'accennata formula di MEISSEL (²).

Per meglio comprendere la portata delle due formule di LEGENDRE e di MEISSEL, e per constatare i vantaggi della seconda sulla prima, ricorreremo ad un esempio.

a) Posto $n=100$, $\psi(\sqrt{100})=4$

$$\Phi\left(n;\ \psi(\sqrt{n})\right)=\Phi(100;\ 4)=\Phi(100;\ 2,\ 3,\ 5,\ 7)=$$

$$=100\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\left(1-\frac{1}{5}\right)\left(1-\frac{1}{7}\right).$$

$$=100-E\left(\frac{100}{2}\right)-E\left(\frac{100}{3}\right)\ldots.-E\left(\frac{100}{7}\right)+$$

$$E\left(\frac{100}{2\cdot3}\right)+\ldots.+E\left(\frac{100}{5\cdot7}\right)-E\left(\frac{100}{2\cdot3\cdot5}\right)\ldots.$$

$$-E\left(\frac{100}{3\cdot5\cdot7}\right)+E\left(\frac{100}{2\cdot3\cdot5\cdot7}\right)=22$$

$$\psi(100)=22+4-1=25.$$

(¹) Ricordiamo, come si è precedentemente avvertito, che $\Phi\left(n;\ (\psi\sqrt{n})\right)$ sta in luogo di $\Phi\left(n;\ p_1p_2\ldots.p_{\psi(\sqrt{n})}\right)$.

(²) *Matematische Annalen.* Bd. II, III, XXI, XXV.

$$b)\ m = \psi(\sqrt[3]{100}) = \psi(4) = 2 \quad m + \mu = \psi(\sqrt{100}) = 4$$

$$\psi(100) = \Phi(100;\ 2) + \psi(\sqrt{100}) - \sum_{s=1}^{s=\mu=2} \psi\left(E\frac{100}{p_{2+s}}\right) + 5 - 2 - 1$$

$$= 100\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right) + 4 - \psi\left(\frac{100}{5}\right) - \psi\left(E\frac{100}{7}\right) + 5 - 2 - 1$$

$$= 100 - E\left(\frac{100}{2}\right) - E\left(\frac{100}{3}\right) + E\left(\frac{100}{2 \cdot 3}\right) + 4$$

$$- \psi(20) - \psi(14) + 5 - 2 - 1 = 25.$$

Il vantaggio notevole che la formula di MEISSEL presenta al confronto con quella di LEGENDRE, consiste in ciò che per quest'ultima occorre il calcolo di $\Phi(n;\ m + \mu) = \Phi(n;\ \psi(\sqrt{n}))$, mentre per la prima basta invece la determinazione di $\Phi(n;\ m) = \Phi(n;\ \psi(\sqrt[3]{n}))$ che riesce considerevolmente più rapida.

Sostituendo ai due limiti $\sqrt[3]{n}$, $\sqrt{n}$ rispettivamente $\sqrt[4]{n}$, $\sqrt[3]{n}$ e quindi $\sqrt[5]{n}$, $\sqrt[4]{n}$ e così di seguito sintantochè tra $\sqrt[r+1]{n}$, $\sqrt[r]{n}$ esista per lo meno un numero primo (ipotesi che come vedremo in seguito da un limite molto basso in poi è sempre ammissibile), ROGEL, seguendo un procedimento analogo è giunto a stabilire una serie di formule affini a quelle di MEISSEL, nelle quali il secondo argomento della funzione Φ diviene sempre più basso.

Giova però osservare che, mentre con la relazione di LEGENDRE basta la conoscenza di $\psi(\sqrt{n})$, con quella del MEISSEL, è necessario determinare $\psi\left(\frac{n}{p_{m+s}}\right)$ che può risultare eguale a $\psi(\sqrt[3]{n^2}) > \psi(\sqrt{n})$.

Un'osservazione analoga si può ripetere per le formule di ROGEL.

§ 7. **Riassunto del Teorema di Tchebycheff. - Postulato di Bertrand.** — Le precedenti formule di LEGENDRE-MEISSEL-ROGEL vennero successivamente perfezionate ed estese, in particolar modo da TORELLI e CIPOLLA: anche in queste però la totalità dei numeri primi in un dato intervallo viene desunta da quella di un intervallo minore.

Il primo lavoro in cui si sia affrontato con successo il problema di determinare il numero dei numeri primi di un intervallo solo in funzione dei limiti è dovuto a TCHEBYCHEFF.

In questo paragrafo, seguendo l'esposizione che ne dà il SERRET [1] procureremo di riassumere la trama di questa importante memoria, che il LUCAS giudica come una delle più interessanti della Teoria dei numeri.

Dalla formula di STIRLING [2] che serve a calcolare con forte approssimazione il fattoriale $\pi(n)$ per n molto grande, e da alcune proprietà dell'integrale euleriano di 2ª specie, detta $T(x)$ la somma dei logaritmi naturali dei numeri

$$1, \quad 2, \quad 3, \ldots \quad E(x)$$

si deduce in primo la limitazione:

$$T(x) > \log \sqrt{2\pi} + x \log x - x - \frac{1}{2} \log x$$

$$T(x) < \log \sqrt{2\pi} + x \log x - x + \frac{1}{2} \log x + \frac{1}{12}.$$

Dopo ciò, indicando con $\theta\left(\frac{x}{n}\right)^{\frac{1}{m}}$ (m, n interi positivi) la somma dei logaritmi neperiani dei numeri primi non superiori a $\sqrt[m]{\frac{x}{n}}$, si dimostra che tra le due funzioni $T(x)$, $\theta(x)$ ha luogo la relazione:

$$\begin{aligned} T(x) = {} & \theta(x) + \theta(x)^{\frac{1}{2}} + \theta(x)^{\frac{1}{3}} + \ldots \\ & + \theta\left(\frac{x}{2}\right) + \theta\left(\frac{x}{2}\right)^{\frac{1}{2}} + \theta\left(\frac{x}{2}\right)^{\frac{1}{3}} + \ldots \\ & + \theta\left(\frac{x}{3}\right) + \theta\left(\frac{x}{3}\right)^{\frac{1}{2}} + \theta\left(\frac{x}{3}\right)^{\frac{1}{3}} + \ldots \\ & \ldots\ldots\ldots\ldots\ldots\ldots \end{aligned}$$

dove le orizzontali e le verticali si devono intendere prolungate fino ad ottenere una funzione evidentemente nulla [3].

[1] SERRET, *Algebre Superieure*, tomo II.

[2] CESARO, *Analisi algebrica*, cap. XXXVIII, § 6.

[3] Si confronti questa proposizione con quella data al § 2 sotto il titolo di Teorema di TCHEBYCHEFF e POLIGNAC.

Stabiliti questi due principii, con un ingegnosissimo procedimento che mal si presta ad un riassunto, deduce da essi che la $\theta(x)$ deve soddisfare alle disuguaglianze:

$$\theta(x) < \frac{6}{5} A \cdot x - A x^{\frac{1}{2}} + \frac{5}{4 \log 6} \log^2 x + \frac{5}{2} \log x + 2 = F(x)$$

$$\theta(x) > Ax - \frac{12}{5} A x^{\frac{1}{2}} - \frac{5}{8 \cdot \log 6} \cdot \log^2 x - \frac{15}{4} \log x - 3 = f(x)$$

dove A è una costante; cioè che la somma dei logaritmi naturali dei numeri primi non superiori ad x dev'essere compresa tra i limiti $F(x)$, $f(x)$.

Sia ora m il numero che dà la totalità dei numeri primi tra l ed L (estremi inclusi). Avremo allora manifestamente:

$$\theta(L) - \theta(l) > m \log l$$

$$\theta(L) - \theta(l) < m \log L$$

da cui:

$$\frac{\theta(L) - \theta(l)}{\log L} < m < \frac{\theta(L) - \theta(l)}{\log l}.$$

Ma per i limiti precedentemente stabiliti per la $\theta(x)$:

$$f(L) < \theta(L) < F(L)$$

$$f(l) < \theta(l) < F(l)$$

per cui a fortiori:

$$\frac{f(L) - F(l)}{\log L} < m < \frac{\Gamma(L) - f(l)}{\log l}$$

e restano così determinati due limiti tra i quali deve trovarsi m.

Come corollarii di queste formule risulta in modo abbastanza semplice che, prestabilito L, si potrà sempre determinare, qualora il problema sia solubile, un limite inferiore l in modo che tra L ed l vengano a trovarsi più di k numeri primi, ed in particolare almeno 1.

Successivamente si dimostra pure che da un certo valore di n in poi tra n e $(2n - 2)$ cade sempre almeno un numero primo.

Quest'ultima proposizione è nota sotto il titolo di « postulato di BERTRAND » poichè l'illustre matematico ne usò sotto questa forma per dimostrare che l'indice di un gruppo di sostituzioni su n lettere non può essere contemporaneamente maggiore di 2 e minore di n, od in altri termini che una funzione algebrico razionale intera di n variabili indipendenti, non può assumere per tutte le permutazioni delle variabili, più di due e meno di n valori tra loro *algebricamente* diversi.

Ritornando ora alla proposizione del § 5, ricordiamo che essa venne dimostrata al coperto dell'ipotesi restrittiva che tra $\sqrt[3]{n}$ e $\sqrt{n}$ esistesse per lo meno un numero primo.

In seguito alla dimostrazione del postulato di BERTRAND, quell'ipotesi non è più necessaria.

Infatti ammessa la disuguaglianza:

$$\sqrt{n} > 2\sqrt[3]{n}$$

discende $n > 64$, e reciprocamente: per cui per $n > 64$ sarà pure

$$E(\sqrt{n}) + \theta > 2(E(\sqrt[3]{n}) + \theta')$$

dove ϑ, θ' sono < 1 ma positivi, e quindi:

$$E(\sqrt{n}) > 2 \cdot E(\sqrt[3]{n}) + (2\vartheta' - \theta)$$

cioè

$$E(\sqrt{n} > 2 \cdot E(\sqrt[3]{n}) - 2$$

per cui tra $E(\sqrt[3]{n})$ ed $E(\sqrt{n})$ a più forte ragione dovrà trovarsi un numero primo.

Analoga osservazione si può ripetere per le formule di ROGEL.

§ 8. **Cenno riassuntivo della Memoria di Riemann sul numero dei numeri primi da 1 ad n.** — Pochi anni dopo la comparsa della Memoria di TCHEBICHEFF, il RIEMANN pubblicava nel 1859 il suo classico lavoro « Über die Anzahl der Primzahlen unter gegebenen Grenze » in cui risolveva la questione di costruire una funzione del limite x atta a dare il numero dei numeri primi non superiori ad x.

Il nome illustre dell'Autore, l'enorme difficoltà del problema, e le profonde e sottili questioni di Analisi sollevate dal metodo di soluzione adottato, fecero sì che questa memoria desse principio ad una lunga serie di lavori da parte dei più eminenti analisti con lo scopo di assicurare, chiarire, semplificare i passi incerti, oscuri, complicati.

Un breve riassunto della memoria di RIEMANN è quasi impossibile, per la mole del lavoro analitico che in essa è profuso: ci limiteremo quindi a lumeggiarne per quanto è possibile, il substrato aritmetico prescindendo da tutto ciò che riguarda l'analisi.

Il principale strumento analitico a cui si ricorre è la serie armonica generalizzata $\Sigma\frac{1}{n^s}$ convergente assolutamente ed uniformemente per s reale e >1, e che tale si conserva anche per s complesso, purchè la parte reale sia $>1+\varepsilon$ dove ε è positivo ed arbitrariamente piccolo.

Come aveva già notato EULERO, la $\Sigma\frac{1}{n^s}$ gode della proprietà espressa dall'eguaglianza:

$$\Sigma\frac{1}{n^s}=\frac{1}{\Pi\left(1-\frac{1}{p^s}\right)}$$

dove il prodotto infinito viene esteso a tutti i numeri primi, e questo già accenna all'uso che verrà fatto dalla funzione $\Sigma\frac{1}{n^s}$ per risolvere la questione.

Il primo passo consiste nella determinazione del « prolungamento analitico » della $\Sigma\frac{1}{n^s}$ ed a tal uopo si determina una funzione uniforme della variabile complessa s, che, mentre coincide con $\Sigma\frac{1}{n^s}$ in quella parte del piano in cui quest'ultima è convergente, rimane pure definita in tutto il piano: tale funzione s'indicherà con $\zeta(s)$.

Dopo ciò, rappresentando con $\theta(x)$ la totalità dei numeri primi inferiori ad x, sia $f(x)$ una funzione tale che

$$f(x)=\theta(x)$$

se x non è primo, ed

$$f(x) = \theta(x) + \frac{1}{2}$$

se x è primo, ed inoltre sia $f_1(x)$ una funzione legata ad $f(x)$ dalla:

$$(1) \qquad f_1(x) = f(x) + \frac{1}{2} f\left(x^{\frac{1}{2}}\right) + \frac{1}{3} f\left(x^{\frac{1}{3}}\right) + \dots + \frac{1}{n} f\left(x^{\frac{1}{n}}\right) \dots$$

dove la successione continua fino a che si raggiunga una $f\left(x^{\frac{1}{n}}\right)$ nulla e manifestamente con tutte le seguenti.

Partendo ora dalla

$$\log \zeta(s) = \sum_p p^{-s} + \frac{1}{2} \sum_p p^{-2s} + \frac{1}{3} \sum_p p^{-2s} \dots$$

che è conseguenza dell'identità di Eulero, risolvendo un arduo problema di inversione che costituisce la parte più difficile della dimostrazione, si perviene alla formula:

$$(2) \qquad f_1(x) = \frac{1}{2\pi i} \int_{s_1 - i\infty}^{s_1 + i\infty} \frac{\log \zeta(s)}{s} x^s \cdot ds$$

dove l'integrale s'intende esteso lungo la parallela all'asse immaginario e ad una distanza da esso eguale ad s_1.

Ricordando ora il significato della funzione aritmetica $\mu(n)$ (§ 4) è facile dimostrare che se X_r, Y_s sono funzioni tali che tra di esse si abbiano le relazioni in numero finito

$$Y_1 = X_1 + X_2 + X_3 + \dots + X_m$$

$$Y_2 = X_2 + X_4 + X_6 + \dots + X_{E\left(\frac{m}{2}\right) \cdot 2}$$

$$Y_3 = X_3 + X_6 + X_9 + \dots + X_{E\left(\frac{m}{3}\right) \cdot 3}$$

. . . . ; . . . . . .

moltiplicando la prima eguaglianza per $\mu(1) = 1$, la seconda per $\mu(2) = -1$, la terza per $\mu(3) = -1$, la quarta per $\mu(4) = 0$ ecc., e sommando membro a membro risulta:

$$(3) \qquad X_1 = \mu(1) Y_1 + \mu(2) Y_2 + \mu(3) Y_3 + \dots$$

Ora per la (1) si ha:

$$f_1(x) = f(x) + \frac{1}{2} f\left(x^{\frac{1}{2}}\right) + \frac{1}{3} f\left(x^{\frac{1}{3}}\right) + \ldots.$$

$$\frac{1}{2} f_1\left(x^{\frac{1}{2}}\right) = \frac{1}{2} f\left(x^{\frac{1}{2}}\right) + \frac{1}{4} f\left(x^{\frac{1}{4}}\right) + \frac{1}{6} f\left(x^{\frac{1}{6}}\right) \ldots.$$

$$\frac{1}{3} f_1\left(x^{\frac{1}{3}}\right) = \frac{1}{3} f\left(x^{\frac{1}{3}}\right) + \frac{1}{6} f\left(x^{\frac{1}{6}}\right) + \frac{1}{9} f\left(x^{\frac{1}{9}}\right) \ldots.$$

. . . . . .

continuando così fino a che le funzioni del secondo membro, e quindi il primo, sono nulle.

Applicando la (3) si ha:

$$f(x) = \mu(1) \cdot f_1(x) + \mu(2) \frac{1}{2} f_1\left(x^{\frac{1}{2}}\right) + \mu(3) \cdot \frac{1}{3} f_1\left(x^{\frac{1}{3}}\right) + \ldots.$$

$$f(x) = f_1(x) - \frac{1}{2} f_1\left(x^{\frac{1}{2}}\right) - \frac{1}{3} f_1\left(x^{\frac{1}{3}}\right) - \frac{1}{5} f_1\left(x^{\frac{1}{5}}\right) + \frac{1}{6} f_1\left(x^{\frac{1}{6}}\right) + \ldots.$$

cioè

$$f(x) = \sum_n \frac{\mu(n)}{n} f_1\left(x^{\frac{1}{n}}\right) \tag{4}$$

dove la sommatoria s'intende estesa fino alla prima $f_1\left(x^{\frac{1}{n}}\right)$ che si annulla insieme a tutte le successive, e le $f_1\left(x^{\frac{1}{n}}\right)$ risultano determinate da (2).

La (4) è la classica formula di RIEMANN: ad essa, prescindendo dalla sua complessità per cui è da considerarsi più che altro come dotata di un valore potenziale ben difficilmente attuabile, sono stati mossi parecchi appunti (1).

Così, ad esempio, si può osservare che in conseguenza dell'uso della funzione $\mu(n)$, il cui valore si ottiene con la scomposizione di n in fattori primi, detto $\bar{n}$ il primo valore di n per cui la corrispondente $f_1\left(x^{\frac{1}{n}}\right)$ diventa nulla, risulta

(1) Per più larghe informazioni sull'argomento, si veda l'interessante monografia del prof. G. TORELLI, premiata dall'Accademia di Napoli, *Sulla totalità dei numeri primi fino ad un limite assegnato* « Atti della R. Accademia di scienze fisiche e matematiche », vol. XI, 1902.

manifesto che non si può far a meno di supporre dati tutti i numeri primi nell'intervallo da 1 ad $\bar{n}$.

Ricordando però il significato di $f(x)$ e la relazione (1) che definisce le $f_1\left(x^{\frac{1}{n}}\right)$, si comprende come quest'ultime decrescano rapidissimamente, per cui l'intervallo $1\bar{n}$ è sempre molto piccolo relativamente all'intervallo $1x$.

§ 9. **Riassunto di una memoria di T. Levi-Civita sullo stesso soggetto.** — Un notevole contributo alla teoria analitica dei numeri primi è dovuto a T. Levi-Civita.

Prendendo le mosse dalla serie $\sum_1^\infty{}_n \frac{x^n}{1-x^n}$ dovuta a Lambert, convergente in tutti i punti x del piano tali che $|x|<1$, e sviluppabile in serie di potenze $\Sigma c_n x^n$ dove c_n, per $n>1$, egualia il numero dei divisori di n, prende a considerare la funzione:

$$S(x)=\sum_1^\infty{}_n \frac{x^n}{1-x^n}-\frac{2x^2}{1-x^2}-x$$

pure sviluppabile in serie di potenze $\Sigma c_n x^n$ in cui però sarà $c_n=0$ se n è primo, ≥ 1 negli altri casi.

Se si considera quindi un cerchio C con centro nell'origine e raggio <1 per es.: $\frac{1}{2}$, $\Sigma c_n x^n$ convergerà in egual grado lungo la circonferenza di C e sarà quindi integrabile termine a termine e lo stesso accadrà di $x^z \Sigma c_n x^n$ dove z è un qualsiasi numero complesso, poichè lungo C la x nè si annulla nè diviene infinita. Siccome $x^z \Sigma c_n x^n$ è ad infinite determinazioni, bisognerà fissare su qual ramo di $x^z \Sigma c_n x^n$ si eseguisca l'integrazione e ciò risulta nel modo più semplice ponendo $x=\rho e^{i\theta}$ e conducendo l'integrazione lungo C da $\theta=0$ a $\theta=2\pi$.

Ciò premesso, posto

$$P(z)=\frac{1}{2\pi i}\int_c x^{z-1}S(x)\cdot dx=\frac{1}{2\pi}\int_0^{2\pi}\rho^z e^{iz\theta}S(\rho e^{i\theta})\cdot dz$$

viene così definita una funzione della variabile complessa z, uniforme e singolare solo per $z=\infty$.

Per $z=n$ dove n è un qualsiasi intero positivo, si ha $P(z)=0$; mentre invece per $n\geq 1$ risulta $P(-n)=c_n$ e

quindi $P(-n)=0$ ogni qualvolta n sia primo; e con ciò si ha intanto un criterio per riconoscere se un intero è primo o no.

Dopo ciò si dimostra che $P(z)=0$ non ha radici complesse, cioè che si annulla solo per punti z situati sull'asse reale; e successivamente che ad ogni $z=-n$ $(n>12)$ si può far corrispondere un cerchio di centro $(-n)$ e di raggio $r_n=\frac{1}{2^{n+2}}$ tale che sul diametro di questo cerchio non cade alcuna radice di $P(z)=0$ se n è composto, od una ed una sola (radice semplice) se n è primo.

Dati ora due numeri positivi α, β tali che $12<\alpha<\beta$, sia h un intero

$$\alpha<h\leq\beta$$

e s'indichi con C_h il cerchio di centro $(-h)$ e di raggio $\frac{1}{2^{h+2}}$. Per il noto *Teorema di Cauchy* sarà:

$$\frac{1}{2\pi i}\int_{C_h}\frac{P'(z)}{P(z)}\,dz=0;\ 1$$

secondochè nell'interno di C_h, la $P(z)$ non si annulla, od ha un'unica radice, cioè secondochè h è composto e primo.

Se ora per ogni intero h compreso tra i limiti indicati si ripete la stessa operazione, risulta che il numero dei fattori primi tra α e β sarà dato dall'espressione:

$$\frac{1}{2\pi i}\sum_{E(\alpha)+1}^{E(\beta)}\int_{C_h}\frac{P'(z)}{P(z)}\,dz.\ (^1)$$

(1) T. Levi-Civita, *Di un' espressione analitica atta a rappresentare il numero dei numeri primi in un dato intervallo.* « Rendiconti della R. Accademia dei Lincei », 1895.

Capitolo II.

ANALISI INDETERMINATA

Introduzione. — Lo sviluppo delle idee matematiche che produce la differenziazione dei problemi, toglie talora la veduta di ciò che ne costituisce l'intimo legame, il quale si manifesta invece a chi risalga il corso della storia fino a ritrovare, nelle origini, la primitiva unità. Così per es. le equazioni algebriche, l'analisi indeterminata, ed anche le costruzioni geometriche del II Libro di Euclide, si riconducono ad un unico problema originale, che è il problema della risoluzione delle equazioni.

Infatti, risolvere un'equazione o un sistema di equazioni può avere diverso significato a seconda del campo di numeri o di grandezze a cui si riferisca. L'aspetto originale del problema dev'esser stato appunto la risoluzione delle equazioni mediante numeri (assoluti) interi o fratti.

L'introduzione degli irrazionali, che i Greci guadagnarono invero sotto forma geometrica (e svilupparono mercè la teoria delle proporzioni di Eudosso, esposta nel V libro di Euclide), da luogo ad una considerazione del problema stesso da un punto di vista più largo, che si estende poi successivamente coll'aggiunta degli immaginarii (vedi Art. X del I Vol.). In questo campo la Teoria delle equazioni assume la forma più semplice che è oggetto della nostra Algebra.

Ma, nell'evoluzione delle Matematiche, uno sviluppo intensivo si accompagna generalmente allo sviluppo estensivo, e così il problema delle equazioni che l'Algebra moderna tratta nel campo esteso dei numeri complessi, viene anche ripreso in un senso che corrisponde alla sua posizione originaria come problema della risoluzione delle equazioni in numeri interi o fratti o come problema dell'Analisi indeterminata o delle congruenze. Ed è notevole che i matematici italiani Luca Paciolo e Bombelli, i quali, prima dei francesi Bachet di Meziriac e Fermat, a questi problemi furono condotti riprendendo il commento dell'« Arithmetica » di Diofanto d'Alessandria (IV secolo d. C.) appartengano pure alla schiera di coloro che, proseguendo la Teoria geometrica delle equazioni nella forma simbolica assunta per opera

degli arabi, posero i fondamenti delle teorie generali dell'Algebra.

Per DIOFANTO che non conosceva gl'irrazionali, almeno come numeri, e tanto meno i negativi, il problema aritmetico delle equazioni si presentava naturalmente così:

Data una o più equazioni algebriche:

$$f_1(x, y, z....) = 0$$
$$f_2(x, y, z....) = 0$$
$$\ldots\ldots\ldots\ldots$$

trovare una soluzione cioè un sistema di numeri assoluti interi o fratti $x, y, z....$ tali che sia

$$f_1 = 0, \quad f_2 = 0.....$$

Limitiamoci per semplicità al caso di una sola equazione

$$f(x, y, z....) = 0.$$

Si riconosce subito che il problema anzidetto si riconduce sempre al caso della risoluzione in numeri interi, bastando per ciò sostituire ad $x, y, z....$ i rapporti $\frac{x_1}{x_n}, \frac{x_2}{x_n}....$ e rendere omogenea l'equazione stessa moltiplicando per una conveniente potenza di x_n.

Ciò posto, il problema delle equazioni secondo era considerato da DIOFANTO si converte nel problema generale dell'Analisi indeterminata quale FERMAT lo ha considerato nel campo dei numeri interi relativi (positivi e negativi).

Il caso più semplice di questo problema consiste nell'*assegnare tutte le coppie di numeri interi* x, y *che soddisfano ad un' equazione algebrica di grado* n *a coefficienti interi*

$$f(x, y) = 0.$$

Il problema dell'analisi indeterminata di 1° grado ($n = 1$) trovasi già risoluto, mercè i metodi di DIOFANTO, da BACHET DI MEZIRIAC nei suoi « Problémes plaisants et deléctables qui se font par les nombres ».

Per $n > 1$, si hanno varii sviluppi, e tra i più notevoli l'equazione di PEEL-FERMAT per $n = 2$, ed in particolare le celebri *proposizioni negative* di FERMAT.

In questo Capitolo riporteremo le soluzioni di alcuni dei problemi classici di Analisi indeterminata scelti tra i più elementari, ma bastanti a fornire una prima idea dei varii aspetti di questa particolare dottrina a cui, secondo l'opinione di LEGENDRE, si può ricondurre ogni questione della Teoria dei numeri.

§ 1. **Risoluzione in numeri interi dell'equazione $ax+by=c$. - Metodo di Diofanto-Bachet.** — Detti n, a, r numeri interi il primo dei quali, per semplicità, ci limitiamo a considerare come positivo, mentre gli altri due possono essere anche negativi, dimostriamo la seguente proposizione di cui si farà molto uso nel seguito.

Lemma. « Se n è primo con r, i resti che si ottengono dividendo per n, n termini consecutivi quali si vogliano dalla progressione aritmetica

$$a, \quad a+r, \quad a+2r, \ldots \quad a+kr \ldots$$

sono tutti tra loro diversi ».

Sieno infatti $a+kr$, $a+hr$ due termini qualunque estratti da un gruppo di n consecutivi: dico che divisi per n devono dare resti diversi. Infatti se ciò non fosse, la loro differenza $r(k-h)$ dovrebbe essere multipla di n, e per essere n primo con r, $(k-h)$ dovrebbe pure essere divisibile per n il che è impossibile poichè in seguito all'ipotesi è $|k-h|<n$.

Segue, come immediato corollario, che di questi n termini consecutivi uno, ed uno solo, risulterà multiplo di n.

Applichiamo ora la precedente proposizione al problema classico attribuito a DIOFANTO ma la cui trattazione completa è dovuta a BACHET e che consiste nel determinare le formule di risoluzione in numeri interi dell'equazione

$$ax+by=c \tag{1}$$

dove a, b, c sono interi qualunque, il primo dei quali, senza ledere punto la generalità della questione, possiamo supporre positivo.

In primo luogo, si vede subito che condizione necessaria per l'esistenza di soluzioni intere di (1) è che c sia divisibile pel m. c. d. $D(a, b)$ dei coefficienti delle incognite, e che una

volta soddisfatta, le predette soluzioni si possono dedurre da quelle della

$$\frac{a}{D(a,\ b)}x + \frac{b}{D(ab)}\cdot y = \frac{c}{D(a,\ b)}$$

in cui i coefficienti di x, y sono primi tra loro.

È palese quindi che possiamo ammettere senz'altro, che in (1) si abbia $D(a,\ b) = 1$.

Ciò premesso, risolta la (1) rispetto alla x

$$x = \frac{c - by}{a}$$

si attribuiscano successivamente ad y i valori

$$0,\quad 1,\quad 2,\ldots.\quad (a-1).$$

Per il *Lemma* precedente, tra gli a termini consecutivi della progressione

$$c,\quad c-b,\quad c-2b,\ldots.\quad c-(a-1)b$$

essendo per ipotesi a primo con la ragione b, ve ne sarà uno, ed uno solo, divisibile per a e sia questo $c - \beta b$; e detto α il quoziente, risulta allora:

$$a\alpha + b\beta = c.$$

Combinando questa identità con l'altra

$$ax_0 + by_0 = c$$

ammesso che $x_0 y_0$ sia un'altra qualsiasi soluzione, si ricava:

$$a(x_0 - \alpha) + b(y_0 - \beta) = 0$$
$$\frac{\beta - y_0}{x_0 - \alpha} = \frac{a}{b}$$

e poichè a, b sono primi tra loro:

(2) $$x_0 = \pm kb + \alpha \qquad y_0 = \mp ka + \beta$$

dove k è un intero qualunque.

Ogni altra soluzione di (1) ha quindi la forma (2); e reciprocamente ogni coppia di numeri $x_0 y_0$ dedotta dalla (2) soddisfa manifestamente alla (1), la quale ammette quindi infinite soluzioni.

Nel caso generale, risolta la

$$\frac{a}{D(ab)} x + \frac{b}{D(a,\ b)} y = \frac{c}{D(a,\ b)}$$

basterà moltiplicare le soluzioni di quest'ultima per $D(a,\ b)$ e si ricaveranno quelle di

$$ax + by = c.$$

Riassumendo si può dire che « la condizione necessaria per la risolubilità di (1) in numeri interi, è anche sufficiente, e che determinatane una qualsiasi soluzione $(x_0 y_0)$, tutte le altre sono fornite dalle espressioni

$$x = x_0 \pm kb \quad y = y_0 \mp ka$$

variando k per valori interi da $+\infty$ a $-\infty$.

§ 2. **Metodo di Lagrange.** — Nel paragrafo precedente dimostrando la condizione di risolubilità, si è pure ottenuto il procedimento per la completa determinazione delle soluzioni intere della (1). Tale metodo se da un lato offre il vantaggio della semplicità dei mezzi, diventa però prolisso e quasi impraticabile se i coefficienti $a,\ b$ sono entrambi piuttosto grandi. Ad ovviare a tale inconveniente sono stati proposti diversi metodi tra i quali, per la sua eleganza, merita di essere ricordato quello di LAGRANGE.

Supposto, com'è lecito, $a,\ b$ primi tra loro si sviluppi il quoziente $\frac{a}{b}$ in frazione continua e sieno $\frac{P_{n-1}}{Q_{n-1}}$, $\frac{P_n}{Q_n}$ le due ultime ridotte.

Sarà intanto:

$$\frac{P_n}{Q_n} = \frac{a}{b} \quad P_n Q_{n-1} - P_{n-1} Q_n = (-1)^n$$

e poichè $P_n = a,\ Q_n = b$:

(1) $$aQ_{n-1} - b \cdot P_{n-1} = (-1)^n.$$

Ciò premesso, si consideri il sistema:

$$ax + by = c$$
$$P_{n-1}x + Q_{n-1}y = k$$

dove k è un intero qualunque. Risolvendo si ha:

$$x = \frac{cQ_{n-1} - k \cdot b}{aQ_{n-1} - bP_{n-1}} \qquad y = \frac{ka - cP_{n-1}}{aQ_{n-1} - bP_{n-1}}$$

e per la (1)

$$x = cQ_{n-1} - kb \qquad y = ka - cP_{n-1}$$

se n è pari, od ai loro contrari se n è dispari.

La proprietà delle ridotte su cui si basa la risoluzione è indipendente dal segno di a, b; tuttavia è sempre possibile evitare di dover prendere in considerazione lo sviluppo in frazione continua di $\frac{a}{b}$ per a, b non entrambi positivi, osservando che tutti i casi possibili si possono ridurre ai due

$$ax + by = c$$
$$ax - by = c$$

con a, b entrambi positivi, pel secondo dei quali si procederà come prima considerando il sistema

$$ax - by = c$$
$$P_{n-1}x - Q_{n-1}y = k$$

in cui il determinante dei coefficienti è $-(-1)^n$.

§ 3. **Il Teorema di Fermat e sue applicazioni alla questione precedente.** — Passiamo ora ad un'altra trattazione dello stesso problema che presenta il vantaggio di condurre ad un'espressione formale delle soluzioni intere dell'equazione indeterminata a due incognite.

Dobbiamo premettere a tale scopo la dimostrazione del seguente

Teorema. « Se p è un numero primo ed a un intero qualunque primo con p, la differenza $a^{p-1} - 1$ è divisibile per p ».

Dallo sviluppo delle potenze $(a+1)^p$, notando che i coefficienti binomiali

$$\binom{p}{r} = \frac{p(p-1)(p-2)....(p-r+1)}{1 \cdot 2....r}$$

per p primo e, salvo i casi $r=0$, $r=p$, sono tutti multipli di p, si ricava:

$$(a+1)^p = kp + a^p + 1$$
$$(a+1)^p - (a+1) = kp + a^p - a.$$

Per $a=1$, il secondo membro è divisibile per p, e tale sarà pure il primo $2^p - 2$; facendo ora $a=2$, il secondo membro risulta nuovamente multiplo di p, e multiplo di p risulta pure il primo $3^p - 3$.

Così continuando, si ottiene che per $a = 1, 2, ... (p-1)$

$$a^p - a = a(a^{p-1} - 1)$$

è divisibile per p; e poichè a, p sono primi tra loro, dovrà necessariamente esser multiplo di p il fattore $a^{p-1} - 1$.

Se poi $a = kp + r$, $r < p$, è palese che $a^{p-1} - 1$ sarà divisibile per p insieme ad $r^{p-1} - 1$.

Questa proposizione venne scoperta da FERMAT, ma fu dimostrata per la prima volta da EULERO: essa è un caso particolare del seguente

Teorema. Se $\alpha_1, \alpha_2, ... \alpha_{\varphi(n)}$ sono i $\varphi(n)$ numeri inferiori ad n e primi con esso, ed α un numero qualsiasi non multiplo di n, la differenza.

$$\alpha^{\varphi(n)} - 1$$

è multiplo di n ».

Se infatti consideriamo i $\varphi(n)$ prodotti:

$$(1) \qquad \alpha_1 \cdot \alpha, \quad \alpha_2 \cdot \alpha, ... \quad \alpha_{\varphi(n)} \cdot \alpha$$

si scorge subito che due qualunque di essi $\alpha_r \cdot \alpha$; $\alpha_s \cdot \alpha$ divisi per n non possono dare resti eguali poichè, ove ciò fosse,

$$\alpha(\alpha_r - \alpha_s)$$

dovrebbe esser multiplo di n, il che è impossibile per α primo con n ed $|\alpha_r - \alpha_s| < n$.

D'altra parte i numeri (1) come prodotti di fattori primi con n, daranno resti primi con n; ed essendo tutti diversi ed

in numero di $\varphi(n)$, tali resti coincideranno ordine a parte, con $\alpha_1, \alpha_2, \ldots \alpha_{\varphi(n)}$.

Potremo per ciò porre:

$$\begin{aligned}
\alpha_1 \cdot \alpha &= k_1 n + \alpha_1' \\
\alpha_2 \cdot \alpha &= k_2 n + \alpha_2' \\
&\cdots\cdots\cdots\cdots \\
\alpha_{\varphi(n)} \cdot \alpha &= k_{\varphi(n)} \cdot n + \alpha_{\varphi(n)}'
\end{aligned}$$

e moltiplicando membro a membro:

$$\alpha^{\varphi(n)} \cdot \alpha_1 \cdot \alpha_2 \ldots \alpha_{\varphi(n)} = k \cdot n + \alpha_1' \alpha_2' \ldots \alpha_{\varphi(n)}'$$

è poichè:

$$\alpha_1 \alpha_2 \ldots \alpha_{\varphi(n)} = \alpha_1' \cdot \alpha_2' \ldots \alpha_{\varphi(n)}'$$

avremo in fine:

$$(\alpha^{\varphi(n)} - 1) \cdot \alpha_1 \alpha_2 \ldots \alpha_{\varphi(n)} = kn$$

e per essere n primo con $\alpha_1 \cdot \alpha_2 \ldots \alpha_{\varphi(a)}$

$$\alpha^{\varphi(n)} - 1 = k' \cdot n. \tag{2}$$

ed il *Teorema* resta dimostrato.

Riprendiamo ora l'equazione

$$ax + by = c \tag{3}$$

in cui come precedentemente a, b sono primi tra loro e diversi da zero.

Posto

$$x = c \cdot a^{\varphi(b)-1} + kb$$

dove k è un intero qualsiasi positivo o negativo, e sostituendo in (3) si ha:

$$c \cdot a^{\varphi(b)} + kab + by = c \tag{4}$$

e poichè essendo a, b primi tra loro per la (2):

$$a^{\varphi(b)} = k_1 \cdot b + 1$$

sostituendo in (4) risulta:

$$k_1 cb + c + kab + by = c$$

che verrà soddisfatta ove si faccia:

$$y = -k_1 c - ka.$$

Otteniamo così per le incognite le espressioni:

$$(5) \qquad \begin{cases} x = ca^{\varphi(b)-1} + kb \\ y = -\dfrac{a^{\varphi(b)}-1}{b} \cdot c - ka \end{cases}$$

che danno la completa risoluzione formale dell'equazione lineare indeterminata a due incognite.

Infatti le (5) per qualunque valore dell'intero k forniscono una soluzione di (3); e reciprocamente, dall'ipotesi che sussista l'identità:

$$a\alpha + b\beta = c$$

moltiplicando primo e secondo membro per $a^{\varphi(b)-1}$ e ricordando che $a^{\varphi(b)} = 1 + kb$, si ricava subito che α, β sono della forma data dalle (5).

Le (5) non sono di pratica applicazione per la difficoltà inerente al calcolo di $a^{\varphi(b)}$, ma da esse si possono agevolmente ricavare alcune importanti conseguenze intorno alle soluzioni intere e positive.

Per ottenere intanto dalle (5) soluzioni positive, è necessario dare a k valori negativi, e si scorge subito che l'esistenza ed il numero delle predette soluzioni corrisponderanno all'esistenza ed al numero degli interi positivi $|k|$ compresi nell'intervallo

$$(6) \qquad c\frac{a^{\varphi(b)}-1}{ab} \leq |k| \leq c\frac{a^{\varphi(b)}}{ab}$$

estremi inclusi.

Posto

$$c\frac{a^{\varphi(b)}}{ab} = c\frac{a^{\varphi(b)}-1}{ab} + \frac{c}{ab}$$

$$\frac{c}{ab} = q + \frac{r}{ab} \qquad r < ab$$

si scorge che detto numero coinciderà coi valori di $|k|$ soddisfacenti la:

$$(7) \qquad c\frac{a^{\varphi(b)}-1}{ab} \leq |k| < c\frac{a^{\varphi(b)}-1}{ab} + q + \frac{r}{ab}$$

che saranno $(q+1)$ o q, secondochè nell'intervallo:

$$c\frac{a^{\varphi(b)}-1}{ab} \qquad c\cdot\frac{a^{\varphi(b)}-1}{ab}+\frac{r}{ab}$$

esiste o no un intero.

Ma a quest'ultimo intervallo si può sostituire l'altro, sotto tale rapporto, equivalente:

$$r\frac{a^{\varphi(b)}-1}{ab} \qquad r\frac{a^{\varphi(b)}-1}{ab}+\frac{r}{ab}$$

cioè

$$r\frac{a^{\varphi(b)}-1}{ab}, \quad r\frac{a^{\varphi(b)}}{ab}$$

e siccome l'esistenza di interi tra i predetti limiti equivale in base alle (6) alla possibilità di risolvere in interi positivi la

$$ax+by=r$$

si può concludere col seguente

Teorema. « Il numero delle soluzioni intere e positive di

$$ax+by=c$$

è dato da $(q+1)$ o q secondochè è o no solubile nello stesso senso la

$$ax+by=r$$

essendo

$$c=a\cdot b\cdot q+r \qquad r<ab \text{ ».}$$

§ 4. **Risoluzione in numeri interi positivi di $ax+by=ab$.** — Per l'importanza dell'argomento che si connette al problema della ripartizione dei numeri, ed in vista delle applicazioni, crediamo non inutile presentare sotto un nuovo aspetto il problema della risoluzione in numeri interi positivi dell'equazione lineare indeterminata a due incognite.

Notiamo intanto che supposti a, b, c interi e positivi, i diversi casi che si possono presentare si riducono ai seguenti:

$$ax+by=c; \quad ax-by=c; \quad ax+by=-c; \quad ax-by=-c.$$

Il terzo si può ommettere poichè è palese l'impossibilità

di risolverlo nel senso voluto, ed il quarto è riducibile al secondo, per cui possiamo limitarci ai primi due.

Per il secondo, supposto $D(a, b) = 1$, si ha:

$$x = \frac{c + by}{a}$$

e detto β il valore di y positivo e minore di a per cui la frazione assume un valore positivo intero α, risulta l'identità:

$$a\alpha - b\beta = c$$

che, combinata con l'equazione, dà:

$$a(x - \alpha) - b(y - \beta) = 0$$

$$\frac{x - \alpha}{y - \beta} = \frac{b}{a}$$

$$x = \alpha + kb \quad y = \beta + ka$$

da cui si deduce l'esistenza d'infinite soluzioni intere positive per $k = 0, 1, 2....$ senza escludere che ve ne sieno anche per valori negativi di k.

Il caso $ax + by = c$ presenta maggiori difficoltà, e ne daremo una trattazione diversa dalle consuete, come esempio dei vantaggi che si possono ricavare applicando considerazioni geometriche anche a questioni di numeri interi.

Sia intanto la

$$ax + by = a \cdot b \tag{1}$$

che, com'è palese, è sempre risolubile in numeri interi.

Alla (1) si può dare la forma:

$$\frac{x}{b} + \frac{y}{a} = 1 \tag{2}$$

e ci si presenta così come equazione di una retta che stacca sugli assi ortogonali positivi due segmenti OB, OA di lunghezze rispettivamente $x = b$, $y = a$.

È chiaro che se la (1) ha soluzioni intere e positive, il segmento AB passa per punti di coordinate intere e positive, e reciprocamente. Sia $P(x, y)$ uno di essi distinto da A, e da B; e C la sua proiezione sull'asse delle ascisse.

Dai triangoli simili AOB, PCB si ricava:

$$\frac{y}{b-x} = \frac{a}{b} \tag{3}$$

e si conclude che se $D(a, b) = 1$, per essere $y < a$; $b - x < b$ la (3) non può sussistere e che quindi AB contiene i soli punti interi positivi $A(0, a)$, $B(0, b)$.

Se invece $D(a, b) = \delta > 1$, posto $a = \delta \cdot a'$, $b = \delta \cdot b'$ è manifesto che AB oltre agli estremi contiene i punti interi positivi:

$$\begin{array}{c|l} x & b',\ 2b',\ 3b',\ldots.\ (\delta-1)\cdot b' \\ y & (\delta-1)a',\ (\delta-2)a',\ (\delta-3)a'\ldots.a'. \end{array}$$

Concludiamo quindi che « la (1) è sempre solubile in interi positivi e che essa ammette un numero di soluzioni dato da

$$\sigma = D(a, b) + 1$$

che, se $D(a, b) = 1$, si riducono a quelle corrispondenti ai soli estremi di AB ».

§ 5. **Risoluzione in numeri interi positivi di $ax + by = c$.** — Consideriamo ora, nell'ipotesi $D(a, b) = 1$ la

$$ax + by = c$$

e, detto Δ il segmento che risulta scomponendo l'unità di lunghezza in $a \cdot b$ parti eguali, si dividano i due membri per c ponendola quindi sotto la forma:

$$\frac{x}{\left(\frac{cb}{ab}\right)} + \frac{y}{\left(\frac{ca}{ab}\right)} = 1$$

in cui ci si presenta come equazione di una retta che determina sui semi-assi positivi due segmenti multipli di Δ secondo i numeri $c \cdot b$ e $c \cdot a$. Con le stesse considerazioni del § 4 si trova che sul segmento AB giaceranno $c + 1$ punti a coordinate positive razionali multiple di Δ secondo i numeri:

$$\begin{array}{c|l} x & 0,\ b,\ 2b,\ \ldots.\ (c-1)b,\ c\cdot b \\ y & c\cdot a,\ (c-1)a,\ (c-2)a,\ \ldots.\ a,\ 0. \end{array}$$

Considerando ora un punto generico:

$$P(k \cdot b, \quad (c - k)a)$$

perchè esso sia a coordinata intera sarà necessario e sufficiente che kb e $(c - k)a$ sieno multipli di $a \cdot b$, ovvero, per essere a, b primi tra loro, che k sia multiplo di a cioè $k = k' \cdot a$, e $(c - k'a)$ multiplo di b.

Sia ora $k' = \beta$ l'intero positivo minore di b tale che $(c - \beta \cdot a)$ sia divisibile per b e della cui esistenza ed unicità ci garantisce il *Lemma* del § 1.

Il punto

$$P(\beta \cdot a \cdot b, \quad (c - \beta a)a)$$

sarà allora manifestamente intero, e lo saranno pure gli altri che si ottengono sostituendo a β successivamente:

$$\beta + b, \quad \beta + 2b, \ldots \quad \beta + k''b$$

dove k'' è il massimo intero per cui sia

$$c - (\beta + k'' \cdot b)a \geq 0$$

cioè:

$$k'' \leq \frac{c - a\beta}{ab}$$

dal che risulta che il numero delle soluzioni intere e positive viene dato da

$$\sigma = E\left(\frac{c - a\beta}{ab}\right) + 1.$$

Si ponga ora:

(1) $$c = q \cdot ab + r \quad r < ab.$$

Segue

$$\sigma = E\left(q + \frac{r - a \cdot \beta}{a \cdot b}\right) + 1$$

ed essendo $|r - a\beta| < ab$, risulta che se $r - a\beta \geq 0$ si ha:

$$\sigma = q + 1$$

diversamente

$$\sigma = q.$$

Ricordando poi che β è il più piccolo valore positivo di k' per cui

$$c - k' \cdot a = q \cdot ab + r - k'a$$

è multiplo di b, cioè è divisibile per b la differenza $r - k' \cdot a$, se ne deduce che, l'essere $r - a\beta \geq 0$ oppure $r - a\beta < 0$ equivale all'essere o no solubile in numeri interi positivi la

$$ax + by = r$$

§ 6. **Applicazione geometrica.** -- Da quanto precede risulta pure il procedimento che si potrebbe seguire per la risoluzione del problema cioè per la determinazione delle soluzioni stesse.

Senza addentrarci in maggiori particolari accenniamo ad una semplice interpretazione geometrica dei risultati ottenuti, che fa vedere com'essi possano venir applicati a questioni pratiche.

S'immagini a tal uopo segnate sui semi-assi positivi due serie di punti equidistanti, a partire dall'origine che distingueremo con un numero d'ordine

$$0,\ 1,\ 2,\ 3,\ldots.\ n$$

e condotte per essi le parallele agli assi così da segnare nel primo quadrante un reticolato di quadrati, si supponga piantato uno spillo su ciascun vertice dei quadrati.

Volendo ora tendere un filo tra due dei punti segnati sugli assi in modo che non incontri alcuno degli spilli interni all'angolo retto, o che si appoggi ad un determinato numero n di essi, dove se ne dovranno fissare i capi?

Nel primo caso i numeri che segnano la posizione dei capi sugli assi X, Y dovranno esser due numeri b, a primi tra loro, poichè allora (§ 3) l'equazione

$$\frac{x}{b} + \frac{y}{a} = 1$$

ovvero l'equivalente

$$ax + by = a \cdot b$$

non ammette che le sole soluzioni $x = 0$, $y = a$, $x = b$, $y = 0$: nel secondo invece basterà sceglierli in modo che il loro massimo comune divisore sia $n + 1$.

§ 7. **Un problema dei matematici indiani. - Dimostrazione di Eulero.** — Un problema importante per le applicazioni ed

interessante dal punto di vista storico [1] è quello di determinare un intero x che diviso per altri interi $a_1, a_2, \ldots a_n$ dia rispettivamente per resti $r_1, r_2, \ldots r_n$.

Esso si può far dipendere dalla risoluzione del sistema indeterminato di n equazioni lineari con $(n+1)$ incognite

$$\begin{aligned} x &= a_1 y_1 + r_1 \\ x &= a_2 y_2 + r_2 \\ &\cdots\cdots\cdots \\ x &= a_n y_n + r_n \end{aligned}$$

Per brevità ci limiteremo al caso, che del resto è il più importante, in cui i divisori $a_1, a_2, \ldots a_n$ sono primi tra loro due a due, a cui, quando il problema sia solubile, si può sempre ricondurre ogni altro [2].

Poniamo

$$\pi = a_1 \cdot a_2 \ldots a_n$$

e sia α_i il coniugato di $\frac{\pi}{a_i}$ rispetto ad a_i se $\frac{\pi}{a_i} < a_i$, diversamente sia α_i coniugato del resto della divisione di $\frac{\pi}{a_i}$ per a_i per cui in ogni caso

$$\frac{\pi}{a_i} \cdot \alpha_i$$

diviso per a_i darà per resto 1.

Consideriamo quindi l'espressione:

$$\left(\frac{\pi}{a_1} \cdot \alpha_1\right) r_1 + \left(\frac{\pi}{a_2} \alpha_2\right) r_2 + \ldots + \left(\frac{\pi}{a_n} \alpha_n\right) r_n = x.$$

Tutti i termini che compongono x, ad eccezione del primo, sono multipli di a_1; il primo, poichè $\frac{\pi}{a_1}$ ed α_1 sono coniugati, diviso per a_1 dà per resto r_1, e siccome analogamente si può concludere per tutti gli altri divisori $a_2, a_3, \ldots a_n$, resta provato che x soddisfa alle condizioni richieste.

[1] Cfr. « Encyclopedie des Sciences mathèmatiques », tome 1, volume 3, fascicule 1, pag. 15.

[2] Cfr. LE BESGUE, *Exercices d'Analyse numérique*, § 28, pag. 57.

Le soluzioni sono manifestamente in numero infinito, poichè ciascuno dei coefficienti degli r si può variare ad arbitrio di un multiplo di π, senza che l'espressione venga a perdere la sua proprietà.

Nel Capitolo seguente riprenderemo e completeremo la questione.

§ 8. **Equazione pitagorica. - Risoluzione di Klein.** — Uno dei problemi la cui risoluzione risale ai geometri greci e di cui s'occuparono PITAGORA, PLATONE, EUCLIDE e quindi DIOFANTO, è quella della determinazione dei *triangoli razionali*, vale a dire dei triangoli che hanno lati ed area espressi da numeri razionali, e che si riduce a quella dei *triangoli rettangoli in numeri* detti anche *triangoli pitagorici*, pei quali

$$x^2 + y^2 = z^2 \tag{1}$$

dove x, y, z sono interi.

Di questo importante problema che ha contemporaneamente un substrato geometrico ed aritmetico riportiamo un'elegante soluzione proposta dal KLEIN (1).

Dividendo per z^2, la (1) assume la forma:

$$\xi^2 + \eta^2 = 1 \tag{2}$$

ed è palese l'equivalenza dei due problemi di risolvere la (1) in numeri interi e la (2) in numeri razionali.

La (2) è l'equazione in coordinate cartesiane ortogonali di un cerchio di raggio 1 e centro nell'origine; e sieno ξ_0, η_0 le coordinate razionali di un suo punto che diremo *punto razionale*. La retta che passa per (ξ_0, η_0), e $(-1, 0)$ ha per equazione:

$$\eta = \frac{\eta_0}{1 + \xi_0}(1 + \xi)$$

cioè

$$\eta = \lambda(1 + \xi)$$

dove λ è razionale.

Ogni punto razionale della circonferenza è il secondo punto d'intersezione di una retta per $(-1, 0)$ ed a parametro razionale λ.

(1) G. SCORZA, Recensione dell'opera di F. KLEIN, *Die Elementar matematik von höheren Standpunkte aus.* « Bollettino di Mathesis », II, fascicoli 7, 8, 9.

Reciprocamente, se si considera il sistema:

$$\xi^2 + \eta^2 = 1$$
$$\eta = \lambda(\xi + 1)$$

risolvendo si trovano per ξ, η i valori:

$$\eta = 0, \quad \frac{2\lambda}{1+\lambda^2}$$

$$\xi = -1, \quad \frac{1-\lambda^2}{1+\lambda^2}$$

che per λ razionale, sono pure razionali, dal che segue che il secondo punto comune alla retta ed alla circonferenza è razionale insieme con λ.

I punti razionali della circonferenza sono quindi tutti e solo quelli comuni ad essa ed al fascio di raggi di centro $(-1, 0)$ e che risulta attribuendo a λ tutti i possibili valori razionali.

Posto ora $\lambda = \frac{m}{n}$ (m, n interi) si ha:

$$\xi = \frac{2 \cdot m \cdot n}{m^2 + n^2} \qquad \eta = \frac{n^2 - m^2}{m^2 + n^2}$$

e di qui:

$$x = 2 \cdot m \cdot n \quad y = n^2 - m^2 \quad z = m^2 + n^2.$$

§ 9. **Il " grande „ teorema di Fermat. - Impossibilità di risolvere in numeri interi $x^4 + y^4 = z^4$. - Metodo di dimostrazione di Fermat.** — Dopo l'equazione Pitagorica, il primo caso che si presenta volendo procedere in questo senso, è dato dall'equazione:

$$x^3 + y^3 = z^3$$

la cui impossibilità in numeri interi è stata dimostrata da Eulero e nelle medesime condizioni si trova la:

$$x^4 + y^4 = z^4$$

e queste due sono casi particolari della:

$$x^n + y^n = z^n$$

che Fermat afferma di aver dimostrato insolubile in numeri interi per $n > 2$.

Per quanto la questione sia stata oggetto di profonde investigazioni da parte dei più valenti geometri, non fu ancora possibile ottenerne una soluzione completa.

È manifesto che basterebbe provare l'impossibilità per n primo, poichè essendosi già stabilita per $n = 4$, una volta accertata per un certo intero n, resta pur dimostrata per ogni multiplo di n.

Il *Teorema* in questione è stato dimostrato dal DIRICHLET per $n \leq 5$, dal LAMÉ e dal LE BESGUE per $n = 7$ e dal KUMMER per $n \leq 100$ e per certe classi di numeri superiori al 100.

Non sarebbe conforme al piano di questo lavoro una lunga digressione su questo argomento, e ci limitiamo per ciò a trattare il solo caso $n = 4$ che si presta per la sua semplicità e che ha pure il vantaggio di offrire un esempio dell'elegante principio di dimostrazione di cui soleva usare il FERMAT in questioni analoghe (1).

Teorema. « L'equazione

$$x^4 + y^4 = z^2 \tag{1}$$

è insolubile con numeri interi non nulli ».

Facciamo vedere in primo luogo che se la (1) è soddisfatta da una certa terna di valori per le incognite, essa lo è pure da un'altra terna di numeri primi tra loro due a due

Sia infatti $\bar{x}, \bar{y}, \bar{z}$ una soluzione di (1) e sia pure $D(x, y) = q$. Avremo, posto $x = q\bar{x}_1$ $y = q\bar{y}_1$, l'identità:

$$q^4\bar{x}_1^4 + q^4\bar{y}_1^4 = \bar{z}^2$$

da cui $\bar{z}^2 = q^4 \cdot \bar{z}_1^2$ e dividendo per q^4:

$$\bar{x}_1^4 + \bar{y}_1^4 = \bar{z}_1^2$$

identità in cui $\bar{x}_1$, $\bar{y}_1$ sono primi tra loro e quindi tali pure $\bar{z}_1$ ed $\bar{x}_1$, $\bar{z}_1$ ed $\bar{y}_1$.

Basterà quindi limitarci a constatare l'irresolubilità di (1) con numeri primi tra loro due a due, escludendo così l'ipotesi che sieno tutti e tre pari, che sieno pari x, y, e

(1) Cfr. E. LUCAS, *Recherches sur l'Analyse indeterminée*, 1873.

dispari z; o pari z ed x o z ed y e dispari y od x rispettivamente, le quali, tolta la prima, risultano a prima vista inammissibili.

Parimenti si può escludere che x, y sieno entrambi dispari, poichè in questo caso z non potrebbe esser dispari, e se pari il secondo membro z^2 sarebbe divisibile almeno per 4, mentre il primo, come somma di due numeri dispari, lo sarebbe solo per due.

Ammesso quindi che la (1) sia solubile, dobbiamo necessariamente ritenere x pari ed y dispari (o viceversa) e z pure dispari, e possiamo inoltre supporre x, y, z primi tra loro due a due.

Sostituiamo quindi ad x, $2^n \cdot x$ e cerchiamo a quale conseguenze conduce l'ipotesi della risolubilità di

$$2^{4n} \cdot x^4 + y^4 = z^2. \tag{2}$$

Detta $\bar{x}, \bar{y}, \bar{z}$ una soluzione di (2) soddisfacente alla predetta condizione, si avrà l'identità:

$$(\bar{z} - \bar{y}^2)(\bar{z} + \bar{y}^2) = 2^{4n} \cdot \bar{x}^4. \tag{3}$$

I fattori del primo membro di (3) danno per somma $2\bar{z}$, e per differenza $2\bar{y}^2$, per cui non potranno esser l'uno pari e l'altro dispari, e nemmeno, essendo pari il loro prodotto, entrambi dispari.

Saranno quindi entrambi pari, e poichè $2 \cdot \bar{z}$, $2 \cdot \bar{y}^2$ hanno per m. c. d. il 2, uno solo di tali fattori sarà divisibile per una potenza del 2 superiore alla prima. Potremo quindi porre:

$$\bar{z} \pm \bar{y}^2 = 2t_1 \quad \bar{z} \mp \bar{y}^2 = 2^{4n-1} \cdot u_1 \tag{4}$$

dove t_1, u_1 oltrechè dispari e manifestamente primi con $\bar{z}$, $\bar{y}$ devono esser primi tra loro, poichè, diversamente, un loro fattore comune primo $p > 2$ dovrebbe contemporaneamente dividere $2\bar{z}$ e $2\bar{y}^2$ contro l'ipotesi che $\bar{z}$, $\bar{y}$ sieno primi tra loro.

Ma $t_1 \cdot u_1$ deve essere eguale ad $\bar{x}^4$, per cui, necessariamente, essendo primi tra loro:

$$t_1 = t^4 \quad u_1 = u^4$$

e le (4) divengono

$$\bar{z} \pm \bar{y}^2 = 2t^4; \quad \bar{z} \mp \bar{y}^2 = 2^{4n-1} \cdot u^4.$$

Assumendo i segni inferiori si ricava sottraendo dalla 1ª la 2ª:

$$\bar{y}^2 = 2^{4n-2} u^4 - t^4$$

che dà luogo all'identità:

$$\bar{y}^2 + t^4 = 2^{4n-2} u^4$$

inammissibile poichè, mentre il 2° membro è multiplo di 4, non lo può essere il 1° come somma di due numeri dispari.

Assumendo invece i superiori:

$$\bar{y}^2 = t^4 - 2^{4n-2} \cdot u^4$$

$$(t^2 + \bar{y})(t^2 - \bar{y}) = 2^{4n-2} \cdot u^4.$$

Ripetendo il precedente ragionamento si ottiene:

$$t^2 \pm \bar{y} = 2v^4 \quad t^2 \mp \bar{y} = 2^{4n-3} \cdot w^4$$

dove v, w sono dispari, primi tra loro e con t ed $\bar{y}$, dopo di che sommando si ricava:

$$t^2 = v^4 + 2^{(n-1)4} \cdot w^4 \tag{6}$$

da cui segue l'importante conseguenza che se la (1) è solubile in numeri primi tra loro due a due $2^n\bar{x}$, $\bar{y}$, $\bar{z}$, essa è pure soddisfatta da t, v, $2^{n-1} \cdot w$ essi pure primi due a due, ed in cui w è dispari.

Operando su questa seconda soluzione come sulla prima, se ne ricaverebbe una terza

$$t_1, \quad v_1, \quad 2^{n-2} \cdot w_1$$

e così di seguito fino a che si dovrebbe pervenire ad una soluzione

$$t_{n-1}, \quad v_{n-1}, \quad w_{n-1}$$

composta di tre numeri dispari, il che è impossibile.

La (1) è quindi insolubile in numeri interi

Una volta stabilita l'impossibilità della (1), ne discende immediatamente quella di:

$$x^4 + y^4 = z^4 = (z^2)^2 \quad (^1).$$

§ 10. **Identità di Fibonacci ed Eulero. — Intorno all'equazione:**

$$x_1^2 + x_2^2 + x_3^2 + x_4^2 = n.$$

È ben nota, come conseguenza della proprietà del prodotto di due numeri complessi coniugati, l'identità:

$$(a^2 + b^2)(a_1^2 + b_1^2) = (aa_1 + bb_1)^2 + (ab_1 - ba_1)^2$$

secondo cui il prodotto di due somme di due quadrati, è pure la somma di due quadrati.

Questa identità compare già nel « Liber quadratorum » di LEONARDO da Pisa detto « FIBONACCI » (1202) e si può considerare come una generalizzazione della seguente che PROCLO attribuisce a PLATONE

$$(a^2 + b^2)^2 = (2ab)^2 + (a^2 - b^2)^2$$

e che risulta dalla precedente ponendo

$$b_1 = a \quad a_1 = b.$$

(1) La dimostrazione che qui si riporta di questo Teorema è un *commento* di quella che ne dà il LE-BESGUE nei suoi *Exercices d' Analyse numérique*, Paris, 1859, alla quale si possono pure riferire alcune considerazioni che l'Autore stesso espone poche pagine dopo, e che meritano di esser riprodotte.

« Dans la théorie des nombres, une démonstration, pour être complète, demande souvent l'éxamen des cas particuliers assez nombreux et qui exigent quelquefois des méthodes différents. Il est donc assez prudent de regarder seulement comme probables certaines propositions dont les démonstrations ont été omises, ou considerablement abrégées par l'emploi fréquent de la locution « on verra facilement »; c'est souvent à ces endroits que beaucoup de lecteurs sont arrêtés, et il est même permis de croire que les auteurs qui emploient fréquemment ce moyen d'abréviation pourraient bien être aussi arrêtés, s'ils venaient à relire leurs mémoires quand *certaines liaisons d' idées ont cessé d' exister dans leur cerveau.* Or, d'après une notice intéressant de M. BIOT sur LAPLACE, on voit que ce la arrivait quelquefois au grand géomètre ».

Devesi poi ad EULERO la seguente:

$$(a^2+b^2+c^2+d^2)(a_1^2+b_1^2+c_1^2+d_1^2)=$$
$$=(aa_1+bb_1+cc_1+dd_1)^2+(ab_1-a_1b-cd_1+c_1d)^2+$$
$$+(ac_1+bd_1-a_1c-b_1d)^2+(ad_1-bc_1+b_1c-a_1d)^2.$$

Tutte queste risultano poi casi particolari di un'altra più complessa secondo cui il prodotto di due somme di otto quadrati è pure una somma di otto quadrati (1).

Passiamo ora ad applicare l'identità di EULERO alla dimostrazione dell'importante

Teorema. « Se un numero primo dispari p, divide una somma di quattro quadrati di cui due almeno non divisibili per p, è esso pure la somma di quattro quadrati ».

Sia il numero primo dispari p divisore della somma

$$A^2+B^2+C^2+D^2.$$

Possiamo intanto supporre A, B, C, D primi tra loro infatti, se ciò non fosse, detto δ il loro m. c. d. e posto

$$A=\delta_1 A_1 \ldots D=\delta_1 D_1$$

ne verrebbe che dividendo p il prodotto:

$$\delta^2(A_1^2+\ldots D_1^2)$$

ed essendo, in seguito all'ipotesi, primo con δ, anche la somma

$$A_1^2+\ldots D_1^2$$

sarebbe multipla di p con $A_1 \ldots D_1$ primi tra loro.

Ciò premesso, prendendo i minimi resti (positivi o negativi) di $A \ldots D$ rispetto p ed indicando con $m \cdot p$ un multiplo in generale di p, dalle

$$A=m\cdot p+a;\quad B=m\cdot p+b;\quad C=mp+c;\quad D=mp+d$$

discende

$$A^2+\ldots+D^2=mp+a^2+b^2+c^2+d^2$$

e quindi:

$$a^2+b^2+c^2+d^2=p\cdot q \tag{1}$$

(1) Cfr. G. PEANO, *Formulaire de mathématiques*, tome II, n. 2, pag. 25.

dove $q > 0$ poichè diversamente $a = b = c = d = 0$ ed $A \ldots . D$, contro l'ipotesi, tutti multipli di p.

Essendo p dispari:

$$2|a| < p \quad 2|b| < p \quad 2|c| < p \quad 2|d| < p$$

$$4(a^2 + b^2 + c^2 + d^2) < 4p^2$$

$$a^2 + b^2 + c^2 + d^2 < p^2 \tag{1'}$$

e da (1), (1')

$$q < p.$$

Se $q = 1$, il *Teorema* è dimostrato.

Sia invece $q > 1$, e prendiamo nuovamente i minimi resti di a, b, c, d rispetto a q

$$a = q \cdot f + \alpha; \quad b = q \cdot g + \beta; \quad c = q \cdot h + \gamma; \quad d = qk + \delta$$

dalle quali:

$$a^2 + b^2 + c^2 + d^2 = m \cdot q + \alpha^2 + \beta^2 + \gamma^2 + \delta^2$$

e quindi per (1)

$$\alpha^2 + \beta^2 + \gamma^2 + \delta^2 = q \cdot q'. \tag{2}$$

In primo luogo, $q' > 0$.

Infatti se $q' = 0$, da (2) seguirebbe

$$\alpha = \beta = \gamma = \delta = 0$$

e quindi a, b, c, d multipli di q e per (1) dovrebbe essere pq divisibile per q^2 cioè p per q il che richiede o $q = 1$ che è stato escluso, o $q = p$ mentre si è già provato $q < p$.

Successivamente, $q' < q$.

In vero:

$$2|\alpha| \leq q \quad 2|\beta| \leq q \quad 2|\gamma| \leq q \quad 2|\delta| \leq q$$

$$\alpha^2 + \beta^2 + \gamma^2 + \delta^2 \leq q^2$$

e per (2):

$$q' \leq q.$$

L'eguaglianza non è possibile, poichè da (2) discenderebbe:

$$\alpha^2 + \beta^2 + \gamma^2 + \delta^2 = q^2 \tag{2'}$$

e siccome α, β, γ, δ non oltrepassano in modulo $\frac{q}{2}$, l'unico

caso in cui possa aver luogo la (2)′ è quello in cui

$$\alpha=\beta=\gamma=\delta=\frac{q}{2}$$

ed allora:

$$a=\frac{q}{2}(2f+1) \quad b=\frac{q}{2}(2g+1)$$

$$c=\frac{q}{2}(2h+1) \quad d=\frac{q}{2}(2k+1)$$

dalle quali

$$a^2+b^2+c^2+d^2=q^2(f^2+g^2+h^2+k^2+f+g+h+k)+q^2$$

e per (1)

$$p=q(f^2+g^2+h^2+k^2+f+g+h+k)+q$$

e quindi p multiplo di q, il che non può essere.

Resta quindi provato che:

$$0<q'<q.$$

Applicando ora l'identità di EULERO ad (1) e (2) risulta:

$$(a^2+\ldots.+d^2)(\alpha^2+\ldots.\delta^2)=p\cdot q^2\cdot q'$$

(3)
$$A_1^2+B_1^2+C_1^2+D_1^2=pq^2q'$$

dove

$$A_1=a\alpha+b\cdot\beta+c\gamma+d\cdot\delta$$
$$B_1=a\beta-\alpha b-c\delta+\gamma d$$
$$C_1=a\gamma+b\delta-\alpha c-\beta d$$
$$D_1=a\delta-b\gamma+\beta c-\alpha d.$$

Se ora sostituiamo ad a, b, c, d le loro espressioni in funzione di q e di α, β, γ, δ si ottiene tenendo conto della (2)

$$A_1=q(f\cdot\alpha+g\beta+h\gamma+k\delta+q')$$
$$B_1=q(f\cdot\beta-g\alpha-h\delta+k\gamma)$$
$$C_1=q(f\gamma+g\delta-h\alpha-k\beta)$$
$$D_1=q(f\delta-g\gamma+h\beta-k\alpha)$$

dalle quali appare che $A_1\ldots.D_1$ sono divisibili per q. Detti quindi a_1, b_1, c_1, d_1 i valori assoluti dei polinomii che moltiplicano q nei secondi membri delle precedenti eguaglianze,

avremo dalla (3)

$$q^2(a_1^2 + b_1^2 + c_1^2 + d^{12}) = p \cdot q^2 \cdot q'$$

$$a_1^2 + b_1^2 + c_1^2 + d_1^2 = pq'.$$

Se $q' = 1$ il *Teorema* è dimostrato: diversamente notando che $a_1 \ldots d_1$ non possono essere tutti multipli di p poichè allora per la (3) risulterebbe $q^2 \cdot q'$ divisibile per p, operando sui numeri $a_1 \ldots d_1$ come sui precedenti, si passa ad una terza identità

$$a_2^2 + b_2^2 + c_2^2 + d_2^2 = p \cdot q''$$

dove

$$0 < q'' < q'$$

e così di seguito, per cui dal fatto che i fattori q vanno decrescendo senza poter raggiungere lo zero, resta provato che si arriverà sempre ad un'identità in cui $q = 1$ ed il teorema è dimostrato (1).

Corollario. « Se un intero qualunque divide la somma di quattro quadrati primi tra di loro, esso è pure la somma di quattro quadrati ».

Cominciamo dall'osservare che per $p = 2$ si ha:

$$2 = 1 + 1 = 1^2 + 1^2 + 0^2 + 0^2.$$

Ciò premesso, sia n un intero qualunque che divida

$$a^2 + b^2 + c^2 + d^2$$

dove $a \ldots d$ sono primi tra loro.

Di qualunque fattore primo dispari di n si potrà dire che divide pure la somma di quattro quadrati due dei quali almeno non multipli di p poichè, diversamente a, b, c, d non sarebbero primi tra loro, e quindi poichè pel *Teorema* dimostrato, ciascun fattore primo dispari di n è somma di quattro quadrati e tale può considerarsi il 2, ne segue, applicando reiteratamente l'identità di EULERO, che anche al numero composto n compete la stessa proprietà (2).

(1) La dimostrazione di questo Teorema condotta sulla traccia di quella proposta da EULERO è dovuta ad A. MATROT. Cfr. HUMBERT, *Traité d'Aritmétique avec des compléments*, Paris, Vinbert et Nony, 1908.

(2) Questo Corollario è dato come Teorema negli *Exercices d'Analyse numérique* del LE BESGUE già citati, e nell'*Algèbre Supérieure* del SERRET, tome II, pag. 99, ma le dimostrazioni riportate sono incomplete.

Capitolo III.

NUMERI CONGRUI E CONGRUENZE

Introduzione. — Il problema dell'Analisi indeterminata prende una nuova forma più semplice mercè l'introduzione di un concetto e di un simbolo appropriato dovuto a Gauss. Nasce in tal modo la così detta *teoria delle congruenze.*

L'idea di Gauss consiste nel trattare come una specie di eguaglianza (congruenza) la relazione intercedente tra due numeri che divisi per un terzo (modulo) danno resti uguali, godendo, tale relazione, delle proprietà fondamentali riflessiva, simmetrica e transitiva (Cfr. F. Enriques - *I numeri reali* - Articolo IX del I Vol.). Le congruenze contenenti incognite corrispondono a problemi equivalenti d'analisi indeterminata; per es. la risoluzione della congruenza

$$f(x) \equiv 0 \qquad \text{mod } n$$

equivale alla risoluzione in numeri interi dell'equazione indeterminata:

$$f(x) - ny = 0.$$

Ma la trattazione di questi problemi riesce semplificata del concetto di congruenza come apparirà dagli sviluppi seguenti.

In questo Capitolo, esposte le principali proprietà delle congruenze identiche, passeremo a dimostrare i più importanti teoremi sulle radici di una congruenza ad una incognita di grado n rispetto ad un modulo primo, applicando quindi i risultati ottenuti alla risoluzione delle congruenze generali di 1° grado ad un'incognita, e di quelle binomie della forma

$$x^n \equiv 1 \qquad \text{mod } p$$

ed allo studio delle principali proprietà dei residui onde completare la dimostrazione del *Teorema di Bachet.*

Chiuderemo col trattare brevemente delle *radici primitive* e della *teoria degli indici* mostrando l'uso che se ne può fare nella risoluzione delle congruenze binomie generali

$$ax^n \equiv b \qquad \text{mod } p.$$

§ 1. **Definizione e proprietà delle congruenze identiche.** — *Definizione.* « Due interi qualunque (positivi o negativi) si dicono congrui rispetto ad un *intero positivo* n chiamato *modulo*, quando, divisi per n, danno resti eguali ».

Per evitare ogni incertezza, sia il dividendo positivo o negativo, il resto si assumerà sempre positivo.

Così ad esempio, come resto della divisione di (-12) per 5 si considererà 3 e non (-2).

Per indicare la congruenza di due numeri a, b rispetto ad un modulo n si usa la notazione:

$$a \equiv b \mod n.$$

Corollario. « Se a è multiplo di n, si può dire congruo a $0 \pmod n$ ed inversamente ».

Teorema 1°. Se

$$a \equiv b \mod n$$

si ha pure:

$$(a - b) \equiv 0 \mod n$$

e reciprocamente ».

Per ipotesi:

$$a = nq + r \quad b = n \cdot q' + r$$

quindi:

$$a - b = n(q - q') \equiv 0 \mod n.$$

Supposto invece:

$$a - b \equiv 0 \mod n$$

da

$$a = n \cdot q + r \quad b = n \cdot q' + r'$$

si ricava:

$$a - b = n(q - q') + r - r'$$

e quindi dall'ipotesi, segue:

$$r - r' \equiv 0 \mod n$$

e poichè

$$r, \quad r' < n, \quad r = r'.$$

Alla data definizione di congruenze si può sostituire la seguente « Due numeri si dicono congrui mod n, quando la loro differenza è divisibile per n ».

Dalla seconda delle due definizioni, si deduce immediatamente:

Corollario 1°. « Aggiungendo (o togliendo) uno stesso

intero ai due membri di una congruenza, risultano numeri (1) congrui rispetto allo stesso modulo ».

Corollario 2°. « Moltiplicando i due membri di una congruenza per uno stesso numero, si ottiene una nuova congruenza riferita allo stesso modulo ».

Teorema 2°. « Dividendo due numeri congrui mod n per un loro comune divisore m, i quozienti sono in generale congrui. mod $\frac{n}{\delta}$, essendo $\delta = D(m, n)$ ».

Sieno infatti $a \cdot m$, $b \cdot m$ dotati del divisore comune m, e si abbia:

$$a \cdot m \equiv b\, m \qquad \text{mod } n.$$

Segue pel *Teorema 1°*

$$m(a - b) \equiv 0 \qquad \text{mod } n$$

da cui non si può dedurre in generale

$$a - b \equiv 0 \qquad \text{mod } n.$$

Se però si pone $m = m' \cdot \delta$; $n = n' \cdot \delta$, risulta che

$$m'(a - b)$$

dev'essere divisibile per n'; e siccome m' ed n' sono primi tra loro, necessariamente dovrà esser multipla di n' la differenza $(a - b)$, cioè:

$$a \equiv b \qquad \text{mod } n' = \frac{n}{\delta}.$$

Corollario. « Se $\delta = 1$, $n' = n$ e quindi

$$a \equiv b \qquad \text{mod } n$$

cioè « i due membri di una congruenza si possono dividere per un loro fattore comune primo col modulo ».

Osservazione. « Che il fattore comune sia primo col modulo, è condizione sufficiente perchè esso si possa eliminare senza cambiare il modulo, ma non però necessaria.

(1) Per brevità con « numero » intenderemo sempre un intero positivo o negativo.

Così ad esempio, da

$$21 \equiv -15 \qquad \text{mod } 12$$

si ottiene, dividendo per 3:

$$7 \equiv -5 \qquad \text{mod } 12.$$

Teorema 3°. « Date due o più congruenze rispetto allo stesso modulo, sommandole e sottraendole membro a membro, risulta una nuova congruenza rispetto allo stesso modulo ».

Teorema 4°. « Se più congruenze con lo stesso modulo si moltiplicano membro a membro, si ha una nuova congruenza con lo stesso modulo ».

Corollario. I due membri di una congruenza si possono innalzare a potenza con lo stesso qualsiasi esponente intero e positivo ».

Applicando reiteratamente i *Teoremi* 1, 3, 4 ed i *Corollarii* si ricava che da un sistema di congruenze:

$$\left.\begin{aligned} a_1 &\equiv b_1 \\ a_2 &\equiv b_2 \\ &\cdots\cdots \\ a_r &\equiv b_r \end{aligned}\right\} \quad \text{mod } n$$

se ne possono dedurre infinite altre del tipo:

$$\begin{aligned} & c_1 \cdot a_1^{\lambda_1} \cdot a_2^{\lambda_2} \ldots a_r^{\lambda_r} + c_2 a_1^{\mu_1} \cdot a_2^{\mu_2} \ldots a_r^{\mu_r} + \ldots \\ & \equiv c_1 b_1^{\lambda_1} \cdot b_2^{\lambda_2} \ldots b_r^{\lambda_r} + c_2 b_1^{\mu_1} \cdot b_2^{\mu_2} \ldots b_r^{\mu_r} + \ldots \qquad \text{mod } n \end{aligned}$$

dove c_1, c_2.... sono interi qualunque e λ, μ interi positivi.

§ 2. **Teorema di Fermat generalizzato. - Dimostrazione di Gauss.** — Sia n un intero positivo qualsiasi ed

$$(1) \qquad \alpha_1, \quad \alpha_2, \ldots \quad \alpha_{\varphi(n)}$$

i $\varphi(n)$ numeri primi ad n e non maggiori di n.

Detto α uno qualunque degli (1), consideriamo i $\varphi(n)$ prodotti:

$$(2) \qquad \alpha \cdot \alpha_1, \quad \alpha \cdot \alpha_2, \ldots \quad \alpha \cdot \alpha_{\varphi(n)}.$$

Essi sono tutti tra loro incongrui mod n. Infatti dall'ipotesi:

$$\alpha \cdot \alpha_r \equiv \alpha \cdot \alpha_s \qquad \text{mod } n$$

pel *Teorema* 2° § 1, discenderebbe:

$$\alpha_r \equiv \alpha_s \qquad \text{mod } n$$

il che è assurdo. Siccome poi i numeri (2) sono anche tutti primi con n, ne segue che divisi per n dovranno dare per resti i numeri (1) e quindi:

$$\left.\begin{aligned} \alpha \cdot \alpha_1 &\equiv \alpha_1' \\ \alpha \cdot \alpha_2 &\equiv \alpha_2' \\ &\cdots\cdots \\ \alpha \cdot \alpha_{\varphi(n)} &\equiv \alpha'_{\varphi(n)} \end{aligned}\right\} \text{mod } n$$

dove α_1', α_2',.... $\alpha'_{\varphi(n)}$ costituiscono una permutazione dei resti (1).

Moltiplicando membro a membro (*Teorema 4'*, § 1)

$$\alpha^{\varphi(n)} \cdot (\alpha_1 \alpha_2 \ldots \alpha_{\varphi(n)}) \equiv \alpha_1' \cdot \alpha_2' \ldots \alpha'_{\varphi(n)} \qquad \text{mod } n.$$

Ma il prodotto $\alpha_1 \alpha_2 \ldots \alpha_{\varphi(n)}$ di fattori primi con n, è pure primo con n per cui (*Teorema* 2°, *Corollario.* § 1°)

$$\alpha^{\varphi(n)} \equiv 1 \qquad \text{mod } n$$

la qual relazione costituisce il *Teorema* di FERMAT, generalizzato da EULERO.

La precedente dimostrazione è dovuta a GAUSS.

§ 3. **Campo di razionalità.** — Dato un numero primo p, immaginiamo di scomporre tutti gli interi positivi o negativi in classi, seguendo il principio di collocare in una stessa classe tutti quelli che divisi per p danno uno stesso resto.

Due elementi appartenenti ad una stessa classe saranno congrui mod p, mentre ciò non accadrà mai di due termini estratti da classi diverse.

Siccome poi la relazione di congruenze soddisfa alla proprietà riflessiva, simmetrica e transitiva, gli elementi di una stessa classe si potranno identificare con uno qualunque di loro. Ne viene che prendendo da ciascuna classe un individuo, si viene a formare un insieme di enti

$$r_0 \quad r_1, \quad r_2, \ldots \quad r_{p-1}$$

tali che le operazioni:

$$r_h \pm r_k; \quad r_h \cdot r_k; \quad \frac{r_h}{r_k}(r_k \not\equiv 0); \quad r_h^n$$

resteranno pienamente definite e daranno sempre un risultato appartenente allo stesso insieme, valendo per esse il principio di *sostituzione* e tutte le altre leggi che valgono per le medesime operazioni sui numeri reali e, più in generale, nei numeri complessi.

Così, p. es., nel caso della divisione è facile provare che dati due elementi r_h, $r_k(r_k \not\equiv 0)$, ne esiste sempre un terzo ed uno solo r_q per cui: $r_h \equiv r_k \cdot r_q \pmod p$.

Infatti, se si considerano i prodotti

$$r_k \cdot r_0; \quad r_k \cdot r_1; \quad r_k \cdot r_2 \ldots; \quad r_k \cdot r_{p-1}$$

si trova che essi sono tutti incongrui mod p per cui uno ed uno solo di essi sarà $\equiv r_h$. Se questo è $r_k \cdot r_q$, considereremo la notazione

$$r_h \equiv r_k \cdot r_q \qquad \text{mod } p$$

come equivalente all'altra:

$$\frac{r_h}{r_k} \equiv r_q \qquad \text{mod } p\ .$$

È poi palese che essendo p, primo se $r_q' \not\equiv r_q$, non potrà essere

$$r_h \equiv r_k \cdot r_q' \qquad \text{mod } p$$

e di qui l'unicità del quoziente.

In seguito a queste considerazioni si può dire che gli elementi r costituiscono un « campo di razionalità » e tale campo è il caso particolare più semplice del così detto « campo di GALOIS » [1].

§ 4. **Teorema d'identità di due polinomii.** — Definito così il campo di razionalità:

$$(C) \qquad r_0, \quad r_1, \quad r_2, \ldots \quad r_{p-1}$$

[1] Da questo momento in poi le congruenze che seguono saranno sempre riferite ad uno stesso modulo p, e quindi si ommetterà l'indicazione del modulo stesso.

consideriamo l'espressione:

$$f(x) = a_0 x^n + a_1 x^{n-1} + ... + a_n$$

in cui i coefficienti sono estratti dal campo, ed x è una variabile suscettibile dei p valori di C.

È palese, in primo luogo, che la funzione $f(x)$ potrà assumere, in corrispondenza alla variabile, al più p valori distinti mod p.

Facciamo quindi vedere che si può limitarsi a considerare funzioni il cui grado non superi $(p-1)$.

Se infatti $n - i > p - 1$, posto:

$$n - i = k(p-1) + \nu_i; \quad \nu_i \leq p - 1$$

sarà:

$$a_i x^{n-i} = a_i (x^{p-1})^k \cdot x^{\nu_i} \equiv a_i \cdot x^{\nu_i}$$

e quindi ad ogni termine della data funzione di grado $> p-1$ si può sostituirne uno di grado $\leq (p-1)$ ad esso congruo per ogni valore di x.

Ciò premesso, dimostriamo il seguente

Teorema 1°. » La condizione necessaria e sufficiente perchè una funzione $f(x)$ di grado $n \leq p-1$ sia identicamente nulla mod p, cioè sia:

$$f(x) \equiv 0$$

per ogni valore di x in (C), è che sia:

$$a_0 \equiv a_1 \equiv a_2 \equiv .... \equiv a_n \equiv 0.$$

Che la condizione sia sufficiente, è manifesto.

Per provare che essa è pure necessaria attribuiamo ad x i valori:

$$1, \quad 2, \quad 3, ... \quad (n+1)$$

in numero al più di $n + 1 = p$.

Avremo così un sistema di congruenze:

$$a_0 i^n + a_1 i^{n-1} + ... + a_n \equiv 0$$
$$i = 1, \ 2, \ 3, ... \ (n+1)$$

che equivale ad un sistema di equazioni lineari rispetto ai coefficienti:

$$a_0 \cdot 1^n + a_1 \cdot 1^{n-1} + ... + a_n = k_1 \cdot p$$
$$a_0 2^n + a_1 2^{n-1} + ... + a_n = k_2 \cdot p$$
$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots$$
$$a_0 (n+1)^n + a_1 (n+1)^{n-1} + ... + a_n = k_{n+1} \cdot p$$

delle quali, considerando come incognite le a e risolvendo, si trova:

$$a_i = \frac{\begin{vmatrix} 1^n & 1^{n-1} & \dots k_1 p & \dots 1 \\ 2^n & 2^{n-1} & \dots k_2 p & \dots 1 \\ \dots & \dots & \dots & \dots \\ (n+1)^n & (n+1)^{n-1} & \dots k_{n+1} p & \dots 1 \end{vmatrix}}{\begin{vmatrix} 1^n & 1^{n-1} & \dots & 1 \\ 2^n & 2^{n-1} & \dots & 1 \\ \dots & \dots & \dots & \dots \\ (n+1)^n & (n+1)^{n-1} & \dots & 1 \end{vmatrix}}$$

Il denominatore è il determinante di VANDERMONDE formato con le $(n+1)$ quantità

$$1, \quad 2, \quad 3, \dots \quad (n+1)$$

che, a meno del segno, coincide col prodotto:

$$\Pi(\alpha - \beta)$$

$$\alpha \gtrless \beta; \quad \alpha = 1, 2, \dots (n+1); \quad \beta = 1, 2, \dots (n+1)$$

in cui nessuno dei fattori potrà esser nullo, nè, in conseguenza dell'ipotesi $n < p$, divisibile per p. Essendo quindi il denominatore diverso da zero e primo con p, mentre il numeratore contiene manifestamente il fattore p, si conclude che a_i è multiplo di p, cioè:

$$a_i \equiv 0.$$

Corollario. « Se due funzioni $f_1(x)$, $f_2(x)$ dello stesso grado $< p$ sono tali che, per ogni valore di x, si abbia:

$$f_1(x) \equiv f_2(x)$$

i coefficienti dell'una sono congrui mod p ai corrispondenti dell'altra: e se sono di grado diverso, ma sempre $< p$, i coefficienti di quella di grado maggiore che non hanno il corrispondente nell'altra, devono esser nulli mod p ed i rimanenti della prima congrui ai rimanenti della seconda ».

§ 5. **Condizione di divisibilità per $x - \alpha$.** — Date due funzioni $f_1(x)$, $f_2(x)$ di gradi m, n $m \geq n$, applicando ad esse il noto procedimento della divisione si giunge all'identità algebrica:

$$f_1(x) = f_2(x) \cdot Q(x) + R(x) \tag{1}$$

dove $Q(x)$ ed $R(x)$ sono pienamente determinati qualora si imponga le condizioni che $Q(x)$ sia di grado $(m - n)$ e che il grado di $R(x)$ sia $< n$.

È quindi manifesto che, anche limitando il significato di x e dei coefficienti al campo (C), si avrà identicamente [1]:

$$f_1(x) \equiv f_2(x) \cdot Q(x) + R_1(x). \tag{2}$$

Se $R_1(x)$ si riduce ad una costante nulla mod p o ad un polinomio a coefficienti nulli si dirà che « $f_1(x)$ è divisibile per $f_2(x)$ ».

Ponendo ora in (1), $f_2(x) = x - \alpha$, com'è ben noto essa si cambia nella:

$$f_1(x) = (x - \alpha) \cdot Q(x) + f_1(\alpha)$$

e la (2) nella congruenza:

$$f_1(x) \equiv (x - \alpha) \cdot Q(x) + f_1(\alpha)$$

da cui si deduce immediatamente il *Teorema* « La condizione necessaria e sufficiente perchè $f_1(x)$ sia divisibile per $(x - \alpha)$ in senso congruenziale è espressa da:

$$f_1(\alpha) \equiv 0 \ ».$$

§ 6. **Soluzioni e radici di una congruenza $f(x) \equiv 0$ mod p. - Teorema fondamentale sul numero delle radici.** — Data una funzione $f(x)$ di grado $n < p$, se per un certo valore α di x

$$f(\alpha) \equiv 0$$

[1] Notiamo, a questo proposito, che nella divisione *algebrica*, i coefficienti di $Q(x)$, $R(x)$ risultano funzioni razionali frazionarie di quelli di $f_1(x)$, $f_2(x)$ aventi però per denominatori le successive potenze del coefficiente, diverso da zero, del termine di grado più elevato del divisore; e, che, anche restringendo il significato dei predetti coefficienti ad elementi di (C), il primo di quelli del divisore si suppone sempre non nullo mod p.

si dirà che α è una soluzione della congruenza:

$$f(x) \equiv 0.$$

È palese (§ 1) che se la precedente ammette una soluzione α, ne possiede infinite che vengono date da $x \equiv \alpha$.

Tra le infinite soluzioni che può ammettere una congruenza, converremo per maggior chiarezza di distinguere come « radici » quelle positive e minori del modulo.

Dopo ciò dimostriamo il seguente:

Teorema « Una congruenza non identica

$$f(x) \equiv 0 \mod p \tag{1}$$

di grado $n < p$, non può ammettere più di n radici distinte ».

Sia α_1 una radice di (1). Avremo identicamente:

$$f(x) \equiv (x - \alpha_1) f_1(x). \tag{2}$$

Se ora α_2 è una seconda radice di (1) incongrua ad α_1, sostituendo in (2) si ricava:

$$f(\alpha_2) \equiv (\alpha_2 - \alpha_1) \cdot f_1(\alpha_2)$$

da cui essendo per ipotesi $f(\alpha_2) \equiv 0$ ed $(\alpha_2 - \alpha_1)$ primo con p, si deduce:

$$f_1(\alpha_2) \equiv 0$$

e quindi (§ 2)

$$f_1(x) \equiv (x - \alpha_2) \cdot f_2(x)$$

e sostituendo in (2)

$$f(x) \equiv (x - \alpha_1)(x - \alpha_2) \cdot f_2(x). \tag{3}$$

Parimenti se esiste una terza radice α_3 distinta da α_1 ed α_2 per la (3) si ricava:

$$f(\alpha_3) \equiv 0 \equiv (\alpha_3 - \alpha_1)(\alpha_3 - \alpha_2) \cdot f_2(\alpha_3)$$

da cui come prima

$$f_2(\alpha_3) \equiv 0$$

$$f_2(x) \equiv (x - \alpha_3) \cdot f_3(x)$$

e quindi sostituendo in (3):

$$f(x) \equiv (x - \alpha_1)(x - \alpha_2)(x - \alpha_3) \cdot f_3(x). \tag{4}$$

Così continuando, una volta che si pervenga alla:

$$(5) \qquad f(x) \equiv (x - \alpha_1)(x - \alpha_2) \ldots (x - \alpha_n) \cdot f_n(x)$$

la $f_n(x)$ deve esser ridotta ad una costante poichè $f_1(x), f_2(x) \ldots$ vanno decrescendo di grado ed $f_1(x)$ è di grado $(n-1)$.

Ma se $f_n(x)$ è una costante, essa non può esser nulla mod p, poichè diversamente il polinomio che risulta dallo sviluppo del secondo membro avrebbe tutti i coefficienti multipli di p e, data la sua identità con $f(x)$, pel *Teorema 1°* (*Corollario*) anche i coefficienti di quest'ultimo dovrebbero esser tutti nulli, ed allora la (1), contro l'ipotesi, sarebbe identica.

Stabilito così che $f_n(x)$ è una costante non nulla, è subito provato che la (1) non può aver altre radici oltre le supposte: se infatti ve ne fosse un'altra β distinta dalla α, il prodotto

$$(\beta - \alpha_1)(\beta - \alpha_2) \ldots (\beta - \alpha_n) \cdot f_n(\beta)$$

dovrebbe esser multiplo di p, senza che lo fosse alcuno dei suoi fattori.

Osservazione. Si è dimostrato che una congruenza di grado n non può avere più di n radici distinte mod p. Definendo però il concetto di *radice multipla* e di *ordine di molteplicità*, il *Teorema* precedente si può estendere dimostrando che se $\lambda_1, \lambda_2, \ldots \lambda_h$ sono gli ordini di molteplicità delle radici distinte $\alpha_1, \alpha_2, \ldots \alpha_h$ non può essere

$$\lambda_1 + \lambda_2 + \ldots + \lambda_h > n$$

senza che la $f(x) \equiv 0$ si riduca ad una identità.

Non insistiamo però su questo argomento che non ci sarebbe utile pel seguito: notiamo solo che dal *Teorema* precedente discende immediatamente il

Corollario 1°. « Se la $f(x) \equiv 0$ di grado $< p$ ammette più radici distinte che unità il suo grado, essa deve avere i suoi coefficienti nulli mod p ».

Corollario 2°. « Se $\alpha_1 \alpha_2 \ldots \alpha_h$ sono tutte le radici di una congruenza priva di radici multiple, si ha identicamente:

$$f(x) \equiv (x - \alpha_1)(x - \alpha_2) \ldots (x - \alpha_h) \cdot f_1(x)$$

dove $f_1(x)$ è un polinomio di grado $(n-h)$ che in (C) non ammette alcuna radice ».

Osservazione. Se avviene che una congruenza $f(x) \equiv 0$, i cui coefficienti appartengono a (C) non sia soddisfatta da alcun elemento di (C), tuttavia estendendo il campo con l'introduzione dei così detti « immaginarii di GALOIS » si può sempre costruire un campo di razionalità più esteso (K) detto « pseudo-ortoide » il quale risulta costituito da un insieme di enti che il DICKSON giustamente distingue col nome di « marche » sui quali si può operare formalmente secondo le ordinarie leggi dell'Aritmetica, e tra cui la

$$f(x) \equiv 0.$$

possiede tante radici quante unità il suo grado.

§ 7. **Risoluzione di $ax \equiv b \mod n$ per a ed n primi tra loro.** — Proponiamoci la risoluzione della congruenza di 1° grado ad un'incognita.

$$ax \equiv b \mod n \tag{1}$$

in cui si suppone a primo con n.

Essendo $D(n, a) = 1$ i prodotti:

$$a \cdot 1 \quad a \cdot 2 \ldots \quad a \cdot n \tag{2}$$

sono tutti tra loro incongrui, poichè dall'ipotesi:

$$a \cdot r \equiv a \cdot s \mod n$$

seguirebbe che $a(r - s)$ dovrebbe esser multiplo di n, il che è impossibile essendo n primo con a ed $(r - s)$ in valore assoluto minore di n.

Fra i numeri (2) ve ne sarà quindi uno ed uno solo $a \cdot \eta$ pel quale:

$$a\eta \equiv b \mod n$$

cioè esiste un numero positivo $\eta \leq n$ tale che soddisfa alla proposta

È poi palese che la (1), oltrechè da $x = \eta$, è verificata pure da $x = \eta + k \cdot n$ dove k è un intero qualunque, per cui si conclude che essa ammette infinite *soluzioni* dando il nome di *radice* (§ 6) all'unica positiva e $\leq n$.

Ciò premesso, moltiplicando i due membri di

$$a\eta \equiv b \mod n$$

per $a^{\varphi(n)-1}$ e rammentando (§ 2) che

$$a^{\varphi(n)} \equiv 1 \mod n$$

si ottiene

$$\eta \equiv b \cdot a^{\varphi(n)-1} \mod n.$$

Volendo adunque determinare la radice di (1) bisogna calcolare il resto di $b \cdot a^{\varphi(n)-1}$ rispetto al divisore n.

Abbiamo così il

Teorema. « Se a è primo con n, la congruenza

$$ax \equiv b \mod n$$

ammette una ed una sola radice

$$\eta \equiv b \cdot a^{\varphi(n)-1} \mod n.$$

§ 8. **Risoluzione in generale di $ax \equiv b \bmod n$.** — Consideriamo ora la

(1) $$ax \equiv b \mod n$$

in cui supponiamo solo $a \not\equiv 0 \bmod n$ e si ponga $\delta = D(a, n)$.

In primo è manifesto che per la risoluzione di (1) è necessario che b sia divisibile per δ; ed ammesso ciò, ponendo

$$a = \delta\alpha \quad b = \delta \cdot \beta \quad n = \delta \cdot \nu$$

avremo

$$\alpha\delta x \equiv \beta \cdot \delta \mod \delta \cdot \nu$$

e sopprimendo il fattore comune δ (§ 1, *Teorema* 2°)

(2) $$\alpha x \equiv \beta \mod \nu$$

dove α, ν sono primi tra loro.

Le (1) (2) sono equivalenti per quanto concerne le soluzioni, poichè quelle dell'una lo sono pure dell'altra; ma, la (2) (§ 7) ammette una ed una sola radice η, e quindi una radice η (minore a più forte ragione di n) compete pure ad (1).

Ma le soluzioni della (2):

$$\eta + \nu; \quad \eta + 2\nu; \quad \ldots \quad \eta + (\delta - 1)\nu$$

soddisfano pure la (1) e sono tutte minori di n, quindi esse sono altrettanti radici di (1) che ne ammette così δ. Essa poi

non può averne altre: infatti se ξ è una radice di (1) e quindi soluzione di (2) essa dev'esser congrua ad $\eta \bmod \nu$ poichè se:

$$\xi \equiv \eta' \qquad \bmod \nu; \quad \eta' < \nu$$

η' sarebbe pure radice di (2) che ne avrebbe due contro il paragrafo precedente.

Abbiamo così il

Teorema. « Se $\delta = D(a, n)$ e b è divisibile per δ senza che sia a multiplo di n, la congruenza

$$ax \equiv b \qquad \bmod n$$

ammette δ radici

$$\eta, \quad \eta + \nu, \ldots \quad \eta + (\delta - 1)\nu$$

essendo η radice di

$$\alpha x \equiv \beta \qquad \bmod \nu$$

dove si è posto:

$$\alpha = \frac{a}{\delta} \quad \beta = \frac{b}{\delta} \quad \nu = \frac{n}{\delta} \text{ ».}$$

Osservazione. È manifesta l'equivalenza del problema relativi alla soluzione di

$$ax \equiv b \qquad \bmod n$$

con l'altro che ha per iscopo la risoluzione in numeri interi di

$$ax - ny = b.$$

Notiamo che le δ radici di (1) si riducono, conformemente al § 6, ad una sola se n è primo; nel qual caso è sempre soddisfatta la condizione $D(n, a) = 1$ per $a \not\equiv 0 \bmod n$.

Ove poi sia contemporaneamente.

$$a \equiv b \equiv 0 \qquad \bmod n$$

la (1) diviene indeterminata; e se

$$a \equiv 0 \quad b' \not\equiv 0 \qquad \bmod n$$

insolubile.

§ 9. **Altra risoluzione del problema trattato al § 9 del Cap. II.** — Al § 7 del Cap. 2° si è risolto il problema di determinare un intero che diviso per altri $a_1, a_2, \ldots a_n$ dia rispettivamente per resti $r_1, r_2, \ldots r_n$.

Riprendiamo ora la questione per trattarla in modo completo e risolviamo intanto il

Problema. « Supposti a_1, a_2 primi tra loro e detto π il loro prodotto, determinare la forma dei numeri che divisi per a_1, a_2 danno rispettivamente per resti r_1, r_2 ».

Il problema corrisponde alla soluzione del sistema di congruenze:

$$(1) \qquad \begin{cases} x \equiv r_1 & \mod a_1 \\ x \equiv r_2 & \mod a_2 . \end{cases}$$

Della prima si ricava:

$$x = r_1 + ka_1$$

dove k è un intero qualunque, e sostituendo nell'altra:

$$r_1 + ka_1 \equiv r_2 \qquad \mod a_2$$

e risolvendo rispetto a k:

$$k \equiv (r_2 - r_1)a_1^{\varphi(a_2)-1} \qquad \mod a_2$$
$$k = (r_2 - r_1)a_1^{\varphi(a_2)-1} + k' \cdot a_2 .$$

Sostituendo tale valore di k nella precedente espressione di x, otteniamo:

$$x = r_1 + (r_2 - r_1)a_1^{\varphi(a_2)} + k' \cdot a_1 a_2$$

e quindi passando dalla eguaglianza alla congruenza:

$$x \equiv r_1 + (r_2 - r_1)a_1^{\varphi(a_2)} \qquad \mod \pi$$
$$x \equiv r_1\left(1 - a_1^{\varphi(a_2)}\right) + r_2 \cdot a_1^{\varphi(a_2)} \qquad \mod \pi .$$

Osservando ora che l'espressione

$$1 - a_1^{\varphi(a_2)} - a_2^{\varphi(a_1)}$$

è per il *Teorema* di FERMAT multipla di a_1 ed a_2 e quindi di π essendo $D(a_1, a_2) = 1$, si conclude che

$$1 - a_1^{\varphi(a_2)} \equiv a_2^{\varphi(a_1)} \qquad \mod \pi$$

per cui la precedente espressione diventa:

$$x \equiv r_1 \cdot a_2^{\varphi(a_1)} + r_2 a_1^{\varphi(a_2)} \qquad \mod \pi$$

ed in fine:

$$x \equiv r_1\left(\frac{\pi}{a_1}\right)^{\varphi(a_1)} + r_2\left(\frac{\pi}{a_2}\right)^{\varphi(a_2)} \qquad \text{mod}\,\pi$$

che ci dà la forma di tutti e soli i numeri soddisfacenti alle volute condizioni.

Osservazione. Il problema si estende al caso di quanti si vogliano moduli

$$a_1 \quad a_2 \ldots\ldots \quad a_n$$

primi tra loro due a due, dimostrando in primo luogo come conseguenza del *Teorema* di FERMAT e dell'ipotesi relativa ai numeri a che, posto:

$$P = \left(\frac{\pi}{a_1}\right)^{\varphi(a_1)} + \left(\frac{\pi}{a_2}\right)^{\varphi(a_2)} + \ldots\ldots \left(\frac{\pi}{a_n}\right)^{\varphi(a_n)}$$

si ha

$$P \equiv 1 \qquad \text{mod}\, a_i \qquad (i = 1, 2, \ldots\ldots n)$$

e ricorrendo poi al solito processo d'induzione.

§ 10. **Sistema ridotto o gruppo di residui mod p.** — Dal campo di razionalità (C) immaginiamo tolto l'elemento $r_0 \equiv 0 \pmod p$ e sia:

$$(G) \qquad r_1, \quad r_2, \ldots\ldots \quad r_{p-1}$$

l'insieme degli elementi rimanenti.

Il sistema (G) ammette le seguenti proprietà.

a) Il prodotto di due elementi di (G) è congruo (mod p) ad uno degli stessi.

b) Il prodotto di tre o più elementi di (G) è associativo.

c) Da una delle due relazioni

$$r_k \cdot r_i \equiv r_k \cdot r_j$$

$$r_i \cdot r_k \equiv r_j \cdot r_k$$

si deduce sempre

$$r_i \equiv r_j .$$

In seguito a ciò si dirà che l'insieme (G) costituisce un « gruppo » [1].

Siccome poi in questo caso, oltre alle condizioni *a*), *b*), *c*)

[1] WEBER. *Lehrbuch der Algebra.* T. II.

è pure sempre soddisfatta l'altra:

$$r_i r_k \equiv r_k \cdot r_i$$

il gruppo vien detto « abeliano ».

Ciò premesso consideriamo la congruenza:

$$x^{p-1} \equiv 1 \mod p \tag{1}$$

Segue del *Teorema* di FERMAT, che essa possiede $(p-1)$ radici distinte:

$$1,\ 2,\ 3,\ldots\ (p-1)$$

alle quali (§ 1) possiamo sostituire

$$r_1,\ r_2,\ldots\ r_{p-1}.$$

Avremo quindi identicamente (§ 6):

$$x^{p-1} - 1 \equiv (x-1)(x-2)\ldots(x-(p-1))$$

da cui (§ 4) si deduce che le funzioni simmetriche elementari dei numeri.

$$1,\ 2,\ldots\ (p-1)$$

sono tutte nulle mod p, ad eccezione dell'ultima congrua a (-1) il qual ultimo risultato costituisce il *Teorema* di WILSON già dimostrato al Cap. I.

Le stesse conclusioni valgono pei numeri

$$r_1\ \ r_2\ldots\ r_{p-1}$$

Si deduce poi subito che $(p-1)$ è il più piccolo esponente per cui risulti soddisfatta da qualunque r una congruenza dal tipo (1).

Se infatti vi fosse un altro esponente $\nu < (p-1)$ dotato della stessa proprietà, la

$$x^{\nu} \equiv 1$$

ammetterebbe un numero di soluzioni superiore al suo grado il che è impossibile.

§ 11. **Teorema di Lagrange relativo all'ordine di un sottogruppo.** — Essendo ν un intero qualunque positivo, minore di $(p-1)$ o in generale non multiplo di $(p-1)$, conside-

riamo i resti mod p delle potenze:

$$r_1^{\nu} \quad r_2^{\nu} \ldots \quad r^{\nu}{}_{p-1}$$

e siano:

$$(1) \qquad 1, \quad \rho_1, \quad \rho_2, \ldots \quad \rho_{\mu-1}$$

quelli tra loro diversi mod p. (1).

Poichè:

$$\rho_i \equiv r_k^{\nu} \qquad \rho_h \equiv r_\lambda^{\nu}$$

segue:

$$\rho_i \rho_h \equiv (r_k \cdot r_\lambda)^{\nu} \equiv (r')^{\nu} \equiv \rho'$$

ed anche gli elementi (1) contenuti in (G) costituiscono alla lor volta un gruppo che si dirà un sottogruppo di (G) indicandolo con (G_μ).

Detto quindi λ_2 un elemento di (G) non contenuto in (G_μ) consideriamo i prodotti:

$$(2) \qquad \lambda_2 \quad \lambda_2\rho_1 \quad \lambda_2\rho_2 \ldots \quad \lambda_2\rho_{\mu-1}.$$

Gli elementi di (2) sono tutti tra loro incongrui, poichè dall'ipotesi:

$$\lambda_2 \rho_h \equiv \lambda_2 \rho_k$$

seguirebbe:

$$\lambda_2(\rho_h - \rho_k) \equiv 0$$

che può sussistere solo per $\rho_h \equiv \rho_k$.

Inoltre nessuno dei (2) può coincidere con alcuno degli (1): poichè, diversamente, dall'ipotesi:

$$\lambda_2 \rho_i \equiv \rho_k$$

moltiplicando i due membri per ρ_i^{p-2} seguirebbe:

$$\lambda_2 \rho_i^{p-1} \equiv \rho_k \cdot \rho_i^{p-2}$$

ed essendo $\rho_i^{p-1} \equiv 1$

$$\lambda_2 \equiv \rho_k \rho_i^{p-2}$$

e siccome gli elementi ρ costituiscono essi pure un gruppo, si avrebbe in fine:

$$\lambda_2 \equiv \rho_j$$

e λ_2 si troverebbe in (G_μ).

(1) Siccome uno dei numeri r_1, r_2, r_{p-1} è $\equiv 1 \bmod p$, ne viene che almeno uno dei resti delle potenze r^{ν} sarà l'unità.

Se (1), (2) non esauriscono (G), sia λ_3 un suo nuovo termine non compreso in (1), (2).

Come prima si prova che il sistema:

$$\lambda_3,\ \lambda_3\rho_1,\ \lambda_3\rho_2,\ \ldots\ \lambda_3\rho_{\mu-1} \tag{3}$$

è costituito da elementi tutti tra loro diversi e nessuno dei quali appartiene ad (1) o (2). Se (G) non è completato da (1), (2), (3), esisterà in esso in più un nuovo elemento λ_4, e così procedendo si trova che (G) si può scomporre come segue:

$$(G)\quad \left\{\begin{array}{l} 1,\ \rho_1,\ \rho_2,\ \ldots\ \rho_{\mu-1} \\ \lambda_1,\ \lambda_1\rho_1,\ \lambda_1\rho_2,\ \ldots\ \lambda_1\rho_{\mu-1} \\ \ldots\ldots\ldots\ldots\ldots \\ \lambda_{q-1},\ \lambda_{q-1}\rho_1,\ \lambda_{q-1}\rho_2,\ \ldots\ \lambda_{q-1}\rho_{\mu-1} \end{array}\right.$$

da cui risulta in primo luogo

$$p-1=\mu\cdot q$$

cioè che « l'ordine μ di un sottogruppo (G_μ) di (G) è un divisore dell'ordine $(p-1)$ di G » [1].

§ 12. **Numero dei resti delle potenze simili degli elementi del sistema ridotto di residui.** — Dalla precedente scomposizione di (G) risulta manifestamente:

$$\sum_1^{p-1} r_i \equiv \Sigma\rho_h\cdot\Sigma\lambda_k.$$

Ora $\Sigma\lambda_k = 1+\lambda_2+\ldots+\lambda_{q-1}$, in generale non è nullo mod p: infatti, se fosse tale per un particolare sistema dei λ, lasciando fissi $1, \lambda_1, \lambda_2, \ldots \lambda_{q-2}$ e mutando λ_{q-1} in λ'_{q-1} il qual ultimo, dopo scelti i primi $q-1$ elementi λ, si può prendere arbitrariamente in μ modi diversi, deve risultare

$$1+\lambda_2+\lambda_3+\ldots+\lambda_{q-2}+\lambda'_{q-1}\not\equiv 0$$

poichè, nel caso contrario, λ'_{q-1} non potrebbe esser distinto da λ_{q-1}.

Non potendo quindi essere in generale $\Sigma\lambda\equiv 0$, dovrà esser certamente:

$$\Sigma\rho\equiv 0.$$

[1] Questo importante *Teorema* che si dimostra nello stesso modo anche per gruppi, in generale, di operazioni, è attribuito a LAGRANGE.

Sieno ora:

$$(G_h) \qquad r_1 \equiv 1, \quad r_2, \quad r_3, \ldots \quad r_h$$

quelli degli elementi di (G) le cui potenze di grado ν sono congrue all'unità. Dalle:

$$(r_i)^\nu \equiv 1$$
$$(r_j)^\nu \equiv 1$$

si ricava:

$$(r_i \cdot r_j)^\nu = 1$$

cioè il prodotto $r_i \cdot r_j$ appartiene a (G_h) che viene così ad essere un sottogruppo di G.

Procedendo come prima possiamo scomporre (G) mediante il sottogruppo (G_h) nel quadro seguente:

$$(G) \qquad \left\{ \begin{array}{llll} r_1 = 1 & r_2 & \ldots & r_h \\ \sigma_1 & \sigma_1 r_2 & \ldots & \sigma_1 r_h \\ \ldots & \ldots & \ldots & \ldots \\ \sigma_{k-1} & \sigma_{k-1} r_2 & \ldots & \sigma_{k-1} r_h \end{array} \right.$$

Le potenze di grado ν degli elementi della prima linea sono $\equiv 1 \bmod p$, quelle della seconda a $\sigma_1{}^\nu$ e così di seguito: nè le potenze di due termini in orizzontali diverse possono esser $\equiv \bmod p$.

Ammesso infatti:

$$\sigma_i{}^\nu \equiv \sigma_j{}^\nu$$

potendosi sempre porre:

$$\sigma_j \equiv \sigma_i \cdot r$$

dove r è in (G), se ne ricaverebbe:

$$\sigma_i{}^\nu \cdot r^\nu \equiv \sigma_i{}^\nu$$

da cui

$$r^\nu \equiv 1$$

ed r apparterebbe a (G_h) e quindi

$$\sigma_j \equiv \sigma_i \cdot r_\mu$$

contrariamente al procedimento seguito nella costruzione del quadro precedente. Le potenze:

$$1, \quad \sigma_1{}^\nu, \quad \sigma_2{}^\nu \ldots \quad \sigma_{k-1}{}^\nu$$

sono tutte diverse $\bmod p$ e coincidono necessariamente con

gli elementi di (G_μ) cioè:

$$r_1^{\nu} \equiv r_2^{\nu} \equiv \ldots\ldots r_h^{\nu} \equiv 1$$

$$\sigma_1^{\nu} \equiv (\sigma_1 r_2)^{\nu} \equiv \ldots\ldots (\sigma_1 r_h)^{\nu} \equiv \sigma_1^{\nu} \equiv \rho_1'$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$(\sigma_{k-1})^{\nu} \equiv (\sigma_{k-1} r_2)^{\nu} \equiv \ldots\ldots \equiv (\sigma_{k-1} r_h)^{\nu} \equiv \rho'_{k-1}$$

dove

$$1 \quad \rho_1' \quad \rho_2' \ldots\ldots \rho_{k-1}'$$

prescindendo dall'ordine, coincidono mod p con

$$1 \quad \rho_1 \quad \rho_2 \ldots\ldots \rho_{\mu-1}$$

per cui $\mu = k$ ed in fine:

$$p - 1 = \mu \cdot h.$$

Inoltre:

$$\sum_{i=1}^{i=p-1} r_i^{\nu} \equiv h \Sigma \rho$$

e poichè:

$$\Sigma \rho \equiv 0$$

è pure:

$$\sum_{1}^{p-1} r_i^{\nu} \equiv 0.$$

Riassumendo quanto è stato dimostrato in questi due paragrafi precedenti, possiamo enunciare il

Teorema. « Il numero μ dei resti differenti che si ottengono dividendo per p le potenze

$$r_1^{\nu} \quad r_2^{\nu} \ldots\ldots \quad r_{p-1}^{\nu}$$

è un divisore di $(p-1)$ e ciascun resto si trova ripetuto lo stesso numero h di volte. Di più:

$$\Sigma r^{\nu} \equiv \Sigma \rho \equiv 0.$$

Osservazione. « Se ν è eguale o multiplo a $(p-1)$, segue dal *Teorema* di FERMAT che i resti sono tutti eguali all'unità e quindi $\mu = 1$, $h = p - 1$ ».

§ 13. **Numero delle radici di una congruenza binomia $x^{\nu} \equiv 1 \bmod p$.** — Consideriamo ora la congruenza

(1) $$x^{\nu} \equiv 1$$

e supponiamo da prima ν divisore di $(p-1)$.

Avremo identicamente:

$$x^{p-1} - 1 \equiv (x^\nu - 1) \cdot f(x)$$

dove $f(x)$ è di grado $(p-1) - \nu$.

Poichè

$$x^{p-1} - 1 \equiv 0$$

ammette $(p-1)$ radici distinte, anche

$$(x^\nu - 1) f(x) \equiv 0$$

ne ammetterà altrettante distribuite tra le

$$x^\nu - 1 \equiv 0; \quad f(x) \equiv 0.$$

Ma $x^\nu - 1 \equiv 0$ non può avere più di ν radici, e se ne avesse un numero minore, la $f(x) \equiv 0$ dovrebbe averne più di quello che consenta il suo grado, per cui la (1) ne avrà effettivamente ν.

Posto ora che ν non divida $p-1$, sieno

$$\alpha_1 = 1, \quad \alpha_2, \ldots \quad \alpha_\delta \tag{2}$$

le sue radici una delle quali, α_1, esisterà in ogni caso; ed indichiamo con ν_1 il più piccolo esponente per cui:

$$\alpha_1^{\nu_1} \equiv \alpha_2^{\nu_1} \equiv \ldots \equiv \alpha_\delta^{\nu_1} \equiv 1.$$

In primo luogo ν_1 dev'essere divisore di ν: poichè, ove non lo fosse, detto r il resto della loro divisione, da:

$$x^\nu - 1 \equiv x^{q \cdot \nu_1} \cdot x^r - 1 \equiv 0$$

si ricaverebbe:

$$\alpha_1^r \equiv \alpha_2^r \equiv \ldots \alpha_\delta^r \equiv 1$$

contro l'ipotesi poichè $r < \nu_1$.

Stabilito così che ν_1 deve dividere ν, si deduce che, oltre agli elementi (2), non ve ne sono altri le cui potenze di grado ν_1 sieno $\equiv 1$, poichè se ve ne fossero, per questi pure le potenze di grado ν dovrebbero a maggior ragione esser $\equiv 1$, mentre i soli dotati di questa proprietà sono i numeri (2).

Con lo stesso procedimento si constata che ν_1 deve divi-

dere $(p-1)$, e poichè in questo caso, da quanto precede, risulta che la:

$$x^{\nu_1} \equiv 1 \tag{3}$$

possiede effettivamente ν_1 radici, si conclude che le radici di (1) coincidono con quelle di (3) ed è $\delta = \nu_1$.

Siccome poi, posto $\delta_1 = D((p-1), \nu)$, segue immediatamente che la (1) possiede tutte le δ_1 radici di:

$$x^{\delta_1} \equiv 1$$

sarà $\delta_1 \leq \delta$; e poichè δ_1, δ sono entrambi divisori comuni di $(p-1)$ e ν

$$\delta_1 = \delta$$

Teorema. « Una congruenza binomia

$$x^{\nu} \equiv 1$$

ammette $\delta = D(p-1, \nu)$ radici distinte ed è equivalente alla:

$$x^{\delta} \equiv 1 \text{ ».}$$

Osservazione. « Se $\delta = 1$, la radice è unica e si riduce all'elemento 1 ».

§ 14. **Equivalenza del sistema delle radici di una congruenza binomia, con quello dei resti delle potenze simili di un sistema ridotto di residui.** -- Consideriamo ora i resti delle potenze:

$$r_1^{\frac{p-1}{\delta}}, \quad r_2^{\frac{p-1}{\delta}} \ldots\ldots \quad r_{p-1}^{\frac{p-1}{\delta}} \tag{1}$$

dove $\frac{p-1}{\delta}$ è pure divisore di $(p-1)$ al pari di δ.

Poichè la:

$$x^{\frac{p-1}{\delta}} \equiv 1$$

per quanto precede possiede $\frac{p-1}{\delta}$ radici distinte, tra i numeri (1) ve ne saranno $\frac{p-1}{\delta}$ congrui all'unità e pel *Teorema* al § 13 segue che i diversi resti saranno quindi in numero di δ.

Detto ρ uno qualunque di essi, esisterà in (1) una potenza tale che sia:

$$r_i^{\frac{p-1}{\delta}} \equiv \rho$$

e quindi innalzando a δ:

$$r_i^{p-1} \equiv \rho^{\delta}$$

e poichè

$$r_i^{p-1} \equiv 1$$

si avrà pure:

$$\rho^{\delta} \equiv 1$$

Teorema. « Se δ è divisore di $p-1$ il sistema delle radici di $x^{\delta} \equiv 1$, coincide con quello dei residui delle potenze:

$$r_1^{\frac{p-1}{\delta}} \quad r_2^{\frac{p-1}{\delta}} \ldots\ldots \quad r_{p-1}^{\frac{p-1}{\delta}} \text{ ».}$$

Osservazione. « Da quanto precede risulta immediatamente che la determinazione di un sistema di residui corrisponde a quella delle radici di una congruenza binomia, e che tutte le proprietà che competono al primo, valgono anche per le seconde.

Così per es. anche le radici di una congruenza binomia costituiscono un gruppo ».

§ 15. **Residui quadratici. - Ogni numero primo divide una somma di due o tre quadrati secondochè è della forma $4k+1$ o $4k-1$. - Ogni numero intero è somma di quattro quadrati.** — Passiamo ora ad applicare i precedenti risultati alla dimostrazione di un *Teorema* che è uno dei più interessanti della *Teoria dei numeri.*

Abbiamo già stabilito che se δ è divisore di $(p-1)$, tra i resti delle potenze:

$$r_1^{\delta}, \quad r_2^{\delta}, \ldots\ldots \quad r_{p-1}^{\delta}$$

ve ne sono $\dfrac{p-1}{\delta}$ tra loro diversi e che ciascuno si trova ripetuto δ volte.

Tali resti, tra i quali figura certamente l'unità, e che indicheremo con:

(1) $$\rho_1 = 1, \quad \rho_2, \quad \rho_3, \ldots\ldots \quad \rho_{\frac{p-1}{\delta}}$$

coincidono con le radici di

$$x^{\frac{p-1}{\delta}} \equiv 1.$$

Per $\delta = 2$, i numeri (1) (e quindi tutti quelli congrui ad essi mod p) si chiamano *residui-quadratici;* e *non-residui* i rimanenti.

Dall'identità:

$$x^{p-1} - 1 \equiv \left(x^{\frac{p-1}{2}} - 1\right)\left(x^{\frac{p-1}{2}} + 1\right)$$

risulta che, poichè la congruenza:

$$\left(x^{\frac{p-1}{2}} - 1\right)\left(x^{\frac{p-1}{2}} + 1\right) \equiv 0$$

ammette $(p-1)$ radici e di queste $\frac{p-1}{2}$ competono alla

$$x^{\frac{p-1}{2}} - 1 \equiv 0 \tag{2}$$

le rimanenti soddisferanno la

$$x^{\frac{p-1}{2}} + 1 \equiv 0. \tag{3}$$

Siccome le radici di (2) sono date dai numeri (1) per $\delta = 2$ [1], cioè dei residui quadratici, segue che quelle della (3) coincideranno con i non-residui, e quindi « condizione necessaria e sufficiente perchè α sia residuo-quadratico è che si abbia:

$$\alpha^{\frac{p-1}{2}} \equiv 1.$$

E perchè sia un non-residuo:

$$\alpha^{\frac{p-1}{2}} \equiv -1.$$

Ciò premesso, posto $q = \frac{p-1}{2}$, sieno

$$\alpha_1^{\,2} \quad \alpha_2^{\,2} \ldots \quad \alpha_q^{\,2} \tag{4}$$

[1] Se infatti ρ è un residuo quadratico sarà $\rho \equiv r^2$ e quindi

$$\rho^{\frac{p-1}{2}} \equiv r^{p-1} \equiv 1.$$

i q elementi di:

$$r_1^2 \quad r_2^2 \ldots\ldots \quad r_{p-1}^2$$

congrui rispettivamente ai q residui quadratici

$$\rho_1 = 1, \quad \rho_2, \quad \rho_3, \ldots\ldots \quad \rho_q \tag{5}$$

ed essi pure residui, e consideriamo il prodotto:

$$(x^2 + \alpha_1^2)(x^2 + \alpha_2^2) \ldots\ldots (x^2 + \alpha_q^2).$$

Essendo i numeri (4) congrui alle radici (5) di (2), dall'identità:

$$x^{\frac{p-1}{2}} - 1 \equiv (x - \alpha_1^2)(x - \alpha_2^2) \ldots\ldots (x - \alpha_q^2)$$

si deduce (§ 10) che per le funzioni simmetriche elementari dei numeri α^2 sussisteranno le relazioni:

$$\Sigma \alpha_i^2 \equiv \Sigma \alpha_i^2 \alpha_j^2 \equiv \ldots\ldots \equiv \Sigma \alpha_i^2 \alpha_j^2 \cdot \alpha_h^2 \equiv 0$$

$$\alpha_1^2 \alpha_2^2 \ldots\ldots \alpha_q^2 \equiv (-1)^{q-1} \equiv \rho_i \rho_2 \ldots\ldots \rho_q$$

per cui si avrà identicamente:

$$(x^2 + \alpha_1^2)(x^2 + \alpha_2^2) \ldots\ldots (x^2 + \alpha_q^2) \equiv x^{p-1} + (-1)^{q-1}. \tag{6}$$

Distinguiamo ora i due seguenti casi.

a) $p = 4k + 1$.

In questa ipotesi essendo q pari e $q - 1$ dispari, la (6) si riduce a:

$$(x^2 + \alpha_1^2)(x^2 + \alpha_2^2) \ldots\ldots (x^2 + \alpha_q^2) \equiv x^{p-1} - 1 \equiv 0$$

e dovendo il prodotto nel primo membro risultare multiplo di p per $x = 1, 2, \ldots\ldots (p - 1)$, ne segue che per qualunque valore di x uno dei fattori (ed uno solo poichè sempre incongrui) dovrà esser divisibile per p.

« Per ogni valore di x esiste una coppia di quadrati x^2, α^2 la cui somma è multipla di p ».

b) $p = 4k - 1$.

In questo caso $q = \dfrac{4k - 2}{2} = 2k - 1$ è dispari e $(q - 1)$ pari, per cui la (6) diventa:

$$(x^2 + \alpha_1^2)(x^2 + \alpha_2^2) \ldots\ldots (x^2 + \alpha_q^2) \equiv 2$$

e nessuno dei fattori del primo membro potrà esser divisibile per p.

Dimostriamo ora che non possono esser tutti congrui a residui, o tutti a non residui.

Dalla prima ipotesi si avrebbe infatti:

$$(x^2 + \alpha_1^2) \dots (x^2 + \alpha_q^2) \equiv \rho_1 \rho_2 \dots \rho_q \equiv 1$$

la quale non può sussistere perchè palesemente in contraddizione con quella che precede.

D'altra parte, non può darsi che i precedenti fattori coincidano mod p con il sistema dei non residui.

Ed invero, poichè $\frac{p-1}{2}$ è dispari, se α è residuo e quindi radice di

$$x^{\frac{p-1}{2}} \equiv 1$$

$(-\alpha)$ lo è di

$$x^{\frac{p-1}{2}} \equiv -1$$

cioè α e $(-\alpha)$ hanno carattere quadratico opposto, e se uno è residuo l'altro non lo è. Segue che se:

$$\rho_1 \quad \rho_2 \dots \quad \rho_q$$

è il sistema dei residui, quello dei non residui è dato da:

$$(-\rho_1), \quad (-\rho_2), \dots \quad (-\rho_q).$$

Se ora i fattori $(x^2 + \alpha^2)$ fossero tutti congrui a non-residui, ne verrebbe:

$$(x^2 + \alpha_1^2) \dots (x^2 + \alpha_q^2) \equiv (-1)^q \cdot \rho_1 \rho_2 \dots \rho_q$$

e poichè per q dispari:

$$\rho_1 \rho_2 \dots \rho_q \equiv \alpha_1^2 \alpha_2^2 \dots \alpha_q^2 \equiv 1$$

si giungerebbe alla congruenza

$$x^{p-1} + 1 \equiv -1$$

e poichè

$$x^{p-1} \equiv 1$$

dovrebbe essere in fine:

$$3 \equiv 0$$

la quale è possibile solo per $p = 3$.

Dal momento che i binomii $(x^2 + \alpha^2)$ non possono esser tutti resti, nè tutti non resti, uno almeno di essi, qualunque sia x, sarà congruo ad un non-residuo, cioè:

$$x^2 + \alpha_i^2 \equiv -\alpha_j^2$$
$$x^2 + \alpha_i^2 + \alpha_j^2 \equiv 0.$$

Concludiamo quindi che per ogni numero primo della forma $4k - 1 > 3$, corrisponde ad ogni valore di x non multiplo di p, una terna, almeno, di quadrati la cui somma è multipla di p. Per $p = 3$, si ha evidentemente:

$$3 = 1^2 + 1^2 + 1^2.$$

Da questi fatti e dal *Teorema* al § 10 del Cap. II viene il *Corollario.* « Ogni numero primo è somma di quattro quadrati, due almeno dei quali diversi da zero ».

Infatti di ogni numero primo, compresi il 2 ed il 3, si può affermare che divide la somma di due o tre quadrati tutti diversi da zero e quindi esso pure sarà somma di quattro quadrati due dei quali, almeno, non nulli.

Teorema. « Ogni numero intero è somma di quattro quadrati, dei quali non più di due nulli ».

Infatti, ogni numero intero si scinde nel prodotto di fattori primi, ed in forza del *Corollario* precedente, applicando reiteratamente l'identità Euleriana (Cap. II, § 10) si perviene sempre a dimostrare la proposizione.

Osservazione. Questo celebre *Teorema* forse già noto a DIOFANTO, è stato enunciato da BACHET DI MÉZIRIAC e dimostrato per primo da LAGRANGE.

Esso però rientra in un *Teorema* molto più generale scoperto da FERMAT e dimostrato e completato da CAUCHY e LEGENDRE secondo cui, detto « numero poligonale ad r lati » un numero $P_n^{(r)}$ della forma:

$$P_n^{(r)} = n + \frac{(n-1)}{2}(r-2)$$

ogni numero intero risulta come somma di r numeri poligonali ad r lati. Per $r = 4$ si ha:

$$P_n^{(4)} = n^2.$$

Notiamo pure che negli autori citati SERRET, LE BESGUE, HUMBERT, il *Teorema* di BACHET viene dedotto dalla proposizione che « se $p = 4k + 1$, esiste sempre un intero a per cui

$$a^2 + 1 \equiv 0 \mod p$$

e se $p = 4k - 1$, ne esiste una coppia a, b tale che:

$$a^2 + b^2 + 1 \equiv 0 \mod p \text{ »}$$

che è un caso particolare di quella data più sopra.

§ 16. **Periodo di un elemento di un sistema di residui. - Radici primitive di una congruenza binomia e loro numero.** — Sia a uno qualunque dei numeri

$$1, \quad 2, \ldots \quad (p-1)$$

e consideriamo la serie di potenze:

$$a, \quad a^2, \quad a^3, \ldots \quad a^{p-1}$$

l'ultima delle quali congrua all'unità mod p.

Il più piccolo esponente n (diverso da zero) per cui si abbia:

$$a^n \equiv 1$$

dicesi « *l'esponente a cui appartiene* a, *ovvero il periodo di* a *mod* p.

Si dice pure che a è *radice primitiva* di

$$x^n \equiv 1$$

ed in particolare, qualora sia $n = p - 1$, a dicesi *radice primitiva* del numero primo p.

Lemma 1°. « Se a appartiene all'esponente n ed è pure

$$a^m \equiv 1$$

sarà m multiplo di n ».

Ammesso infatti che ciò non sia, si avrà:

$$m = n \cdot q + r; \quad r < n$$

e quindi

$$a^m \equiv (a^n)^q \cdot a^r.$$

Ma per ipotesi $a^m \equiv a^n \equiv 1$, e ne segue $a^r \equiv 1$, contro quanto si era supposto che n fosse il più piccolo intero non nullo per cui $a^n \equiv 1$. Sarà quindi $r = 0$.

Da ciò segue che, essendo sempre pel *Teorema* di FERMAT $a^{p-1} \equiv 1$, sarà $(p-1)$ multiplo di n.

Lemma 2°. « Se a appartiene ad n, a^m ha per periodo $(m:\delta)$ essendo $\delta = D(m, n)$ ».

Sia m' l'esponente di a^m: essendo allora $a^{m \cdot m'} \equiv 1$, sarà (*Lemma 1°*) $m \cdot m'$ multiplo di n.

Ponendo $m = \delta \cdot \mu$; $n = \delta \cdot \nu$ ne risulterà che $\delta \cdot \mu \cdot m' = m \cdot m'$ sarà divisibile per $n = \delta \cdot \nu$, cioè $\mu \cdot m'$ divisibile per ν; ed essendo μ, ν primi tra loro, ne segue che m' dev'essere multiplo di ν.

Poichè dall'ipotesi $a^{m \cdot m'} \equiv 1$ discende che m' è multiplo di ν e reciprocamente, si conclude che $\nu = (n:\delta)$ è il più piccolo esponente per cui si abbia:

$$a^{m \cdot \nu} \equiv 1$$

cioè che esso è l'esponente o periodo di a^m.

Se $\delta = 1$, si ha $\nu = n$, ed a^m appartiene pure ad n; per cui, sempre nell'ipotesi che a appartenga ad n, tra le potenze:

$$a, \quad a^2, \quad a^3 \ldots \quad a^{(n-1)}$$

ve ne saranno $\varphi(n)$ dotate dello stesso periodo n.

Corollario. « Se a appartiene ad n, tra le potenze a, a^2, $a^3 \ldots a^n$, una almeno appartiene all'esponente d divisore di n ».

Infatti (*Lemma 2°*) $a^{\frac{n}{d}}$ ha per periodo:

$$n : \left(\frac{n}{d}\right) = d.$$

Lemma 3°. « Se a_1, a_2 appartengono rispettivamente agli esponenti n_1, n_2, il prodotto $a_1 \cdot a_2$ appartiene ad $n_1 \cdot n_2$ qualora n_1, n_2 sieno primi tra loro ».

Essendo intanto per ipotesi

$$(a_1 a_2)^{n_1 \cdot n_2} \equiv 1$$

per il *Lemma 1°*, $a_1 \cdot a_2$ avrà per periodo $n_1 n_2$ od un suo divisore che, com'è lecito, supporemo scomposto nel prodotto $n_1' \cdot n_2'$ essendo n_1' divisore di n_1, ed n_2' di n_2.

Avremo intanto nella seconda ipotesi:

$$(a_1 a_2)^{n_1' \cdot n_2'} = a_1^{n_1' \cdot n_2'} \cdot a_2^{n_1' \cdot n_2'} \equiv 1$$

e ponendo $n_1 : n_1' = q$ ed innalzando a q:

$$a_1^{q n_1' n_2'} \cdot a_2^{q n_1' n_2'} \equiv 1$$

ed essendo per ipotesi $a_1^{n_1} \equiv 1$, si avrà:

$$a_2^{n_1 n_2'} \equiv 1$$

ed appartenendo a_2 ad n_2 primo con n_1 e dovendo essere pel *Lemma 1°* $n_1 \cdot n_2'$ multiplo di n_2, sarà $n_2' = n_2$. Avremo allora:

$$a_1^{n_1' \cdot n_2} \cdot a_2^{n_1' \cdot n_2} \equiv 1$$

ed essendo $a_2^{n_2} \equiv 1$, sarà pure:

$$a_1^{n_1' \cdot n_2} \equiv 1$$

da cui si ricava come prima $n_1' \equiv n_1$.

Osservazione. Se n_1, n_2 non sono primi tra loro e se ne indica con δ il m. c. d. sarà evidentemente:

$$(a_1 \cdot a_2)^{\frac{n_1 \cdot n_2}{\delta}} = a_1^{n_1 \frac{n_2}{\delta}} \cdot a_2^{n_2 \frac{n_1}{\delta}} \equiv 1$$

ma non si può asserire in generale che $a_1 \cdot a_2$ abbia per periodo $\frac{n_1 \cdot n_2}{\delta}$ ».

Corollario. Se a_1, $a_2 \ldots a_r$ hanno per periodi $n_1, n_2, \ldots n_r$ primi tra loro due a due, il prodotto $a_1 \cdot a_2 \ldots a_r$ appartiene all'esponente $n_1 \cdot n_2 \ldots n_r$ ».

Lemma 4°. « Se le radici $r_1 r_2 \ldots r_\delta$ di $x^\delta \equiv 1$ appartengono rispettivamente agli esponenti $n_1, n_2, \ldots n_\delta$, uno di questi sarà il m. m. c. di $n_1, n_2, \ldots n_\delta$ ».

Sia infatti $m = p_1^{\lambda_1} \cdot p_2^{\lambda_2} \ldots$ questo m. c. m. scomposto nei suoi fattori primi: segue che $p_1^{\lambda_1}$, $p_2^{\lambda_2} \ldots$, compariranno come divisore in qualcuno dei numeri n.

Supponiamo che $p_1^{\lambda_1}$ si trovi in n_1. Allora poichè r_1 appartiene ad n_1 pel *Corollario* del *Lemma 2°* una delle potenze di r_1 congrua evidentemente ad un'altra delle radici in questione, apparterà a $p_1^{\lambda_1}$: sia questa r_1'. Similmente si troverà una radice r_2' e così di seguito.

Ma $p_1^{\lambda_1}$, $p_2^{\lambda_2} \ldots$ sono primi tra loro due a due per cui, in virtù del precedente *Corollario*, il prodotto $r_1' \cdot r_2' \ldots$ che, per essere

$$(r_1' \cdot r_2' \ldots)^\delta \equiv (r_1') \cdot (r_2')^\delta \ldots \equiv 1$$

è pure radice di $x^\delta \equiv 1$, apparterrà all'esponente $p_1^{\lambda_1} \cdot p_2^{\lambda_2} \ldots$. Una radice di $x^\delta \equiv 1$ ha quindi per periodo m, cioè m si trova tra i numeri $n_1, n_2, \ldots n_\delta$.

Dopo ciò possiamo dimostrare il seguente

Teorema. « Tra le radici di $x^\delta \equiv 1$ dove δ è divisore di $p-1$, ve ne sono $\varphi(\delta)$ appartenenti all'esponente δ, cioè *primitive* ».

Sieno $n_1, n_2, \ldots, n_\delta$ gli esponenti cui appartengono le radici: tra di essi (*Lemma 4°*) ve ne sarà uno che indicheremo con m e che sarà il loro m. c. m.

Avremo allora:

$$r_1^m \equiv r_2^m \ldots \equiv r_\delta^m \equiv 1.$$

Ma m non può essere $< \delta$ poichè allora la $x^m \equiv 1$ ammetterebbe un numero δ di radici superiore al suo grado m, e siccome è già per ipotesi:

$$r_1^\delta \equiv r_2^\delta \equiv \ldots \equiv r_\delta^\delta \equiv 1$$

m non può essere maggiore di δ e si conclude quindi che $m = \delta$.

Fra le radici di $x^\delta \equiv 1$ ne esiste quindi una appartenente a δ e che indicheremo con g. Le potenze:

$$(1) \qquad g, \quad g^2, \ldots \quad g^\delta$$

sono tutte tra loro incongrue mod p: invero, ammesso che fosse:

$$g^\lambda \equiv g^\mu \quad \lambda > \mu$$

ne seguirebbe $g^{\lambda-\mu} \equiv 1$ e quindi essendo λ, μ due numeri qualunque delle serie

$$1, \quad 2, \ldots \quad \delta$$

si concluderebbe che g apparterebbe ad un esponente $< \delta$ contro l'ipotesi.

Oltre a ciò le potenze (1) sono altrettante radici di $x^\delta \equiv 1$ poichè:

$$(g^\lambda)^\delta \equiv (g^\delta)^\lambda \equiv 1$$

qualunque sia λ, e quindi il sistema (1) coincide con quello delle radici di $x^\delta \equiv 1$.

Ma (*Lemma 2°*) tutte quelle potenze di g il cui esponente è primo con δ hanno per periodo δ, per cui resta dimostrato che il numero delle radici primitive di $x^\delta \equiv 1$ è dato da $\varphi(\delta)$.

Da quanto precede risulta poi che la soluzione di una congruenza $x^\delta \equiv 1$, sta tutta nella determinazione di una sua radice primitiva qualsiasi, poichè le sue successive potenze ci somministreranno indistintamente tutte le altre.

§ 17. **Radici primitive di un numero primo.** — Nella Teoria dei numeri hanno grande importanza le radici primitive della congruenza $x^{p-1} \equiv 1$ che si dicono anche *radici primitive del numero primo* p.

Per la determinazione di tali radici non si conosce algoritmo ben determinato, ma vennero suggeriti due metodi uno dei quali si potrebbe dire di *successive eliminazioni* e l'altro di *successive approssimazioni.*

Daremo un esempio del primo [1]. Sia da determinarsi una radice primitiva di 19. Si scrivano in linea i numeri naturali dall'1 al 18 e sotto in un altra linea i loro residui quadratici che si calcoleranno facilmente tenendo conto che due numeri complementari rispetto al modulo danno lo stesso residuo.

1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18
1, 4, 9, 16, 6, 17, 11, 7, 5, 5, 7, 11, 17, 6, 16, 9, 4, 1.

Intanto i numeri 1, 18 come radici di $x^2 \equiv 1$ sono da eliminarsi e così pure i numeri

$$4,\ 9,\ 16,\ 6,\ 17,\ 11,\ 5$$

che, come residui quadratici, soddisfano la:

$$x^{\frac{18}{2}} \equiv 1.$$

Rimangono così i termini:

$$2,\ 3,\ 8,\ 10,\ 12,\ 13,\ 14,\ 15$$

e determiniamone i loro residui cubici moltiplicandoli pei loro

[1] SERRET. *Algèbre Supérieure.* Sezione 3ª, § 813.

resti quadratici. Essi sono:

$$8,\ 8,\ 18,\ 12,\ 18,\ 12,\ 8,\ 12.$$

I residui cubici 8, 12 sono da eliminarsi come radici di

$$x^{\frac{18}{3}} \equiv 1$$

per cui rimangono i numeri

$$2,\ 3,\ 10,\ 13,\ 14,\ 15$$

che essendo in numero di $\varphi(18) = 6$, ci daranno le radici primitive richieste.

Infatti essi sono congrui, benchè in altro ordine ai resti delle potenze:

$$2,\ 2^5,\ 2^7,\ 2^{11},\ 2^{13},\ 2^{17}$$

essendo 1, 5, 7, 11, 13, 17 i numeri inferiori a 18 e primi con esso.

§ 18. **Indice di un residuo rispetto ad una radice primitiva. - Teoremi fondamentali e loro uso nella risoluzione di una congruenza binomia generale.** — Sia g una radice primitiva qualunque del numero primo p: per quanto si è dimostrato i numeri:

$$g^1,\ g^2,\ldots.\ g^{p-1}$$

sono congrui mod p benchè in altro ordine ai numeri:

$$1,\ 2,\ 3,\ldots.\ (p-1).$$

Segue che se n è un intero qualunque non multiplo di p, si potrà sempre determinare uno ed un solo esponente $\lambda < p$ pel quale si abbia

$$n \equiv g^\lambda.$$

All'esponente λ si dà il nome di *indice* del numero n rispetto alla base g e si scrive:

$$\lambda = (\text{ind}\ n)_g$$

omettendo l'indicazione della base g qualora non vi sia a temere equivoco.

Osserviamo, intanto, che tutti i numeri n congrui tra loro mod p, ammettono manifestamente lo stesso indice.

Oltre a ciò, se $\lambda' = \lambda + k(p-1)$ si ha:

$$g^{\lambda'} = g^{\lambda} \cdot g^{k(p-1)}$$

e poichè $g^{p-1} \equiv 1$, si ottiene:

$$g^{\lambda'} \equiv g^{\lambda}$$

per cui possiamo considerare come indice di n, qualunque numero λ' congruo a $\lambda \bmod (p-1)$.

Ciò premesso, essendo pel *Teorema* di FERMAT:

$$g^{p-1} - 1 = \left(g^{\frac{p-1}{2}} - 1\right)\left(g^{\frac{p-1}{2}} + 1\right) \equiv 0$$

uno dei due fattori del 2° membro dovrà esser divisibile per p, e non potendo essere

$$g^{\frac{p-1}{2}} - 1 \equiv 0$$

poichè ciò contraddice all'ipotesi di g radice primitiva, sarà:

$$g^{\frac{p-1}{2}} + 1 \equiv 0$$

cioè:

$$\frac{p-1}{2} = \text{ind}\,(-1).$$

Qualunque sia la base g, i numeri $1, (-1)$ hanno costantemente per indici $(p-1)$ e $\frac{p-1}{2}$.

Un sistema di indici relativamente ad una data base, gode di proprietà del tutto analoghe a quelle dei logaritmi come lo provano le seguenti proposizioni.

Teorema 1°. « L'indice di un prodotto è congruo mod $(p-1)$ alla somma degli indici dei singoli fattori ».

Sieno λ, λ' gli indici di a, a'.

Per definizione sarà:

$$a \equiv g^{\lambda}$$

$$a' \equiv g^{\lambda'}$$

e quindi:

$$a \cdot a' \equiv g^{\lambda+\lambda'}$$

cioè:

$$\lambda + \lambda' \equiv \text{ind}\, a \cdot a' \qquad \bmod (p-1).$$

Teorema 2°. « L'indice di una potenza è congruo mod $(p-1)$ al prodotto dell'esponente per l'indice della base ».

Sia λ l'indice della base di a, per cui:

$$a \equiv g^{\lambda} \mod p$$

e quindi:

$$a^n \equiv g^{n\lambda} \mod p$$

cioè:

$$n\lambda = n \cdot (\text{ind } a) \equiv \text{ind } a^n \mod (p-1).$$

Questi due *Teoremi* si applicano alla risoluzione delle congruenze binomie generali come per es. la:

$$x^n \equiv a \mod p. \tag{1}$$

Sia η infatti una radice di (1): sarà:

$$\eta^n \equiv a \mod p$$

e prendendo gli indici dei due membri:

$$n \cdot \text{ind } \eta \equiv \text{ind } a \mod (p-1)$$

per cui se η è radice di (1), il minimo valore positivo di ind η sarà radice di

$$n \cdot x \equiv \text{ind } a \mod (p-1). \tag{2}$$

Inversamente da una radice di (2) se ne ricava una per la (1), per cui la soluzione di (1) si può far dipendere dalla (2) purchè si disponga di una tavola di indici a base g radice primitiva di p.

Da tale specie di equivalenza tra le (1) (2) si scorge che lo studio della congruenza binomia di grado n mod p, si può far dipendere da quello di una congruenza di 1° grado mod $(p-1)$.

Infatti la condizione necessaria e sufficiente per la risolubilità di (1) ed il numero delle radici che può ammettere si possono ricavare facilmente dalla (2) fondandosi sui risultati del § 8.