PREMESSA. Questo capitolo non fa parte delle antiche dispense del 1969, delle quali abbiamo messo in rete i CAP. 0. I, II. L'argomento fu trattato come Tesi di Laurea , dalla allora laureanda Maria Antonietta Garzia, sotto la guida del Prof. Franco Eugeni che ne fu relatore. Maria Antonietta Garzia, circa un paio d'anni dopo la Laurea, divenne professore di ruolo di Matematica e Fisica nei Licei, dove ha portato avanti il suo ruolo di educatrice e fisico-matematica, collaborando anche, come Docente, nei Master per gli Insegnanti con l'Università di Teramo. Successivamente la Tesi fu adattata come Capitolo III, ed inserita nelle dispense del 1972-73.
Data la complessità del Capitolo abbiamo inserito un indice.

CAPITOLO III

LA TEORIA DELLA DIVISIBILITA' NELL'ANELLO DEGLI INTERI RELATIVI

INDICE

INTRODUZIONE

Per illustrare esaurientemente la divisibilità nell'anello Z, abbiamo bisogno di definizioni e simbologia che utilizzeremo nell'esposizione teorica, storica e didattica. Richiameremo brevemente l'attenzione inoltre su alcuni teoremi e concetti fondamentali per la costruzione e la definizione delle proprietà assiomatiche dell'insieme dei numeri naturali mentre altri verranno dati per scontati nella trattazione teorica e per acquisiti dai discenti nella impostazione didattica dell'argomento.

Indichiamo con N_0, N_1, N_2, rispettivamente l'insieme induttivo minimale secondo gli assiomi di Peano che ha come minimo l'elemento 0, 1, 2: $N_0=\{0, 1, 2, \ldots\}$,

$N_1=\{1, 2, 3, \ldots\}$, $N_2=\{2, 3, 4, \ldots\}$. È ben noto che l'assiomatica di Peano definisce le successioni di primo termine fissato, è la critica di Russel, e quindi per definire una struttura numerica propriamente detta occorre introdurre anche le operazioni. Ci interessa la struttura $(N_1; +, \cdot)$ data dagli assiomi di Giuseppe Peano (Cuneo 1858 – Torino 1932) e dalle operazioni binarie. È chiaro che, per i teoremi del massimo e del minimo, presupponiamo già fissata la relazione d'ordine (che è totale) in N_1 di "$>$". Questa struttura può essere identificata con $(+N_1; +, \cdot)$ (le strutture sono isomorfe), dove abbiamo indicato con $(+N_0, +, \cdot)$, le immersioni naturali di $(N_0, +, \cdot)$nell'anello Z degli interi relativi (indicheremo con Z anche il solo insieme di sostegno di tale anello, ma sarà chiara di volta in volta il significato). Inoltre essendo $(+N_0; +, \cdot)$ identificato con $(N_0; S, P)$, per esso valgono i teoremi del massimo e del minimo, ovvero ogni sottoinsieme non vuoto limitato superiormente ammette massimo ed ogni sottoinsieme non vuoto ammette minimo. Dobbiamo inoltre ricordare che per ogni numero composto di $(+N_2; +, \cdot)$ esiste una scomposizione unica in fattori primi diversi tra loro.

1. TEOREMI di MASSIMO E MINIMO in $\pm N_0$

Effettuata l'identificazione di ***(N_0, S, P)*** con ***$(+N_0, S', P')$*** varie questioni possono essere ancora osservate.

In $(+N_0, S', P')$, essendo identificato con (N_0, S, P) valgono i teoremi relativi al massimo e minimo, cioè : ***ogni sottoinsieme non vuoto, limitato superiormente, ha massimo e ogni sottoinsieme non vuoto, limitato inferiormente, ha minimo.***

In $(+N_2, S', P')$ per ogni numero composto vale il **teorema fondamentale** dell'**Aritmetica**.

La ***divisione con resto*** di $(+N_0, S', P')$ sarà d'ora in poi chiamata ***divisione a resto positivo***.

Il valore assoluto e il valore naturale di un elemento di $\pm N_0$ coincidono ad identificazione avvenuta.

Vogliamo ora estendere le nostre considerazioni allargando i concetti ora richiamati a $\pm N_0$.

Teorema del massimo

Ogni sottoinsieme H non vuoto e limitato superiormente di $\pm N_0$ ha massimo.

Dimostrazione
Il **teorema** è ***ovvio*** se ad ***H appartiene almeno lo zero***.

Se ***H*** è un ***sottoinsieme di interi negativi***, si consideri l'***insieme - H*** degli ***opposti degli elementi di H.***

Tale ***insieme*** ha un ***minimo m***; esso è tale che

$$m \in -H,\ m \leq x \quad \forall\, x \in -H$$

Segue che

$$-m \in H,\ -m \geq -x, \quad \forall\, -x \in -H$$

da cui ***-m è il massimo di H***.

Teorema del minimo

Ogni sottoinsieme H non vuoto e limitato inferiormente di $\pm N_0$ ha minimo.

Dimostrazione
Il teorema è ***ovvio*** se $H \subset +N_0$.
Se ***ad H appartiene qualche negativo***, consideriamo $H' = (-N_0) - H$ cioè

$$H' = \{x :\ x \in -N_0,\ x \notin H\}.$$

H' è ***limitato superiormente dallo 0*** e quindi per il **teorema** *precedente* ha ***massimo M***.
Ora, posto

$$m = M + 1,\ m \notin H'$$

poiché

$$m + 1 > M \quad \text{ed} \quad M \text{ è il massimo di } H',$$

allora

$$m \in H$$

ed ogni altro $m' < m$ è tale che $m' \notin H$, onde ***m è il minimo di H***.

2.-DIVISIBILITA' IN $\pm N_1$.

Diremo che, ***dati $x, y \in \pm N_1$, x divide y e scriviamo:***

$$x \mid y$$

se e solo se $|x| \mid |y|$ in N_1.

Elementi primi in $\pm N_1$.
Un ***elemento $x \in +N_1$*** sarà detto ***primo se e solo se***:

a) $|x| > 1$

b) x è divisibile soltanto per $+1, -1, +x, -x$.

Teorema della fattorizzazione unica in $-N_2$.
Ogni elemento di $-N_2$ può essere scritto in uno ed un solo modo come prodotto di fattori primi positivi e di (- 1) prescindendo dall'ordine di tali fattori.

Dimostrazione. Se $x \in -N_2$ segue che $|x| \in +N_2$, da cui

$$|x| = \prod_{i=1}^{n} p_i$$

essendo p_i ***i fattori primi di $|x|$ in N_0***; poiché $x = (-1) \cdot |x|$ l'***asserto è dimostrato***.

Teorema della divisione con resto positivo. *Comunque dati $x \in |Z|$, $y \in |Z|_0$, esiste una ed una sola coppia (q, r), con $q \in |Z|$ ed $r \in +N_0$, tale che sia:*

$$x = q \cdot y + r \qquad r < |y|.$$

Dimostrazione . Consideriamo $|x| \in +N_0$, $|y| \in +N_1$, ***esiste*** allora un'***unica coppia (q', r')*** con $q' \in +N_0$, $r' \in +N_0$, tale che sia:

$$|x| = q' \cdot |y| + r' \qquad r' < |y|$$

a) Se $x \in +N_0$, $y \in +N_1$,
posto

$$q = q', \; r = r'$$

il ***teorema è dimostrato***.

b) Se $x \in -N_0$ ed $y \in +N_1$,

dalla relazione data, si ha, ***moltiplicando per (- 1)*** :

$$x = - q' \cdot y - r' = - (1 + q') \cdot y + (y - r');$$

onde, posto

$$q = - (1 + q'), \qquad r = y - r',$$

essendo ovvio l'***unicità di tale coppia*** il ***teorema è dimostrato***.

c) Se $x \in +N_0$, $y \in -N_1$,
si ha:

$$x = (- q') \cdot y + r',$$

onde, posto

$$q = - q', \quad r = r'$$

il ***teorema è dimostrato***.

d) Infine, se $x \in -N_0$, $y \in -N_1$,
si ha, ***moltiplicando la relazione data per (- 1)*** :

$$x = q' \cdot y - r' = q' \cdot y + y + (|y| - r') = (q' + 1) \cdot y + (|y| - r'),$$

onde, posto

$$q = q' + 1 \quad \text{e} \quad r = |y| - r'$$

il ***teorema è dimostrato***.

L'***unicità della coppia (q, r)*** è provata globalmente per i quattro casi osservando che se

$$\mathbf{(1)} \quad x = q \cdot y + r = q' \cdot y + r'$$

sono ***due diverse decomposizioni con resto positivo di*** x, e se $r > r'$, allora:

$$r - r' = (q' - q) \cdot y$$

e quindi

$$(q' - q) \cdot y > 0;$$

ne segue che, essendo

$$q' - q \neq 0 \quad \text{ed} \quad y \neq 0 \Rightarrow (q' - q) \cdot y \geq |y|,$$

ma essendo:

$$r < |y| \quad ed \quad r' < |y|$$

si ha:

$$r - r' < |y|$$

per cui la **(1)** è ***assurda***.

<u>Teorema della divisione con resto negativo</u>

Comunque dati $x \in |Z|$, $y \in |Z|_0$, esiste una ed una sola coppia (q, r) con $q \in |Z|$, $r \in - N_0$ tale che sia:

$$x = q \cdot y + r, \qquad |r| < |y|.$$

Dimostrazione. Se $x = q' \cdot y + r'$ *è la* **divisione a resto positivo**, *si ha:*

$$x = (q' + 1) \cdot y + (r' - y)$$

e posto

$$q = q' + 1 \quad \text{ed} \quad r = r' - y$$

il ***teorema è dimostrato***.

Dati inoltre $x, y \in \pm N_1$, chiamiamo:
massimo comune divisore di x ed y l'elemento di $+N_1$ ***massimo comune divisore di*** $|x|$ ***e*** $|y|$***;***

minimo comune multiplo di x ed y l'elemento di $+N_1$ ***minimo comune multiplo di*** $|x|$ ***e*** $|y|$***.***

3. - CONGRUENZE ARITMETICHE E ANELLI DELLE CLASSI RESTO.

I
ndichiamo con Z l'*ente* $(|Z|; S', P', >)$.
In base alle nozioni precedentemente introdotte consideriamo la relazione R_n definita su Z ponendo:

$$a \; R_n \; b \Leftrightarrow n \mid a - b \quad , \quad n \in +N_2 \; .$$

Scriveremo :

$$a \equiv b \; (n)$$

e leggeremo "***a congruo b modulo n***" per indicare che $a \; R_n \; b$; tale relazione sarà appunto detta ***congruenza aritmetica***.

Proprietà delle congruenze.
Dalla definizione data segue che
ogni numero è congruo a se stesso rispetto ad un qualsivoglia modulo n .

Inoltre, qualunque siano i numeri $a, b, c \in |Z|$ ed $n \in N_2$ sono ***ovvie*** le seguenti ***proprietà*** :

I. ***La scrittura*** $a \equiv b \; (n)$ ***equivale alla scrittura*** $b \equiv a \; (n)$.

II. ***Se*** $a \equiv b \; (n)$, $b \equiv c \; (n)$ ***allora*** $a \equiv c \; (n)$.

III. ***Se*** $a \equiv b \; (n)$, ***allora*** $a + c \equiv b + c \; (n)$, $ac \equiv bc \; (n)$.

Da quest'ultima proposizione discende che, se

$a_1 , a_2 , b_1 , b_2 \in |Z|$, $n \in N_2$ e risulta $a_1 \equiv b_1 \ (n)$, $a_2 \equiv b_2 \ (n)$, sarà pure :

$$a_1 + a_2 \equiv b_1 + b_2 \ (n) ,$$

$$a_1 a_2 \equiv b_1 b_2 \ (n) ;$$

e di qui, con evidente ***ragionamento per induzione***, si trae che qualunque siano i numeri interi

$$a_1 , a_2 , \dots , a_n , \qquad b_1 , b_2 , \dots , b_n , \qquad \text{con } \forall \ n \geq 2 ,$$

IV. Se $a_1 \equiv b_1 \ (n) , a_2 \equiv b_2 \ (n) \dots , a_n \equiv b_n \ (n)$
allora

$$\sum_1^n k \ a_k \equiv \sum_1^n k \ b_k \ (n) ,$$

$$\prod_{k=1}^{n} a_k \equiv \prod_{k=1}^{n} b_k \ (n) ;$$

in particolare da

$$a \equiv b \ (n)$$

segue

$$a^m \equiv b^m \ (n) , \qquad \forall \ m \in N$$

Notiamo infine ancora che:
V. Se d è ***un numero naturale divisore dei due numeri interi*** a, b ***e del numero naturale*** n, da $a \equiv b \ (n)$ segue

$$\frac{a}{b} \equiv \frac{b}{d}\left(\frac{n}{d}\right).$$

Infatti, se vi è un numero intero q , per cui risulta $a - b = nq$, risulterà pure

$$\frac{a}{d} - \frac{b}{d} = \frac{n}{d} q .$$

VI. ***Se dei due numeri interi*** a , b ***il secondo è primo col numero naturale*** n , ***da*** $ab \equiv 0 \ (n)$
segue

$$a \equiv 0 \ (n) .$$

Infatti, se vi è un intero q, per cui risulta $ab = nq$, essendo ***b ed n privi di divisori comuni maggiori di 1***, ogni ***divisore*** cosiffatto ***di n sarà pure un divisore di*** a , cioè ***a sarà divisibile per n***.

Tale ***relazione di congruenza*** permette di costruire un interessante ***anello finito***, detto ***resto modulo*** n .

Premettiamo:
La ***relazione*** $\equiv$ è una ***relazione di equivalenza su*** $|Z|$.

Infatti, essendo ***ovvie*** le ***proprietà riflessiva*** e ***simmetrica***, la ***transitiva*** segue dal fatto che
se $n \mid a-b$ ***ed*** $n \mid b-c$, allora $n \mid a-c$.

Denotiamo con $|Z|_{(n)}$ l'***insieme quoziente*** $|Z|/R_n$ ed indicheremo con $\bar{a}$ al posto $\bar{a}_{(n)}$ il generico elemento di $|Z|_{(n)}$, con la convenzione che scriveremo $\bar{a}$ al posto di $\bar{a}_{(n)}$, ogni qualvolta non ci sia possibilità di equivoco.

Dimostriamo il seguente

Teorema

Quali che siano $\bar{a},\bar{b} \in |Z|_{(n)}$, $n \in +N_2$ ***posto***

$$\bar{a}+\bar{b}=\overline{a+b}, \quad \bar{a}\cdot\bar{b}=\overline{a\cdot b},$$

risulta che se $a' \in \bar{a}$, $b' \in \bar{b}$, ***allora***

$$a'+b' \in \overline{a+b}, \quad a'\cdot b' \in \overline{a\cdot b}.$$

Dimostrazione
Infatti se $a' \in \bar{a}$, risulta che $n \mid a'-a$, onde $a'=a+kn$, $k \in \pm N_o$ ed analogamente se $b' \in \bar{b}$, risulta che $n \mid b'-b$, onde $b'=b+hn$, $h \in \pm N_o$.
Ne segue che :

$$a'+b'=a+b+(k+h)n$$

$$a'\cdot b' = a\cdot b+(ha+kb+hkn)n,$$

onde il ***teorema è dimostrato*** .

Definizione di addizione e moltiplicazione in $|Z|_{(n)}$.
Diciamo ***addizione*** in $|Z|_{(n)}$ l'***applicazione*** :

$$S_{(n)} : |Z|_{(n)}^{x2} \rightarrow |Z|_{(n)}$$

definita , $\forall \bar{a},\bar{b} \in |Z|_{(n)}$, ponendo :

$$S_{(n)}(\bar{a},\bar{b}) = \overline{a+b}.$$

Diciamo ***moltiplicazione*** in $|Z|_{(n)}$ l'***applicazione*** :

$$P_{(n)} : |Z|^{x^2} \rightarrow |Z|_{(n)}$$

definita ponendo $\forall \bar{a},\bar{b} \in |Z|_{(n)}$:

$$P_{(n)}(\bar{a},\bar{b}) = \overline{a\cdot b}.$$

Denotiamo con $|Z|_{(n)}$ la ***struttura algebrica*** :

$$(|Z|_{(n)}; S_{(n)}, P_{(n)})$$

e dimostriamo il

Teorema :
La struttura algebrica $Z_{(n)}$ è un anello commutativo ed unitario.

Dimostrazione
Infatti, fissato $n \in +N_2$, $\forall \bar{a},\bar{b},\bar{c} \in | Z |_{(n)}$ si ha:

$$\bar{a}+(\bar{b}+\bar{c}) = \bar{a}+\overline{b+c} = \overline{a+(b+c)} = \overline{(a+b)+c} =$$

$$= (\overline{a+b})+\bar{c} = (\bar{a}+\bar{b})+\bar{c}$$

Cioè, vale la ***proprietà associativa rispetto all'operazione addizione.***

Rispetto alla ***moltiplicazione*** si ha :

$$\bar{a}\cdot(\bar{b}\cdot\bar{c}) = \bar{a}\cdot(\overline{b\cdot c}) = \overline{a\cdot(b\cdot c)} = \overline{(a\cdot b)\cdot c} = (\overline{a\cdot b})\cdot\bar{c} = (\bar{a}\cdot\bar{b})\cdot\bar{c}.$$

cioè vale la ***proprietà associativa*** .

Poiché risulta

$$\bar{a}+\bar{b} = \overline{a+b} = \overline{b+a} = \bar{b}+\bar{a}$$

l'***addizione*** soddisfa quindi la ***proprietà commutativa***, analogamente vale per la ***moltiplicazione***:

$$\bar{a}\cdot\bar{b} = \overline{a\cdot b} = \overline{b\cdot a} = \bar{b}\cdot\bar{a}.$$

$\bar{0}$ ed $\bar{1}$ sono gli ***elementi neutri*** rispettivamente per l'***addizione*** e la ***moltiplicazione***,

Esempio

$$\left.\begin{array}{l} \bar{a}+\bar{0} = \overline{a+0} = \bar{a} \\ \\ \bar{a}\cdot\bar{1} = \overline{a\cdot 1} = \bar{a} \end{array}\right\} \quad \forall a \in Z_{(n)}$$

L'elemento $-a$ è l'***opposto di a*** , infatti

$$\bar{a}+(\overline{-a}) = (\overline{a-a}) = \bar{0}.$$

Si noti che è $\overline{n-a} = (\overline{-a})$, infatti

n – a – (- a) è divisibile per n .

OSSERVAZIONE. $Z_{(n)}$ in generale ***non è un campo***.

Per esempio consideriamo che in $Z_{(4)}$ si ha:

$$\bar{2} \cdot \bar{2} = \bar{4} = \bar{0},$$

esistono, cioè, ***divisori dello zero*** e quindi l'***elemento considerato non può avere inverso***.

Più in generale ***se n è un numero composto***, ***$Z_{(n)}$ possiede divisori dello zero***.
Se, infatti risulta

$$n = s \cdot t,$$

con ***s e t divisori propri***, e perciò ***diversi da 1*** e ***da n*** , si ha per gli elementi di $Z_{(n)}$:

$$\bar{s} \neq 0, \quad \bar{t} \neq 0, \text{ con } \overline{s \cdot t} = \bar{n} = \bar{0}.$$

Se n non è composto si dimostra il

Teorema

Se n è un numero primo, $Z_{(n)}$ è un anello di integrità, anzi addirittura un campo.

Dimostrazione . Sia dunque ***n = p = numero primo***.
Consideriamo una ***classe*** $\bar{a} \in |Z|_{(p)}$ ***non nulla*** e un suo rappresentante ***a***; poiché se $x \in \pm N_0$ $p \nmid x$ ***se e solo se*** $x = \bar{0}$, ne segue che un $a \in \bar{a} \neq \bar{0}$ ***è tale che p non | a.***

Consideriamo i ***primi p – 1 multipli di a*** :

$$\{h \cdot a\}_{h \in N_1 - N_P} = \{1 \cdot a = a, 2 \cdot a, \ldots, (p-1) \cdot a\}.$$

Siano:

$$h \cdot a, \quad k \cdot a \qquad \text{con } h, k < p, h \neq k,$$

due ***distinti multipli di a*** tra quelli considerati; essi ***non possono*** in alcun caso ***essere congrui modulo p*** .

Infatti ciò ***significherebbe***

$$p \mid (h\,a - K\,a),$$

cioè

$$p \mid (h - K)\,a .$$

Ma essendo ***p primo***, ***p divide il prodotto (h – K) · a se e soltanto se divide (almeno) uno dei due fattori***, per il I Teorema di Euclide, il che - nel nostro caso - ***non è*** , poiché la ***differenza h – k è inferiore a p*** (in valore assoluto), ed ***a*** , come si è già detto , ***non è multiplo di p*** , essendo un ***elemento di una classe resto diversa dalla classe*** $\bar{0}$.
Tutto ciò significa che i ***p – 1 numeri***

$$\{h \cdot a\}_{h \in N_1 - N_P}$$

possono essere ***assunti*** come ***rappresentanti*** delle ***p -1 classi resto non nulle modulo p*** , cioè che le classi resto:

$$\bar{a}\,,\ \overline{2a}\,,\ \ldots,\ \overline{(p-1)\cdot a}$$

sono, a meno dell'ordine, le ***p - 1 classi non nulle modulo p*** :

$$\bar{1}\ \ ,\ \ \bar{2}\,,\ \ldots,\ \overline{p-1}.$$

Perciò, tra le classi considerate comparirà, una volta e una sola, la classe $\bar{1}$. Sia $x \cdot a \in \{h \cdot a\}_{h \in N_1 - N_p}$ l'elemento che dà luogo alla classe $\bar{1}$. e cioè tale che sia:

$$\overline{x \cdot a} = \bar{1}$$

Sarà allora :

$$\overline{x \cdot a} = \bar{x} \cdot \bar{a} = \bar{a} \cdot \bar{x} = \bar{1}\,,$$

onde $\bar{x}$ è la ***classe inversa della classe*** $\bar{a}$, cioè :

se p è primo, ogni classe resto modulo p non nulla possiede una classe inversa.

Pertanto la ***struttura algebrica*** :

$$(|\,Z\,|_{(p)} - \{\bar{0}\};\ P_{(p)})$$

è un ***gruppo abeliano*** e quindi ***$Z_{(p)}$ è un campo***.

OSSERVAZIONE.
Il teorema ora mostrato assicura nel caso di $Z_{(p)}$ l'***esistenza dell'inverso di ogni elemento non nullo***, ma non ne fornisce l'espressione.

Prima di occuparci dell'espressione dell'inverso di una classe, quando esiste, occorre pervenire al **teorema di Eulero**, mediante il quale, oltre a caratterizzare l'inversa di una classe modulo un numero primo, caratterizzerà anche l'inversa di una classe modulo un numero composto quando esiste.

4.- PROPRIETÀ ED ESPRESSIONE DELLA FUNZIONE DI EULERO- GAUSS.

Indichiamo nel seguito, $\forall n \in N_1$, con (n) , il **numero degli elementi di** F_n, cioè della ***parte di*** $N_1 - N_{n+1}$ ***costituita dai numeri primi con n***.
Si ha ovviamente :

$$\varphi(n) = pot\ F_n .$$

Essendo quindi $F_1 = \{1\}$, $F_p = N_1 - N_p$, $\forall\ p \in P$, segue :

$$\varphi(1) = 1, \qquad \varphi(p) = p - 1 .$$

Si ha il

Teorema

Se $p \in P$ ***e*** $n \in N$, ***allora :***

$$\varphi(p^n) = p^{n-1} \qquad \varphi(p) = p^{n-1} \cdot (p - 1) .$$

Dimostrazione. Posto $a = p^n$, $b = p^{n-1}$, consideriamo $N_1 - N_{a+1}$; gli ***elementi di questo insieme non primi con*** n sono ***tutti e solo quelli che sono multipli di p*** e cioè quelli dell'insieme:

$$A = \{p , 2p , \dots , b \cdot p\} = \{h \cdot p\}_{h \in N_1 - N_{b+1}}$$

onde:

$$F_a = (N_1 - N_{a+1}) - A$$

segue:

$$\varphi(a) = a - b = p^n - p^{n-1} = p^{n-1} \cdot (p - n) .$$

Lemma 1

Quali che siano $a , b \in N$ ***con*** $(a , b) = 1$ ***e se*** $x \in N_0 - N_b$, $y \in N_0 - N_a$, ***allora i resti positivi delle divisioni dei numeri*** $ax + by$ ***per il numero*** $a \cdot b$ ***sono tutti i numeri di*** $N_0 - N_{ab}$.

Dimostrazione

E' intanto evidente che ***ogni resto delle divisioni dette*** è un ***elemento di*** $N_0 - N_{ab}$.
Occorre provare che sono ***tutti*** .
Se $ax + by$ ed $ax' + by'$ sono ***due diversi numeri*** del tipo detto , non può essere:

$$ax + by \equiv ax' + by' \ (ab) ,$$

poichè dalla relazione seguirebbe :

$$a(x - x') = b(y' - y) + k\,ab ,$$

onde

$$b \mid a(x - x') \quad \text{e} \quad a \mid b(y' - y) ,$$

il che è ***assurdo*** poiché $(a , b) = 1$ ed $x, x' \in N_0 - N_b$; $y, y' \in N_0 - N_a$
Allora , poiché $N_0 - N_{ab}$ è ***equipotente*** ad $(N_0 - N_b) \times (N_0 - N_a)$
cioè :

$$(N_0 - N_b) \times (N_0 - N_a) \sim N_0 - N_{ab}$$

segue che i ***resti*** dei ***numeri*** $ax + by$ ***modulo*** ab, dovendo essere tutti ***distinti***, ***minori di*** ab ed ***in numero di*** $ab - 1$, sono gli ***elementi di*** $N_0 - N_{ab}$.

Premettiamo il

Lemma 2

Quali che siano $a , b \in N_1$ ***con*** $(a, b) = 1$ ***e se*** $x \in F_b$, $y \in F_a$, ***allora i resti positivi delle divisioni dei numeri*** $ax + by$ ***per il numero*** $a \cdot b$ ***sono tutti gli elementi di*** $F_{a \cdot b.}$

Dimostrazione. Escluso il ***caso banale*** di $a = b = 1$, considero il numero $ax + by$.
Tale ***numero*** è ***primo con*** $a \cdot b$.
Infatti, detto $p \in P$ un ***divisore primo comune*** si avrà:

$$p \mid a \cdot b \quad , \quad p \mid ax + by .$$

Essendo $(a , b) = 1$ si ha o $p \mid a$ con $p \nmid b$, oppure $p \nmid a$ con $p \mid b$.
Nel ***primo caso*** da $p \mid ax + by$ e da $p \mid a$ segue che $p \mid by$, ma $p \nmid b$ *e* $p \nmid y$ poiché $y \in F_a$ e quindi $(a , y) = 1$ e ***non*** p, onde l'***assurdo***.

Analogamente si ragione nel ***secondo caso***.
Mostriamo ora che se $ax' + by' \neq ax + by$, allora i ***due numeri sono incongrui modulo*** $a \cdot b$.
Se infatti risulta

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

segue

$$a (x' - x) = b (y - y') + k a b$$

da cui dovrebbe essere

$$b \mid a (x' - x) \quad , \quad a \mid b (y - y')$$

il che è ***assurdo***.
Allora i ***resti modulo*** $a \cdot b$ sono ***tutti diversi tra loro*** e sono inoltre ***primi con*** $a \cdot b$ come è ovvio dalla ***relazione***

$$ax + by = q \cdot ab + r .$$

Quindi i ***resti*** sono tutti ***elementi distinti di*** F_{ab} .

Fissato un elemento $c \in F_{ab}$, consideriamo i numeri $ax + by$, con $x \in N_0 - N_b$, $y \in N_0 - N_a$, esiste, per il **lemma 1**, un'***unica coppia*** (x', y') , tale che

$$ax' + by' = q\,(a \cdot b) + c$$

mostriamo che

$$x' \in F_b \qquad y' \in F_a \ .$$

Intanto è $x' \neq 0$, $y' \neq 0$ perché ***c è primo con a · b*** .
Allora se esiste $p \in P$ tale che

$$p \mid x' \quad , \quad p \mid b$$

ne seguirebbe che $p \mid c$, onde ***c ed ab avrebbero il divisore comune p*** , ***contro l'ipotesi che*** $c \in F_{ab}$.

Analogamente si dimostra che ***y' ed a sono primi.***

Pertanto ***ogni*** $c \in F_{ab}$ ***è uno dei resti del nostro teorema***.

Dal **Lemma 2** discende la

Proprietà moltiplicativa della φ .
Quali che siano $a , b \in N_1$ ***con*** $(a, b) = 1$, ***allora :***

$$F_{a \cdot b} \sim F_a \times F_b \quad ,$$

ovvero:

$$pot\ F_{a \cdot b} = pot\,(F_a \times F_b),$$

ovvero :

$$\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b) \ .$$

Si ha inoltre, come è ovvio, di conseguenza :

$$\varphi(n) = \varphi\left(\prod_{i=1}^{r} p_i^{\alpha_i}\right) = \prod_{i=1}^{r} \varphi(p_i^{\alpha_i}) = \prod_{i=1}^{r} p_i^{\alpha_{i-1}}\ \varphi(p_i) = \prod_{i=1}^{r} p_i^{\alpha_{i-1}}\ (p_i - 1) = n \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right)$$

che è l'***espressione della*** φ ***per un qualsisi n*** .

5. TEOREMI DI EULERO – FERMAT – WILSON .

Dimostriamo il seguente

<u>Teorema di Eulero</u>
Quali che siano $a , n \in N_1$ ***con*** $(a , n) = 1$, ***si ha***:

$$a^{\varphi(n)} \equiv \varphi(n).$$

Dimostrazione. Posto infatti $m = \varphi(n)$ ed escluso il ***caso banale*** $n = 1$, consideriamo :

$$F_n = \{ a_1, a_2, \ldots\ldots, a_m \}$$

e indichiamo con $r_1, r_2, \ldots, r_m$ rispettivamente i ***resti positivi della divisione con resto degli*** $a \cdot a_i$ ***per*** n .
Sarà dunque:

$$a \cdot a_i \equiv r_i \quad (n).$$

Ora, poiché $r_i \in N_1 - N_n$ ed è ***primo con*** n , poiché, ***se*** $p \in P$ è tale che $p \mid n$ e $p \mid r$, ne segue che $p \mid a \cdot a_i$ e ciò è ***assurdo***, si ha che $r_i \in F_n$.

Ora gli ***m resti*** r_i sono ***tutti*** tra loro ***distinti***, poiché se fosse $r_i \equiv r_j \quad (i \neq j)$ da

$$a \cdot a_i = q_i \cdot n + r_i$$
$$a \cdot a_j = q_j \cdot n + r_j$$

segue, ***per sottrazione*** :

$$a \cdot (a_i - a_j) = (q_i - q_j) \cdot n$$

relazione che risulta essere ***assurda*** poiché $n \nmid a \;\; e \;\; n \nmid (a_i - a_j)$.

Allora gli r_i ***sono tutti e soli gli elementi di*** F_n .

Consideriamo ora la ***congruenza vera*** :

$$\prod_{i=1}^{m} a \cdot a_i \equiv \prod_{i=1}^{m} r_i \quad (n)$$

Essendo

$$\prod_{i=1}^{m} a_i = \prod_{i=1}^{m} r_i = \prod_{b \in F_n} b = c$$

ed essendo $(c, n) = 1$, dal fatto che

$$a^m \cdot c \equiv c \quad (n)$$

segue

$$a^m \equiv 1 \; (n) \; .$$

Un caso particolare del **Teorema di Eulero** è costituito dal

Teorema di Fermat . *Quali che siano* $a \in N_1$, $p \in P$ *con* $(a, p) = 1$, *risulta:*

$$a^{p-1} \equiv 1 \; (p) \; .$$

Dimostrazione. Infatti dal ***teorema di Eulero*** *e per essere* $\varphi(p) = p - 1$ *segue il* ***teorema di Fermat*** .

Teorema di Wilson. *Condizione necessaria e sufficiente affinché un numero p sia primo è che*

$$(p-1)! + 1 \equiv 0 \quad (p)$$

oppure

$$\{\varphi(p)\}! + 1 \equiv 0 \quad (p)$$

Dimostrazione.

$\Rightarrow$ Consideriamo la ***successione***

$$\mathbf{(1)} \qquad 1, 2, \ldots, p-2, p-1$$

Ad ogni termine i corrisponde ***biunivocamente*** un termine j della stessa successione, tale che

$$\mathbf{(2)} \qquad i \cdot j \equiv 0 \quad (p)$$

Infatti, poiché i è, ovviamente, ***primo con*** p, ciascun termine della successione

$$(3) \qquad i, 2 \cdot i, 3 \cdot i. \ldots, (p-1) \cdot i$$

è ***congruo modulo*** p ***ad uno e uno soltanto dei termini della (1)***, e viceversa.

Dunque, in particolare, il ***primo termine della (1)*** è ***congruo ad uno ed uno soltanto dei termini*** $i \cdot j$ ***della (3)***, cioè

$$\mathbf{(2')} \qquad i \cdot j \equiv 1 \quad (p)$$

e quindi al termine i della **(1)** corrisponde un termine j della **(1)** stessa, tale da ***soddisfare la (2').***

$\Leftarrow$ ***Reciprocamente***, a j corrisponde, nello stesso senso, il termine i, giacchè in caso contrario, essendo $k \neq i$ il ***corrispondente di*** j, si avrebbe

$$j \cdot k \equiv 1 \quad (p)$$

e da questa e dalla **(2')** risulterebbe

$$j \cdot (i - k) \equiv 0 \quad (p)$$

evidentemente ***assurda***, da cui la tesi.

6.- ELEMENTI INVERTIBILI E DIVISORI DELLO ZERO IN $Z_{(m)}$

Ci proponiamo ora, nell'ipotesi di m composto, di caratterizzare gli elementi invertibili ed i divisori dello zero di $Z_{(m)}$. Abbiamo visto che quando m è primo allora l'anello è un campo.

Cominciamo con il provare che

Teorema

Condizione necessaria e sufficiente perché la classe $\bar{a} \neq \bar{0}$ di $Z_{(m)}$ sia un divisore dello zero è che

$$(a, m) > 1$$

Dimostrazione

$\Rightarrow$

Supponiamo $(a, m) = n > 1$. Essendo la classe $\bar{a} \neq \bar{0}$ segue che a non è un multiplo di m ed n non è un multiplo di m (altrimenti lo sarebbe anche a).
Segue che

$$a = h \cdot n \qquad m = k \cdot n \qquad \text{con } 1 < k < m$$

Dunque risulta la classe $\bar{k} \neq \bar{0}$. Ma allora la classe $\bar{a}$ è un divisore dello zero perché esiste una seconda classe $\bar{k}$ tale che

$$\bar{k} \cdot \bar{a} = \overline{k \cdot h \cdot n} = \overline{h \cdot m} = \bar{0}$$

mentre le due classi $\bar{k}$ ed $\bar{a}$ sono non nulle.

$\Leftarrow$

Inversamente supponiamo che la classe $\bar{a} \neq \bar{0}$ sia un divisore dello zero.
Esiste dunque $\bar{b} \neq \bar{0}$ tale che

$$a \cdot b = 0.$$

Ciò significa $a \cdot b = k \cdot m$.
Ora se fosse $(a, m) = 1$ avremmo

$$a^{\varphi(m)} = 1 + h\, m.$$

Segue allora

$$a^{\varphi(m)} \cdot b = b + b \cdot h \cdot m$$

$$a^{\varphi(m)}\, b = a^{\varphi(m)-1} \cdot k\, m$$

e quindi b sarebbe un multiplo di m, cioè $\bar{b} = \bar{0}$, contro l' ipotesi.

Indicheremo nel seguito con $U_{(m)}$ gli elementi $\bar{a}$ tali che (a, m) = 1.

Proviamo che:

Teorema

Condizione necessaria e sufficiente a che un elemento a di $Z_{(m)}$ sia invertibile è che sia in $U_{(m)}$, cioè risulti

$$(a, m) = 1.$$

Dimostrazione.

$\Rightarrow$

La condizione è necessaria.

Se $\bar{a}\ \bar{b}$ è invertibile, cioè se esiste una classe $\bar{x} \neq \bar{0}$ tale che $\bar{a} \cdot \bar{x} = \bar{1}$, allora $\bar{a}$ non può essere un divisore dello zero, cioè non può essere $\bar{a} \cdot \bar{b} = \bar{0}$ con $\bar{b} \neq \bar{0}$, perché altrimenti sarebbe

$$\bar{0} \neq \bar{b} = \bar{b} \cdot \bar{1} = \bar{b} \cdot \bar{a} \cdot \bar{x} = \bar{0} \cdot \bar{x} = \bar{0} \ .$$

$\Leftarrow$

La condizione è sufficiente. Se $\bar{a} \in U_{(m)}$, allora per il teorema precedente a ed m sono primi tra loro, e quindi nessuno degli m -1 numeri

$$\textbf{(1)} \qquad a, 2a, \ldots\ldots\ldots\ldots, (m-1)a$$

è divisibile per m , inoltre anche nessuna delle differenze di due qualunque distinti numeri **(1)** è divisibile per m, giacchè ciascuna di tali differenze è riducibile alla forma

$$(h - k)\, a, \qquad \text{con } 0 < (h-k) < m .$$

Ciò equivale ad affermare che le classi

$$\bar{a}, \overline{2 \cdot a}, \ldots, \overline{a \cdot (m-1)}$$

sono tutte diverse tra loro e dalla classe $\bar{0}$ pertanto esse devono coincidere, a prescindere dall'ordine con le m-1 classi

$$\bar{0}, \bar{1}, \ldots, \overline{m-1}$$

che seguono la prima.

In particolare, una ed una sola $\overline{x \cdot a}$ di quelle deve coincidere con la classe $\bar{1}$, sicchè risulta

$$\bar{x} \cdot \bar{a} = \overline{x \cdot a} = \bar{1}$$

e la classe a è invertibile.

Si ottiene quindi il

Teorema

L' ente $U_{(m)} = \{ U_{(m)}, P_{(m)} \}$ è un gruppo, detto gruppo delle Unità di $Z_{(m)}$.

Dimostrazione.

Per come è stata definita l' operazione di moltiplicazione $P_{(m)}$ l' ente algebrico $U_{(m)}$ è chiuso rispetto ad essa, ed essendo $U_{(m)}$ l'insieme degli elementi che non siano divisori dello zero e diversi dalla classe $\bar{0}$, ognuno di essi sarà dotato di inverso e quindi sono soddisfatte le condizioni perché

$$U_{(m)} = \{ U_{(m)}, P_{(m)} \}$$

sia un gruppo.

Ora osserviamo che se $\bar{a}$ non è divisore dello zero e se risulta il numero $a < m$, certamente $a \dagger m$ e quindi $(a, m) = 1$.

Vale allora il teorema di Eulero e si ha:

$$a^{\varphi(m)} \equiv 1 \qquad (m)$$

ed anche

$$a \cdot a^{\varphi(m)-1} \equiv 1 \qquad (m)$$

e cioè

$$\bar{a} \cdot \overline{a^{\varphi(m)-1}} = \bar{1}$$

da cui l'inversa della classe $\bar{a}$, che non è né lo zero, né un divisore dello zero, si ottiene considerando il rappresentante positivo maggiore di m e pertanto la classe individuata dalla potenza $a^{\varphi(m)-1}$.

Quoziente di due classi

Una classe $\bar{a}$ si dice divisibile per la classe $\bar{b}$ se esiste una classe $\bar{x}$ tale che

(1) $\qquad \bar{a} = \bar{b} \cdot \bar{x}$

In tal caso si dice che si è eseguita una divisione di $\bar{a}$ per $\bar{b}$ e la classe $\bar{x}$ si chiama classe quoziente delle classi $\bar{a}$ (dividendo) e $\bar{b}$ (divisore).

La stessa definizione mostra che una classe $\bar{a}$ è divisibile per la classe $\bar{b} = \bar{0}$, se e solo se essa stessa è nulla ($\bar{a} = \bar{0}$), nel qual caso un'arbitraria classe $\bar{x}$ soddisfa alla **(1)**, cioè è un loro quoziente.

Per evitare questo caso banale, supporremo sempre che il divisore sia non nullo, cioè $\bar{b} \neq \bar{0}$.

Circa l'esistenza e l'unicità del quoziente di due classi possiamo dimostrare il seguente

Teorema

Se nella divisione di $\bar{a}$ per $\bar{b} \neq \bar{0}$ il divisore b è primo con n, allora il quoziente $\bar{x}$ esiste sempre ed è univocamente determinato.

Dimostrazione. Supponiamo per il momento che esista una classe $\bar{x}$ tale che

$$\bar{a} = \bar{b} \cdot \bar{x};$$

possiamo allora moltiplicare entrambi i membri per la classe inversa di $\bar{b}$, cioè $\overline{b^{-1}}$, e il fatto che n sia primo con b ci assicura l'esistenza (per un teorema precedentemente dimostrato).
Otteniamo quindi

$$\bar{x} = \bar{a} \cdot \overline{b^{-1}}$$

il che mostra che la classe quoziente, se esiste è unica. D'altra parte è subito visto che, sostituendo ad $\bar{x}$ l'espressione $\bar{a} \cdot \overline{b^{-1}}$, la **(1)** è effettivamente verificata.

In particolare si ha

Teorema

Se n è un numero primo e, considerato p, esiste sempre uno e uno solo quoziente di una qualsiasi classe $\bar{a}$ per una qualsiasi classe $\bar{b} \neq \bar{0}$ ed esso è dato da

$$\bar{a} \cdot \overline{b^{-1}} = \bar{a} \cdot \overline{b^{p-2}}.$$

Si noti inoltre che sussiste il seguente

Teorema

Se nella divisione di $\bar{a}$ per $\bar{b} \neq \bar{0}$, il divisore b non è primo con n, allora il quoziente $\bar{x}$ non può esistere, o se esiste, non può essere determinato univocamente.

Dimostrazione. Il quoziente $\bar{x}$ può non esistere; basta assumere $\bar{a} = \bar{1}$ e b non primo con n; sappiamo infatti che se b non è primo con n, $\bar{b}$ non ammette inversa, e quindi non esiste una classe $\bar{x}$ tale che

$$\bar{b} \cdot \bar{x} = \bar{1}$$

Facciamo vedere ora che il quoziente, anche se esiste, non può essere unico.
Basta assumere $n = 6$, $\bar{a} = \bar{2}$, $\bar{b} = \bar{4}$, e notare che le classi $\bar{x} = \bar{2}$ e $\bar{x} = \bar{5}$ sono due quozienti distinti di $\bar{a}$ per $\bar{b}$.
Costruiamoci infatti la tabella di $(Z_{(6)}, P_{(6)})$

	1	**2**	**3**	**4**	**5**
1	**1**	**2**	**3**	**4**	**5**
2	**2**	**4**	**0**	**2**	**4**
3	**3**	**0**	**3**	**0**	**3**

4	**4**	**2**	**0**	**4**	**2**
5	**5**	**4**	**3**	**2**	**1**

e osserviamo che

$$\bar{2} \cdot \bar{4} = \bar{5} \cdot \bar{4} = \bar{2}.$$

7. GAUSSIANO E PRIME PROPRIETÀ DELLE POTENZE

Siano $a, m \in N_1$ con $(a, m) = 1$.
Consideriamo la congruenza

$$\textbf{(1)} \quad a^x \equiv 1 \quad (m)$$

una tale congruenza è certamente verificata per qualche $x_0 \in N_0$; è infatti vera per

$$x \in \{ k \cdot \varphi(m) \}_{k \in N_0}$$

Definizione
Si chiama **gaussiano di** m **in base** a e si indica con

$$g(m, a)$$

il più piccolo elemento di N_1 tale che sia

$$a^{g(m,a)} \equiv 1 \quad (m)$$

Si ha pertanto

$$g(m, a) = \min \{x : x \in N_1 \; a^x \equiv 1 \quad (m)\}$$

Si ha ovviamente:
a) $g(m, a) \leq \varphi(m)$
b) a^x non $\equiv 1 \quad (m)$ se $1 < x < g(m, a)$.

Dati $a, m \in N_2$ con $(a, m) = 1$, consideriamo la successione[1] delle potenze di a:

$$a^0, a^1, a^2, \ldots, a^n, \ldots$$

Si ha il seguente
Teorema
Quali che siano $a, m \in N_2$ e $(a, m) = 1$, $h, k \in N_0$, condizione necessaria e sufficiente affinché

$$a^h \equiv a^k \quad (m) \qquad h > k$$

è che sia

[1] Chiameremo successione di numeri naturali o di interi relativi ogni insieme del tipo $\{a_k\}_{k \in N_0}$, oppure $\{a_k\}_{k \in N_1}$, con $a_k \in |Z|$

$$a^{h-k} \equiv 1 \quad (m)$$

Dimostrazione

$\Rightarrow$ La condizione è necessaria.

Infatti se $a^h \equiv a^k \quad (m)$ si ha successivamente

$$a^h - a^k \equiv 0 \quad (m)$$

$$a^k (a^{h-k} - 1) \equiv 0 \quad (m)$$

ed essendo $(a^k, m) = 1$ segue l'asserto.

$\Leftarrow$ La condizione è sufficiente.

Se $a^{h-k} \equiv 1 \quad (m)$, moltiplicando ambo i membri per l'intero a^k segue ovviamente l'asserto.

Si ha:

Corollario. *Se $g = g\ (m,a)$, allora le potenze*

$$a^0, a^1, \ldots, a^{g-1}$$

sono a due a due incongrue tra loro.

Dimostrazione. Infatti se $h, k \in N_0 - N_g$, anche $h - k \in N_0 - N_g$, da cui

$$a^{h-k} \not\equiv 1 \quad (m)$$

e quindi l'asserto.

Teorema. *Se $a, m \in N_2$ e $(a, m) = 1$, condizione necessaria e sufficiente a che sia*

$$a^h \equiv a^k \quad (m)$$

è che sia

$$h \equiv k \quad (g)$$

Dimostrazione

$\Rightarrow$ *La condizione è necessaria.*

Infatti, se $a^h \equiv a^k \quad (m)$, eseguendo la divisione (con resto positivo) di h e k per g, si ottiene

$$h = q_h \cdot g + r_h \quad \text{e} \quad k = q_k \cdot g + r_k .$$

Se $h > k$ per il teorema precedente deve essere

$$a^{h-k} \equiv 1 \quad (m)$$

da cui, sostituendo i valori di h e di k, risulta:

$$a^{(q_h - q_k)g + (r_h - r_k)} \equiv 1 \quad (m)$$

per cui:

$$a^{r_h - r_k} \equiv 1 \quad (m).$$

Essendo $r_h - r_k < g$, la relazione può sussistere solo se $r_h = r_k$, cioè solo se

$$h - k = (q_h - q_k) \cdot g$$

che prova la tesi.

$\Leftarrow$ La condizione è sufficiente.
Se risulta $h \equiv k \ (g)$ è anche $h - k \equiv 0 \ (g)$, da ciò segue che

$$h - k = \rho \cdot g,$$

per cui si ha

$$a^{h-k} = a^{\rho \cdot g} = (a^g)^\rho \equiv 1^\rho \ (m) \equiv 1 \ (m)$$

e quindi la tesi.

Corollario. ***Quali che siano $a, m \in N_2$ e $(a, m) = 1$, risulta***

$$\varphi(m) \equiv 0 \ (g)$$

cioè

$$g \mid \varphi(m)$$

Dimostrazione. E' infatti

$$a^{\varphi(m)} \equiv 1 \ (m) \quad \text{e} \quad a^g \equiv 1 \ (m)$$

da cui

$$a^{\varphi(m)} \equiv a^g \ (m)$$

e quindi

$$\varphi(m) \equiv g \ (g)$$

da cui

$$\varphi(m) - g \equiv 0 \ (g)$$

cioè la tesi.

Teorema. ***Siano $a, m \in N_2$ e $(a, m) = 1$, posto $g = g(m, a)$, allora le potenze $\{a^k\}$ con $k \in N_0$ individuano in $Z_{(m)}$ g elementi distinti e non nulli che formano un sottogruppo moltiplicativo di $Z_{(m)}$.***

Dimostrazione. Consideriamo le potenze

$$a^0, a^1, \ldots a^{g-1}.$$

Esse sono a due a due incongrue tra loro ed individuano g elementi di $Z_{(m)}$.
Ora, se $k > g - 1$, si ha , essendo $k = hg + r$, con $r < g$,

$$a^k \equiv a^r \ (m);$$

pertanto

$$a^k \in [a^h]$$

Inoltre, essendo $a^k \bullet a^h = a^{h+k}$, risulta che le g classi formano un sottogruppo.

Da questo teorema, nelle stesse ipotesi, discende il

Corollario. ***Eseguendo le divisioni con resto degli elementi della successione $\{a^k\}$ con $k \in N_0$ per l'intero m, e posto $a^k = q_k \cdot m + r_k$, $(r_k < m)$ $\forall k \in N_0$, la successione $\{r_k\}$ con $k \in N_0$ è periodica di periodo g, ovvero risulta $r_h = r_k$ se e solo se $h \equiv k \ (g)$.***

Dimostrazione. Infatti, considerati $r_0, r_1, \ldots, r_{g-1}$ *ed essendo per* $k \geq g$

$$a^k \equiv a^h \quad (m) \quad \text{con } h \in N_o - N_g,$$

si ha

$$r_k = r_h$$

se e solo se

$$h \equiv k \quad (g).$$

8. SUCCESSIONI DI POTENZE E TEOREMI DI DIVISIBILITÀ RISPETTO AD UN MODULO NON PRIMO CON LA BASE.

Supponiamo ora che, dati m, $a \in N_2$ sia

$$(m, a) \in N_2.$$

Esiste certamente qualche ***numero primo*** che divide sia m che a, poiché $(m,a) \in N_2$.
Indichiamo con $m_0 \in N_2$ il ***più grande divisore*** di m nella cui fattorizzazione intervengano soltanto numeri primi che dividono (m, a).
Più precisamente, se $p \mid (m, a)$, $p \in P$ e se $\alpha \equiv \alpha \ (p, m)$ è il più grande intero per cui $p^\alpha \mid m$, si ha:

$$m_0 = p \mid \prod_{(m,a)} p^\alpha.$$

Esempio
Siano $m = 2 \cdot 3^2 \cdot 5^4 \cdot 7$, $a = 2^4 \cdot 3 \cdot 5^3 \cdot 11$, allora:

$$m_0 = 2 \cdot 3^2 \cdot 5^4$$

Se considero, allora, i due interi:

$$\frac{m}{m_0} \in N_1, \quad a \in N_2,$$

essi sono primi tra loro, poiché, se esiste un numero primo $p \mid \frac{m}{m_0}$, esso è tale che $p \nmid a$; ha senso pertanto considerare l'intero:

$$g_0 = g\left(\frac{m}{m_0}, a\right), \quad g_0 \in N_1.$$

Consideriamo, infine, la congruenza:

$$a^x \equiv 0 \quad (m_0).$$

Poiché $m_0 \in N_2$ e i fattori primi d m_0 dividono a, detta h la potenza massima dei fattori primi di m_0, certamente $m_0 \mid a^h$, onde la congruenza è vera per qualche $x \in N_1$.

Denoteremo con α il più piccolo elemento di N_1 per il quale la congruenza è verificata.

Nel seguito intervarranno i simboli:

$$a, m \in N_2 \quad \text{con } (a, m) \in N_2 \times N_2$$

nonché $\quad m_0 \in N_2, \quad g_0 \in N_1, \quad \alpha \in N_1.$

Si ha con la nomenclatura precedente il

Teorema

Se $(a, m) \in N_2 \times N_2$; $a, m \in N_2$, allora, eseguendo la divisione con resto positivo degli elementi della successione $\{a^k\}$ con $k \in N_0$, per l'intero m, e posto:

$$a^k = q_k \cdot m + r_k \quad (r_k < m), \quad \forall\, k \in N_0,$$

la successione $\{r^k\}$ con $k \in N_0$ dopo i primi α numeri distinti:

$$r_0, r_1, \ldots, r_{\alpha-1}$$

presenta g_0 numeri distinti:

$$r_\alpha, r_{\alpha-1}, \ldots, r_{\alpha+g0-1}$$

che si ripetono periodicamente, cioè:

$$r_{\alpha-k} = r_{\alpha-k} \quad \Leftrightarrow \quad h \not\equiv k \quad (g_0).$$

Dimostrazione. Cominciamo con il dimostrare che le potenze:

$$a^0, a^1, \ldots, a^{\alpha-1}$$

sono a due a due incongrue tra loro rispetto al modulo m.

Infatti, se $0 < h < k < \alpha$, si ha che se:

$$a^k - a^h \equiv 0 \quad (m),$$

si ha

$$a^h (a^{k-h} - 1) \equiv 0 \quad (m).$$

Ora, essendo m_0 ed $\frac{m}{m_0}$ divisori complementari di m, seguirebbe:

$$a^h (a^{k-h} - 1) \equiv 0 \quad (m_0).$$

Esistendo qualche numero primo divisore comune di m_0 ed a ed essendo $k - h \in N_1$, risulta:

$$a^{k-h} - 1 \not\equiv 0 \quad (m_0).$$

Si deduce che allora successivamente deve essere:

$$a^h \equiv 0 \quad (m_0),$$

ma, poiché è $h < \alpha$, la relazione è falsa, onde non può essere vero che $a^k \equiv a^h \ (m)$, con $h < k < \alpha$, pertanto i resti $r_0, r_1, \ldots, r_{\alpha-1}$ sono tutti distinti.
Consideriamo ora le potenze:

$$a^{\alpha}, a^{\alpha-1}, \ldots., a^{\alpha+g0-1}$$

Se

$$a^{\alpha+h} \equiv a^{\alpha+k} \quad (m) \quad \text{con } 0 \leq h < k < g_0 \ ,$$

risulta:

$$a^{\alpha+h} \ (a^{k-h} - 1) \equiv 0 \quad (m)$$

e, quindi, anche

$$a^{\alpha+h} \ (a^{k-h} - 1) \equiv \ 0 \quad \left(\frac{m}{m_0}\right)$$

Ora poiché $(a, \frac{m}{m_0}) = 1$, ne segue che deve essere necessariamente

$$a^{k-h} - 1 \equiv 0 \quad \left(\frac{m}{m_0}\right) \qquad \text{con} \quad k - h < g_0 \ ,$$

il che è vero solo se $k = h$ per definizione di g_0; ma per ipotesi è $h < k$.
Pertanto anche i resti:

$$r_{\alpha}, \ r_{\alpha-1}, \ \ldots, r_{\alpha+g0-1}$$

sono tutti distinti.

Sia ora $a^{\alpha+h}$, $k > g_0$ una qualunque potenza successiva.
Vogliamo mostrare che esiste un $h < g_0$, tale che

$$a^{\alpha+h} \equiv a^{\alpha+k} \quad (m).$$

Questa relazione è vera se e solo se

$$a^{\alpha+h} \equiv a^{\alpha+k} \quad \left(\frac{m}{m_0}\right).$$

Infatti, se $a^{\alpha+h} - a^{\alpha+k} = \rho \ m$ risulta

$$a^{\alpha+h} - a^{\alpha+k} = (\rho \ m_0) \ \frac{m}{m_0} \qquad (*)$$

ed, inversamente, se

$$a^{\alpha+h} - a^{\alpha+k} = \rho' \ \frac{m}{m_0} \quad \text{con} \quad \alpha \neq 0$$

il primo membro è divisibile per m_0, da cui, essendo $(a, \frac{m}{m_0}) = 1$, si ha che ρ' è divisibile per m_0.
Ne segue quindi che la (*) è vera se e solo se

$$\alpha + h \equiv \alpha + k \quad (g_0)$$

e cioè

$$h \equiv k \quad (g_0)$$

il che dimostra la tesi.

9.- CRITERI DI DIVISIBILITÀ IN UN SISTEMA DI NUMERAZIONE.

Sia $B = \{0 , 1 , \ldots , x \}$ l'insieme dei simboli di un sistema di numerazione. Se x^* è il successivo di x, poniamo x^*. E' quindi $a \in N_1^*$.
Porremo nel seguito sempre $1^* = 2$ (cosa non lecita solo nel caso che la numerazione sia binaria).
Ogni $n \in N_2$ si può rappresentare in uno e un solo modo nella forma

$$n = \sum_{k=0}^{t} a^k = (c_t, c_{t-1}, \ldots, c_0)_a$$

dove ogni $c_k \in B$; tali elementi sono detti ***cifre del numero n nella base a***.

dividendo le potenze $\{a^k\}$ con $k \in N_0$ per un intero $m \in N_2$, si ottengono dei resti non negativi

$$r_0, r_1, \ldots , r_t , \ \ldots$$

Eseguendo ora la divisione con resto non negativo dell'intero m per il naturale 2 si ottiene un quoziente q.
Se esiste qualche r_k tale che sia $r_k > q$, consideriamo il relativo $r_k - m$ e poniamo

$$\rho_k = \begin{cases} r_k & \text{se } r_k \le q \\ r_k - m & \text{se } r_k > q \end{cases}$$

La successione $\{ \rho_k \}$ con $k \in N_0$ è detta ***successione dei coefficienti di divisibilità del numero m nella base a.***
Usando la nomenclatura dei teoremi del paragrafo precedente si possono presentare sostanzialmente due casi:
I caso. E' $(a, m) = 1$. Se allora è $g = g(m, a)$, la successione dei resti è periodica (semplice) di periodo g e quindi lo è anche la successione dei coefficienti di divisibilità, i quali saranno individuati dai g interi relativi appartenenti all'insieme

$$\{\rho_0, \rho_1, \ldots , \rho_{g-1}\}$$

che si dice periodo di m nella base a .

II caso.E' $(a, m) \in N_2$. Se allora è $g_0 = g\left(a, \frac{m}{m_0}\right)$ ed α è il numero dei resti che non si ripete, consideriamo i due insiemi

$$A = \{\rho_0, \rho_1, \dots, \rho_{\alpha-1}\}$$

$$P = \{\rho_\alpha, \rho_{\alpha+1}, \dots, \rho_{\alpha+ g_0 -1}\}$$

di coefficienti di divisibilità individuati rispettivamente dai resti fissi e dai resti periodici. In tale caso si dice che la successione dei resti o dei coefficienti di divisibilità è ***periodico – mista***. Gli insiemi A e P si dicono rispettivamente l'***antiperiodo*** ed il ***periodo*** del naturale m nella base a.
Quando (a, m) = 1 si dirà anche che l'antiperiodo è vuoto e che la successione dei coefficienti di divisibilità, e quindi dei resti, è ***periodico – semplice***.

Si ha il seguente
Teorema generale di divisibilità. ***Se $n = (c_t, c_{t-1}, \dots, c_0) \in N_1$ e se $m \in N_1^*$ allora condizione necessaria e sufficiente perché $m \mid n$ è che m divida l'intero relativo***

$$\sum_{k=o}^{t} c_k \rho_k$$

con $\rho_0, \rho_1, \dots, \rho_t$ primi t coefficienti di divisibilità del numero m in base a.

Dimostrazione. La dimostrazione segue dall'osservare che, essendo

$$n = \sum_{k=ot}^{t} c_k \cdot a^k$$

e

$$a^k \equiv \rho_k \quad (m)$$

vale la relazione

$$\sum_{k=ot}^{t} c_k \cdot a^k = \sum_{k=o}^{t} c_k \cdot \rho_k \quad (m)$$

che prova l'asserto.

Riportiamo ora una tabella che fornisce i coefficienti di divisibilità di alcuni interi della base 10 (dieci):

m	α	g_0	g	A	P
2	1	1		{1}	{0}
3			1		{1}
4	2	1		{1,2}	{0}
5	1	1		{1}	{0}
6	1	1		{1}	{-2}
7			6		{1,3,2,-1,-3,-2}
8	3	1		{1,2,4}	{0}
9			1		{1}
10	1	1		{1}	{0}
11			2		{1,-1}
12	2	1			
13			6		{1,-3,-4,-1,3,4}

Vediamo con qualche esempio come si possa costruire la tabella.

Esempio 1. Se a = 10 , m = 6 , risulta (a , m) = 2 .
Determiniamo allora i numeri:

$$m_0 \ , \ \frac{m}{m_0} \ , \alpha, g_0 .$$

Essendo m_0 il prodotto dei fattori primi di m , distinti e non distinti che dividono a, si ha :

$$m_0 = 2 \ , \ \frac{m}{m_0} = 3.$$

Essendo α il più piccolo elemento x di N_1 , tale che

$$a^x \equiv 0 \ (m_0) ,$$

si ha da :

$$10^x \equiv 0 \ (2),$$

che

$$\alpha = 1.$$

Dall'essere $g_0 = g \left(\frac{m}{m_0}, a \right) = g$ (3 , 10) il più piccolo elemento x di N_1, tale che sia:

$$10^x \equiv 1 \qquad (3) ,$$

segue $g_0 = 1$.

Per determinare ora i coefficienti di divisibilità occorre eseguire la divisione con resto delle sole prime due potenze di a per m e cioè degli interi 1 e 10 per 6.

Si ha :

$$1 = 0 \cdot 10 + 1 ; \qquad r_0 = 1$$
$$10 = 1 \circ 6 + 4 ; \qquad r_1 = 4.$$

Dividendo 6 per 2 si trova q = 3 ed essendo $r_1 > q$, si pone $\rho_1 = r_1 - m = 4 - 6 = -2$.
Si ha , dunque:

$$\rho_o = 1 \ , \ \rho_1 = -2$$

e quindi:

$$A = \{1\} \quad \text{(antiperiodo)} ,$$
$$P = \{-2\} \quad \text{(periodo)}.$$

Esempio 2. Sia $a = 10$, $m = 7$, essendo $(a , m) = (10 , 7) = 1$.
Determiniamo $g (m , a) = g (7 , 10)$.
Consideriamo:

$$10^x \equiv 1 \quad (7).$$

Poiché $g \mid \varphi(7)$ e poiché $\varphi(7) = 6$, può essere $g = 2$, oppure $g = 3$, oppure $g = 6$.

Ora $10^2 - 1 = 99$ non è divisibile per 7 e $10^3 - 1 = 999$ non è divisibile per 7.
Ne segue che

$$g = 6.$$

Occorre allora eseguire sei divisioni con resto e più precisamente dividere le potenze:

$$1, 10, 10^2, 10^3, 10^4, 10^5$$

per 7; così si ottengono rispettivamente i resti:

$$r_0 = 1, \ r_1 = 3, \ r_2 = 2, \ r_3 = 6, \ r_4 = 4, \ r_5 = 5.$$

Essendo $7 = 2 \cdot 3 + 1$ è $q = 3$ e $r_3 > q$, $r_4 > q$, $r_5 > q$;

onde si pone:

$$\rho_3 = 6 - 7 = -1, \quad \rho_4 = 4 - 7 = -3, \quad \rho_5 = 5 - 7 = -2,$$

mentre si pone:

$$\rho_0 = 1, \quad \rho_1 = 3, \quad \rho_2 = 2 .$$

Vediamo ora di dedurre alcuni:

Criteri di divisibilità

a) ***Un numero è divisibile per 2 se l' ultima cifra a destra è un numero pari (lo zero è considerato tale).***
Deve infatti essere , quale che sia

$$n = c_r \ c_{r-1} \ \ldots \ c_0$$

$$\rho_o c_o + \rho_1 c_1 + \ldots + \rho_r c_r \equiv 0 \qquad (2)$$

e cioè:

$$c_o \equiv 0 \ (2)$$

quindi c_o pari o nullo.

b) ***Un numero è divisibile per 3 se lo è la somma delle sue cifre.***
Essendo $\rho_i = 1$, $\forall$ i,
segue:

$$\Sigma c_k \equiv 0 \quad (3) ,$$

da cui l'asserto.

c) ***Un numero divisibile per 10 se l' ultima cifra è zero.***
Da

$$c_o \equiv 0 \quad (10),$$

segue che l'ultima cifra che soddisfa è $c_o = 0$.

Così continuando si può provare che:

d) ***Un numero divisibile per 5 se l'ultima cifra a destra è 0 o 5.***

e) ***Un numero è divisibile per 9 se lo è la somma delle cifre***.

f) ***Un numero è divisibile per 11 se tale è la differenza tra le cifre di indice pari e quelle di indice dispari.***

FINE DEL CAPITOLO III