Questo fascicolo contiene quasi tutti i prerequisiti aritmetici necessari per capire tutto quanto è stato fatto

Prerequisiti aritmetici

In quanto segue indicheremo con $\mathbb{Z}$ l'insieme degli interi positivi, negativi e lo zero e con $\mathbb{N}$ l'insieme dei numeri naturali (cioè gli interi positivi).

Iniziamo con alcune definizioni fondamentali

Def. di divisore

Siano $n, d \in \mathbb{Z}$. Si dice che d divide n, e si scrive $d \mid n$, se esiste $\delta \in \mathbb{Z}$ tale che $n = d\delta$.

Def. di numero primo

Un numero naturale $n > 1$ si dice primo se i suoi soli divisori positivi sono 1 ed n.

Ogni numero non primo verrà detto composto

Il numero 1 non è né primo né composto.

Esempi

I numeri 3, 5, 7, 23 e 101 sono primi. Il numero 21 è composto, infatti $21 = 3 \cdot 7$. Anche 105 è composto, infatti $105 = 3 \cdot 5 \cdot 7$. Inoltre $35 \mid 105$, infatti $105 = 35 \cdot 3$

Osservazione 1

Gli esempi che abbiamo fatto sono banali: infatti i numeri considerati sono "piccoli". Stabilire se numeri "grandi" sono primi non è uno scherzo.

Non è difficile dimostrare il seguente

Teorema 1

Ogni numero naturale $n>1$ è rappresentabile come prodotto di primi (si intende che se n è primo il prodotto è ridotto ad un solo fattore).

Dimostrazione

Ragioniamo per induzione. È immediato verificare che il teorema vale per i primi numeri naturali. Si ha infatti

$$2=2,\ 3=3,\ 4=2.2,\ 5=5,\ 6=2.3,\ 7=7,\ 8=2.2.2,$$

$$9=3.3,\ 10=2.5 \text{ - - -}$$

Supponiamo quindi che il teorema valga per ogni naturale $m \le n-1$ e dimostriamo che allora vale anche per n. Infatti se n è primo non c'è niente da dimostrare, se n è composto si ha

$$1)\quad n = \alpha\delta$$

con $1<\alpha\le n-1$, $1<\delta\le n-1$.

Ma, per ipotesi di induzione, sia α che δ sono rappresentabili come prodotto di primi: quindi sostituendo nella 1) si ottiene una rappresentazione di n come prodotto di primi. Ciò prova il teorema.

Il teorema 1 può essere perfezionato: vale infatti il seguente

Teorema fondamentale dell'Aritmetica.

Ogni numero naturale $n>1$ è rappresentabile come prodotto di primi in modo unico (a parte l'ordine dei fattori).

Non dimostreremo (per il momento) questo teorema.

È però sufficiente il teorema 1 per dimostrare il seguente importante risultato.

Teorema 2

I numeri primi sono infiniti

Dimostrazione

Sia $2, 3, 5, 7, \ldots, P$ la successione dei primi fino al primo P. Definiamo il numero N come

$$2) \quad N = (2.3.5.7\ldots.P) + 1$$

ed osserviamo che nessun primo $p \leq P$ divide N. Infatti se fosse $p|N$ si avrebbe anche

$$3) \quad p\left(\frac{N}{p} - \frac{2.3.5\ldots.P}{p}\right) = 1$$

con $\left(\frac{N}{p} - \frac{2.3.5\ldots.P}{p}\right)$ intero. Quindi p dovrebbe dividere 1 e ciò è assurdo.

D'altronde N o è primo o è esprimibile come prodotto di primi (vedi teorema 1): dunque esistono primi diversi da $2, 3, 5, \ldots, P$ e quindi maggiori di P. Ciò prova il teorema.

Il teorema fondamentale dell'Aritmetica ha molte importanti conseguenze. Mettiamone in luce una che useremo presto. Si tratta della seguente

Proposizione 1

Se $d|n$, nella fattorizzazione prima di d posso no comparire solo primi p che compaiono nella fattorizzazione prima di n, con un esponente minore od uguale a quello che hanno in n.

Dim.

Se $d|n$ si ha

$$4) \quad n = d\delta$$

per un certo $\delta \geq 1$.

Se nella fattorizzazione di d esistesse un primo p che non compare in quella di n, per la 4) si otterrebbero due diverse fattorizzazioni per n (contro il teorema fondamentale).

Lo stesso capiterebbe se si supponesse che

$n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ con i p_j primi distinti e $\alpha_j \geq 1$, $\forall j = 1, \dots, k$

e $d = p_1^{\beta_1} q_1^{\beta_2} \cdots q_s^{\beta_s}$ con $\beta_1 > \alpha_1$ e i q_i primi distinti e diversi da p_1, $\beta_i \geq 1$, $i = 1, \dots, s$. Infatti per la 4) si avrebbe

$$5) \quad \frac{n}{p_1^{\alpha_1}} = p_2^{\alpha_2} \cdots p_k^{\alpha_k} = p_1^{\beta_1 - \alpha_1} p_1^{\beta_2} \cdots q_s^{\beta_s} \cdot \delta$$

con $\beta_1 - \alpha_1 \geq 1$. Dunque il numero $m = \frac{n}{p_1^{\alpha_1}}$ avrebbe due fattorizzazioni distinte, una in cui compare p_1 e l'altra in cui non compare.
Ciò dimostra la proposizione 1.

Osservazione 2

La proposizione 1 ci permette di caratterizzare i divisori di n, se è nota la fattorizzazione prima di n. Infatti se $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$, con i p_j primi distinti e gli $\alpha_j \geq 1$, per $j = 1, \ldots, k$, possiamo dire che $d \mid n$ se e solo se $d = p_1^{\beta_1} \cdots p_k^{\beta_k}$ con $0 \leq \beta_j \leq \alpha_j$ per ogni $j = 1, \ldots, k$.

Def. di massimo comun divisore.
Dati due naturali a e b si dice massimo comun divisore di a e b, appunto il massimo divisore comune ad a e b (e si indica con (a,b)).

Osservazione 3

La precedente osservazione 2 che caratterizza i divisori di un naturale n, ci permette subito di dire che (a,b) è costituito dal prodotto di tutti i fattori primi comuni alle due fattorizzazioni di a e b, presi con il minimo esponente.
Se non esistono fattori primi comuni ad a e b allora si ha $(a,b) = 1$ ed a e b si dicono

sono relativamente primi. Vedremo poi che esiste un metodo (algoritmo euclideo) molto efficiente per calcolare (a,b), metodo che non fa riferimento alla fattorizzazione prima.

—

Introduciamo ora un concetto fondamentale, quello di congruenza.

Congruenze

Dati due numeri interi $a, b \in \mathbb{Z}$ ed un numero naturale m (detto modulo) si dice che a è congruo b modulo m e si scrive

$$6) \quad a \equiv b \pmod{m}$$

se $m \mid (a-b)$.

Osserviamo che la 6) vale se e solo se esiste $k \in \mathbb{Z}$ tale che

$$7) \quad a = b + mk$$

Dunque una congruenza modulo m è un'equaglianza a meno di multipli di m.

Il segno $\equiv$ che indica la congruenza è molto simile a quello di equaglianza $=$, ed è stato scelto da Gauss proprio per sottolineare le analogie tra eguaglianza e congruenza. In effetti le congruenze hanno molte delle proprietà

delle congruenze, come chiarisce la proposizione seguente.

Proposizione 2.
Due congruenze rispetto allo stesso modulo possono essere sommate e moltiplicate membro a membro, come fossero equazioni. Vale infatti l'implicazione seguente:

$$\text{a)} \begin{cases} a \equiv b \pmod m \\ c \equiv d \pmod m \end{cases} \Rightarrow \begin{cases} a+c \equiv b+d \pmod m \\ ac \equiv bd \pmod m \end{cases}$$

Dimostrazione
L'ipotesi ci dice che $a = b + mk$ e $c = d + mh$ con $k, h \in \mathbb{Z}$. Sommando membro a membro otteniamo $a + c = b + d + m(k+h)$ e moltiplicando $ac = bd + mt$, dove $k+h$ e $t \in \mathbb{Z}$.
Ciò prova la tesi.

Corollario
Da $a \equiv b \pmod m$ seguono $a^n \equiv b^n \pmod m$ (per ogni naturale $n \geq 1$) e anche $P(a) \equiv P(b) \pmod m$ dove $P(x)$ è un qualunque polinomio a coefficienti interi.

Dimostrazione
Prendendo $c = a$, $d = b$ nella a) della precedente proposizione si ottiene $a^2 \equiv b^2 \pmod m$ e quindi, iterando il ragionamento si ha

$a^n \equiv b^n \pmod m$. Per ottenere il secondo risultato basta osservare che se $P(x) = \alpha_n x^n + \alpha_{n-1} x^{n-1} + \dots + \alpha_1 x + \alpha_0$ con $\alpha_j \in \mathbb{Z}$, $\forall j = 0, 1, \dots, n$, da $a \equiv b \pmod m$ segue $a^j \equiv b^j \pmod m$, che moltiplicata per la congruenza ovvia $\alpha_j \equiv \alpha_j \pmod m$ ci dà $\alpha_j a^j \equiv \alpha_j b^j \pmod m$ per ogni $j = 0, 1, \dots, n$. Sommando su j si ottiene

$$P(a) \equiv \sum_{j=0}^{n} \alpha_j a^j \equiv \sum_{j=0}^{n} \alpha_j b^j \equiv P(b) \pmod m.$$

Ciò dimostra il corollario.

—

Vediamo ora alcune interessanti applicazioni che illustrano come il precedente corollario possa essere utilizzato.

Le regole di divisibilità per 3, 9, 11 (in base 10)

L'usuale rappresentazione di un numero in base 10 è in realtà del tipo

$$9) \quad n = c_k 10^k + c_{k-1} 10^{k-1} + \dots + c_1 10^1 + c_0$$

dove le cifre c_j sono comprese tra 0 e 9 e $c_k \neq 0$.

In pratica si scrive semplicemente $n = c_k c_{k-1} \dots c_1 c_0$.

Se poniamo $P(x) = c_k x^k + c_{k-1} x^{k-1} + \dots + c_1 10^1 + c_0$ dalla congruenza $10 \equiv 1 \pmod 9$ segue, per il precedente corollario $P(10) \equiv P(1) \pmod 9$ che equivale a

$$10) \quad n \equiv c_k + c_{k-1} + \dots + c_1 + c_0 \pmod 9$$

Dalla 10) segue immediatamente l'equivalenza

$$11)\quad 9 \mid n \iff 9 \mid (c_k + c_{k-1} + \dots + c_1 + c_0)$$

che è, per l'appunto la regola di divisibilità per 9.

Se consideriamo la congruenza $10 \equiv 1 \pmod 3$, ragionando allo stesso modo otteniamo

$$12)\quad 3 \mid n \iff 3 \mid (c_k + c_{k-1} + \dots + c_1 + c_0)$$

e se invece partiamo da $10 \equiv -1 \pmod{11}$ da $P(10) \equiv P(-1) \pmod{11}$ otteniamo

$$13)\quad 11 \mid n \iff 11 \mid \left(\sum_{h=0}^{k} c_h (-1)^h\right)$$

Le 12) e 13) sono le regole di divisibilità per 3 e per 11, rispettivamente.
Ad esempio, se $n = 9581$, dato che $11 \mid (9 - 5 + 8 - 1) = 11$ si ha che $11 \mid 9581$, mentre $3 \nmid 9581$.

—

La legge di cancellazione per le congruenze

Non sempre un fattore può essere cancellato da ambo i membri di una congruenza: ad esempio se nella congruenza $6 \cdot 7 \equiv 6 \cdot 2 \pmod{10}$ cancelliamo il fattore 6 (senza intervenire nel modulo) otteniamo $7 \equiv 2 \pmod{10}$, che è falsa. La questione è chiarita dalla seguente

Proposizione 3 (legge di cancellazione)
Vale l'implicazione seguente

$$14)\quad ca \equiv cb \pmod m \implies a \equiv b \pmod{\frac{m}{(c,m)}}$$

In altre parole un fattore può essere cancellato da ambo i membri di una congruenza se si divide il modulo per il massimo comun divisore tra il modulo stesso ed il fattore che si cancella.
In particolare se $(c,m)=1$, il fattore si può cancellare.

Dimostrazione

L'ipotesi ci dice che $ca = cb + mk$ con $k \in \mathbb{Z}$.
Dunque si ha anche, posto $d=(c,m)$,

$$15) \quad \frac{c}{d} d\, a = \frac{c}{d} \cdot d\, b + \frac{m}{d} d\, k$$

da cui segue $\frac{c}{d} a = \frac{c}{d} b + \frac{m}{d} k$ che equivale a

$$16) \quad \frac{c}{d}(a-b) = \frac{m}{d} k$$

Ma $\left(\frac{c}{d}, \frac{m}{d}\right) = \left(\frac{c}{(c,m)}, \frac{m}{(c,m)}\right) = 1$ e pertanto dalla 16) segue, per il teorema fondamentale dell'Aritmetica

$$17) \quad \frac{m}{d} \mid (a-b)$$

cioè $a \equiv b \pmod{\frac{m}{d}}$.
Ciò prova la proposizione.

—

Esempio.
Dato che $(6,10)=2$ da $6 \cdot 7 \equiv 6 \cdot 2 \pmod{10}$ segue $7 \equiv 2 \pmod{\frac{10}{2}}$, cioè $7 \equiv 2 \pmod 5$, che è corretta.

Def. di sistema completo di resti

Assegnato un modulo $m \geq 1$, si chiama sistema completo di resti modulo m un qualunque insieme di m interi a due a due incongruenti modulo m.

Esempi

Sia $m = 7$. I numeri $0, 1, 2, 3, 4, 5, 6$ costituiscono un sistema completo di resti modulo 7. Anche i numeri $-3, -2, -1, 0, 1, 2, 3$ costituiscono un sistema completo di resti modulo 7, così come i numeri $14, 1, 23, 24, 32, 54, 48$ (verificare).

Per ogni modulo m, con $m \geq 1$, il sistema $0, 1, 2, \ldots, m-1$ si chiama il sistema dei minimi resti positivi.

Vale la seguente

Proposizione 4

Se $(a, m) = 1$ quando x descrive un sistema completo di resti modulo m anche ax lo descrive.

Dimostrazione

Sia $x_1, x_2, \ldots, x_m$ il sistema completo di resti modulo m descritto da x. Si ha

$$18) \quad ax_i \equiv ax_j \pmod{m} \iff x_i \equiv x_j \pmod{m}$$

per la legge di cancellazione (infatti $(a, m) = 1$ per ipotesi).

La 18) prova che gli m numeri $ax_1, ax_2, \dots, ax_m$ sono a due a due incongrui modulo m e quindi costituiscono a loro volta un sistema completo di resti modulo m. Ciò prova la proposizione.

Esempio

Sia $m=6$ e $a=\bar{5}$. Si ha $(a,m)=(\bar{5},6)=1$: se $x_1=0$, $x_2=1$, $x_3=2$, $x_4=3$, $x_5=4$, $x_6=\bar{5}$ si ha

$\bar{5}x_1=0$, $\bar{5}x_2=\bar{5}$, $\bar{5}x_3=10$, $\bar{5}x_4=15$, $\bar{5}x_5=20$, $\bar{5}x_6=25$

ed i numeri $0, \bar{5}, 10, 15, 20, 25$ costituiscono anche un sistema completo di resti modulo 6.

Infatti, modulo 6 si ha $0\equiv 0$, $\bar{5}\equiv\bar{5}$, $10\equiv 4$, $15\equiv 3$, $20\equiv 2$, $25\equiv 1$ e ritroviamo $0, \bar{5}, 4, 3, 2, 1$, cioè una permutazione di $0, 1, 2, 3, 4, \bar{5}$.

Se cade l'ipotesi $(a,m)=1$ il risultato è falso.

Se, ad esempio, $m=6$ e $a=2$ si ottiene

$2\cdot 0=0$, $2\cdot 1=2$, $2\cdot 2=4$, $2\cdot 3=6$, $2\cdot 4=8$, $2\cdot\bar{5}=10$

e modulo 6 si ha la successione

$$0, 2, 4, 0, 2, 4$$

che non costituisce affatto un sistema completo di resti modulo 6.

L'algoritmo della divisione euclidea

Dati $a \in \mathbb{Z}$ e $m \in \mathbb{N}$ esiste un'unica coppia di interi q ed r, con $0 \leq r < m$, tale che

$$19) \quad a = mq + r$$

Dimostrazione

Per ottenere insieme esistenza e unicità basta osservare che a è compreso tra due successivi multipli di m, nel senso che

$$20) \quad mq \leq a < m(q+1)$$

e porre $r = a - mq$.

Vale anche la seguente

Proposizione 5

Si ha $a \equiv b \pmod m$ se e solo se a e b divisi per m danno lo stesso resto.

Dimostrazione

Dividiamo a e b per m ottenendo

$$a = mq_1 + r_1 \quad , \quad \text{con } 0 \leq r_1 < m$$
$$b = mq_2 + r_2 \quad , \quad \text{con } 0 \leq r_2 < m$$

Sottraendo membro a membro otteniamo

$$21) \quad a - b = m(q_1 - q_2) + (r_1 - r_2)$$

dove $|r_1 - r_2| < m$

Se $r_1 = r_2$ la 21) ci dice che $m \mid (a-b)$, cioè $a \equiv b \pmod m$. Se viceversa $a \equiv b \pmod m$ deve (anche essere $m \mid (a-b)$ e quindi per la 21) si deve avere $m \mid (r_1 - r_2)$, cioè $r_1 = r_2$. Ciò prova la proposizione.

Congruenze lineari

Si chiama congruenza lineare una congruenza del tipo

$$22) \quad ax \equiv b \pmod m \qquad \begin{pmatrix} a, b \in \mathbb{Z} \\ m \in \mathbb{N} \end{pmatrix}$$

dove a, b ed m sono assegnati e si cercano i numeri $x \in \mathbb{Z}$ che soddisfano la 22). È chiaro che se la congruenza 22) ha una soluzione x_0 ne ha infinite, infatti tutti gli $x \equiv x_0 \pmod m$ sono ancora soluzioni. Infatti se $x \equiv x_0 \pmod m$ si ha $x = x_0 + mk$ con $k \in \mathbb{Z}$ e quindi $ax = a(x_0 + mk) = ax_0 + amk = b + mh + mak = b + m(h + ak)$ e quindi x è soluzione della 22). Per questo motivo verranno considerate distinte due soluzioni della congruenza 22) solo se sono incongrue modulo m. Vale il seguente importante

Teorema 3

Se $(a, m) = 1$ la congruenza lineare

$$23) \quad ax \equiv b \pmod m$$

ha una sola soluzione modulo m.

Se $(a,m)=d>1$ e $d \nmid b$ (la 23) non ha nessuna soluzione. Se $(a,m)=d>1$ e $d \mid b$ (la 23) ha d soluzioni incongrue mod m, del tipo

24) $x_0,\ x_0+\frac{m}{d},\ x_0+2\frac{m}{d},\ \dots,\ x_0+(d-1)\frac{m}{d}$

dove x_0 è l'unica soluzione della congruenza

25) $\frac{a}{d}x \equiv \frac{b}{d} \pmod{\frac{m}{d}}$

Dimostrazione

Se $(a,m)=1$ quando x descrive un sistema completo di resti modulo m anche ax lo descrive, quindi esiste un solo valore x_0 tale che

$$ax_0 \equiv b \pmod m$$

Ciò prova il primo caso considerato.

Se invece $(a,m)=d$ e $d \nmid b$ (la 23) non ha nessuna soluzione: infatti se esistesse una soluzione x si avrebbe

$$ax = b+mk \quad \text{con } k \in \mathbb{Z}$$

che implica $ax-mk = d\left(\frac{a}{d}x-\frac{m}{d}k\right)=b$

da cui segue $d \mid b$, contro l'ipotesi.

Ci resta da considerare il terzo caso, cioè $(a,m)=d>1$ e $d \mid b$. In questo caso la 23) è equivalente a

24) $\frac{a}{d}x \equiv \frac{b}{d} \pmod{\frac{m}{d}}$

dove ora $\left(\frac{a}{d}, \frac{m}{d}\right) = 1$. Si ricade quindi nel primo caso considerato e la 24) ha una sola soluzione mod $\frac{m}{d}$, diciamo x_0 con $0 \le x_0 < \frac{m}{d}$.
Osserviamo che i numeri

25) $x_0,\ x_0 + \frac{m}{d},\ x_0 + 2\frac{m}{d},\ \dots,\ x_0 + (d-1)\frac{m}{d}$

soddisfano la 24) e quindi anche la 23).
Inoltre i numeri in 25) sono a due a due incongrui modulo m, infatti

26) $x_0 + i\frac{m}{d} \equiv x_0 + j\frac{m}{d} \pmod{m} \iff i \equiv j \pmod{d}$

e quindi sono soluzioni distinte di 23).
Inoltre, sempre per la 26), non ci sono altre soluzioni di 23).
Ciò prova completamente il teorema.

Esempio (illustrativo del precedente teorema).
Consideriamo la congruenza

$3x \equiv 1 \ (10)$

Dato che $(3,10) = 1$ siamo nel primo caso: quindi c'è una sola soluzione mod 10. Vediamo quale: consideriamo i numeri $3x \pmod{10}$ con $x = 0, 1, \dots, 9$

$x = 0, 1, 2, 3, 4, 5, 6, 7, 8, 9$
$3x = 0, 3, 6, 9, 12, 15, 18, 21, 24, 27$
$3x \bmod 10 = 0, 3, 6, 9, 2, 5, 8, (1), 4, 7$

Dunque l'unica soluzione mod 10 è $x = 7$.

Consideriamo ora la congruenza

$$12x = 3 \pmod{26}$$

Dato che $(12, 26) = 2$ e $2 \nmid 3$ la congruenza non ha nessuna soluzione (secondo caso contemplato).

Consideriamo infine la

$$27) \quad 15x \equiv 6 \pmod{24}$$

Dato che $(15, 24) = 3$ e $3 \mid 6$ ci sono tre soluzioni distinte. La 27) è equivalente a

$$28) \quad 5x \equiv 2 \pmod{8}$$

ed ora $(5, 8) = 1$ e quindi quest'ultima congruenza ha una sola soluzione mod 8, si ha

$$x = 0, 1, 2, 3, 4, 5, 6, 7$$
$$5x = 0, 5, 10, 15, 20, 25, 30, 35$$
$$5x \bmod 8 = 0, 5, (2), 7, 4, 1, 6, 3$$

e quindi 2 è la sola soluzione (mod 8) di 28). Applicando la formula 24) con $x_0 = 2$, $m = 24$ $d = 3$ otteniamo che i numeri

$$2, \quad 2 + 8, \quad 2 + 2 \cdot 8$$

cioè la terna

$$2, 10, 18$$

fornisce tutte e sole le soluzioni di 27).

La funzione φ di Eulero

Per ogni $n \geq 1$ si definisce $\varphi(n)$ il numero dei naturali k con $1 \leq k \leq n$ che sono relativamente primi con n. In simboli

$$\varphi(n) = \#\{k \in \mathbb{N} : 1 \leq k \leq n, (k,n) = 1\}$$

(Ricordiamo che se A è un insieme finito con il simbolo $\#A$ si indica il numero di elementi di A).

Esempi

Sia $n = 6$: allora $\varphi(n) = 2$. Infatti tra i numeri $k = 1, 2, 3, 4, 5, 6$ solamente 1 e 5 sono relativamente primi con 6. Sia $n = 7$: in questo caso si ha $\varphi(7) = 6$, infatti tra i numeri $k = 1, 2, 3, 4, 5, 6, 7$ solamente 7 non è relativamente primo con 7. Ciò evidentemente accade per ogni primo p, nel senso che se p è primo si ha $\varphi(p) = p - 1$.

Definizione di sistema ridotto di resti

Un qualunque insieme di $\varphi(m)$ numeri a due a due incongrui modulo m e relativamente primi con m si chiama un sistema ridotto di resti modulo m.

Esempio

Se dal sistema completo di resti modulo 12 eliminiamo i numeri che non sono relativamente primi con 12, cioè

~~1~~, 2, ~~3~~, 4, 5, ~~6~~, 7, ~~8~~, ~~9~~, 10, 11, ~~12~~

ci restano i numeri

1, 5, 7, 11

che sono un sistema ridotto di resti mod 12 (infatti $\varphi(12) = 4$). Evidentemente se a questi numeri aggiungiamo 12 (o un multiplo di 12) otteniamo ancora un sistema ridotto di resti modulo 12. Ad esempio

13, 17, 19, 23

è ancora un sistema ridotto di resti mod 12.

Se prendiamo $m = 9$, un sistema completo di resti modulo 9 è

1, 2, 3, 4, 5, 6, 7, 8, 9

ed un sistema ridotto è

1, 2, 4, 5, 7, 8

(notare che $\varphi(9) = 6$). Se a quest'ultimo sistema aggiungiamo 9 (o multipli di 9) otteniamo ancora un sistema ridotto di resti mod 9. Ad esempio è tale il sistema

19, 20, 22, 23, 25, 26

(ho aggiunto $18 = 2 \cdot 9$ ad ogni elemento).

Vale la seguente

Proposizione 5

Se $(a, m) = 1$ quando x descrive un sistema ridotto di resti modulo m anche ax lo descrive

Dimostrazione

Sia $x_1, x_2, \ldots, x_{\varphi(m)}$ il sistema ridotto di resti mod m descritto da x. Si ha

$$29) \quad ax_i \equiv ax_j \pmod m \iff x_i \equiv x_j \pmod m$$

per la legge di cancellazione (infatti $(a,m)=1$ per ipotesi). Quindi i $\varphi(m)$ numeri $ax_1, ax_2, \ldots, ax_{\varphi(m)}$ sono a due a due incongrui modulo m: inoltre si ha $(ax_i, m) = 1$, poiché $(a,m) = (x_i, m) = 1$. Ciò prova la tesi.

Osservazione

La proposizione 5) è l'analogo della proposizione 4) a pag 11, riguardante il sistema completo di resti mod m, anziché quello ridotto.

Illustriamo la precedente proposizione 5 con un esempio.

Esempio.

Sia $m = 15$, $a = 4$, quindi $(a,m) = (4, 15) = 1$, come deve essere.

Consideriamo un sistema ridotto di resti mod 15, precisamente

$$x = 1, 2, 4, 7, 8, 11, 13, 14$$

Si tratta di $\varphi(15) = \varphi(3 \cdot 5) = \varphi(3)\varphi(5) = 2 \cdot 4 = 8$ numeri, come deve essere. Consideriamo poi

$$4x = 4, 8, 16, 28, 32, 44, 52, 56$$

$$4x \bmod 15 = 4, 8, 1, 13, 2, 14, 7, 11$$

e questi ultimi sono una permutazione del precedente sistema ridotto di resti mod 15.

Dimostriamo ora un importante teorema, precisamente il

Teorema di Eulero - Fermat

Se $(a, m) = 1$ si ha $a^{\varphi(m)} \equiv 1 \pmod m$.

Dimostrazione

Per la precedente proposizione 5, quando x descrive un sistema ridotto di resti mod m, anche ax lo descrive. Quindi se indichiamo con $x_1, x_2, \dots, x_{\varphi(m)}$ il sistema ridotto di resti descritto da x, esiste una permutazione

$$f : \{1, 2, \dots, \varphi(m)\} \longrightarrow \{1, 2, \dots, \varphi(m)\}$$

$$i \longrightarrow f(i)$$

tale che $a x_i \equiv x_{f(i)} \pmod m$, per $i = 1, 2, \dots, \varphi(m)$

Moltiplicando membro a membro queste congruenze otteniamo

$$30)\quad (ax_1)(ax_2)\cdots(ax_{\varphi(m)}) \equiv x_{f(1)}\, x_{f(2)} \cdots x_{f(\varphi(m))} \pmod m$$

cioè

$$31)\quad a^{\varphi(m)}\, x_1 x_2 \cdots x_{\varphi(m)} \equiv x_1 x_2 \cdots x_{\varphi(m)} \pmod m$$

dato che l'applicazione f è una permutazione. Ma $(x_i, m) = 1$ per ogni $i = 1, 2, \ldots, \varphi(m)$, e quindi $(x_1 x_2 \cdots x_{\varphi(m)}, m) = 1$. Quindi, per la legge di cancellazione la 31) implica

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

cioè la tesi.

—

Il concetto di ordine di a mod m

Siano $(a, m) = 1$. Consideriamo le potenze successive di a, cioè

$$a^1, a^2, a^3, \ldots, a^k, \ldots$$

Per il teorema di Eulero–Fermat sappiamo che

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

Potrebbe però esserci un naturale $h < \varphi(m)$ tale che

$$32)\quad a^h \equiv 1 \pmod m$$

Siamo interessati al minimo $h \geq 1$ per il quale vale la 32). Questo numero sarà l'ordine di a modulo m. Diamo quindi la seguente

Definizione di ordine di a mod m

Siano a ed m relativamente primi, cioè $(a,m)=1$ si definisce ordine di a modulo m e si scrive $\sigma_m(a)$ il minimo intero $h \geq 1$ tale che vale la 32)

In simboli

$$33) \quad \sigma_m(a) = \min \{ h \geq 1 : a^h \equiv 1 \pmod m \}$$

Il teorema di Eulero-Fermat ci dice che $\sigma_m(a) \leq \varphi(m)$, $\forall a$ con $(a,m)=1$. Dimostriamo di più, cioè che $\sigma_m(a)$ divide $\varphi(m)$.

Vale infatti la seguente

Proposizione 6

Siano $(a,m)=1$ e sia $\sigma_m(a)$ l'ordine di a mod m. Se $a^s \equiv 1 \pmod m$ allora $\sigma_m(a) \mid s$. In particolare $\sigma_m(a) \mid \varphi(m)$.

Dimostrazione

Per brevità scriviamo $\sigma = \sigma_m(a)$. Dividendo s per σ si ottiene

$$s = \sigma q + r, \quad \text{con } 0 \leq r < \sigma$$

da cui segue

$$34) \quad a^s \equiv a^{\sigma q + r} \equiv (a^\sigma)^q \cdot a^r \pmod m$$

Ma $a^{\delta} \equiv 1 \pmod m$ e quindi anche $(a^{\delta})^q \equiv 1 \pmod m$: perciò dalle 3 4) e dall'ipotesi $a^s \equiv 1 \pmod m$ segue

$$35) \quad 1 \equiv a^s \equiv a^r \pmod m$$

che è assurda a meno che non sia $r = 0$ (infatti $0 \leq r < \delta$ e se fosse $r \geq 1$ la 35) sarebbe in contraddizione con la minimalità di δ).

Ciò prova la tesi.

—

La precedente proposizione ha il seguente

Corollario

Siano $(a, m) = 1$. Allora, ponendo per brevità $\delta = \delta_m(a)$,

i) $a^k \equiv a^h \pmod m \iff k \equiv h \pmod \delta$

ii) I numeri $1 = a^0, a^1, a^2, \dots, a^{\delta-1}$ sono a due a due incongrui mod m.

Dimostrazione

Dimostriamo l'equivalenza i).

Vediamo prima il verso $\Rightarrow$).

Supponiamo $k \neq h$, altrimenti l'implicazione è ovvia. Se $k > h$ (il che non lede la generalità) si ha

$$a^k \equiv a^h \pmod m \Rightarrow a^h (a^{k-h} - 1) \equiv 0 \pmod m,$$

ma quest'ultima congruenza implica, per la legge di cancellazione, $a^{k-h} \equiv 1 \pmod m$ da

cui segue, per la proposizione 6, $\sigma \mid (k-h)$, cioè la tesi $k \equiv h \pmod{\sigma}$.

Vediamo ora il verso ($\Leftarrow$. (supponendo $k>h$)

Dall'ipotesi $k \equiv h \pmod{\sigma}$ segue $k = h + t\sigma$ con $t \in \mathbb{N}$ e quindi $a^k \equiv a^h \cdot a^{t\sigma} \equiv a^h (a^\sigma)^t \equiv a^h \pmod{m}$, poiché $a^\sigma \equiv 1 \pmod{m}$, da cui la tesi.

La ii) è un'immediata conseguenza di i).

Definizione di radice primitiva

Siano $(a,m)=1$. Se $\sigma_m(a) = \varphi(m)$ si dice che a è radice primitiva mod m

Osservazione

Per la parte ii) del precedente corollario una radice primitiva mod m genera con le sue potenze successive

$$a^0, a^1, a^2, \ldots, a^{\varphi(m)-1}$$

un intero sistema ridotto di resti mod m.

Le precedenti definizioni ed i precedenti risultati sono molto importanti e penso che valga la pena di illustrarli con qualche esempio.

Esempi

Siano $a = 2$ e $m = 7$.

Il teorema di Eulero - Fermat ci dice che $a^6 \equiv 1 \pmod 7$, $\forall a = 1, 2, 3, 4, 5, 6$, quindi è anche $2^6 \equiv 1 \pmod 7$. Ma si ha $2^0 \equiv 1 (7)$, $2^1 \equiv 2 (7)$, $2^2 \equiv 4 (7)$, $2^3 \equiv 8 \equiv 1 (7)$ e quindi $\underset{7}{o}(2) = 3$. Ne segue che 2 non è radice primitiva modulo 7 (notare che $\underset{7}{o}(2) = 3 \mid 6 = \varphi(7)$, come deve essere).

Siano $a = 3$ e $m = 7$

In questo caso si ha $3^0 \equiv 1 (7)$, $3^1 \equiv 3$, $3^2 \equiv 2$, $3^3 \equiv 6$, $3^4 \equiv 18 \equiv 4$, $3^5 \equiv 12 \equiv 5$, $3^6 \equiv 15 \equiv 1 \pmod 7$, quindi 3 è radice primitiva mod 7, infatti $\underset{7}{o}(3) = 6 = \varphi(7)$. Notiamo anche che le potenze

$3^0, 3^1, 3^2, 3^3, 3^4, 3^5$ sono, modulo 7,

$1, 3, 2, 6, 4, 5$ e quindi

rappresentano un intero sistema ridotto di resti mod 7.

Siano $a = 4$, $m = 9 = 3^2$.

In questo caso si ha $4^0 \equiv 1 (9)$, $4^1 \equiv 4 (9)$, $4^2 = 16 \equiv 7 (9)$ $4^3 \equiv 28 \equiv 1 (9)$ e quindi $\underset{9}{o}(4) = 3$. Siccome $\varphi(9) = \varphi(3^2) = 3(3-1) = 6$, 4 non è radice primitiva mod 9. (Notare che $\underset{9}{o}(4) = 3 \mid 6 = \varphi(9)$).

Siano $a=2$, $m=9=3^2$

In questo caso si ha $2^0 \equiv 1 (9)$, $2^1 \equiv 2$, $2^2 \equiv 4$, $2^3 \equiv 8$, $2^4 \equiv 16 \equiv 7$, $2^5 \equiv 14 \equiv 5$, $2^6 \equiv 10 \equiv 1 (9)$. In questo caso si ha $o(2)_9 = 6 = \varphi(9)$ e pertanto 2 è radice primitiva mod 9, e le sue potenze successive generano l'intero sistema ridotto di resti mod 9.

Sia $m = 8 = 2^3$

In questo caso è $\varphi(8) = \varphi(2^3) = 2^2(2-1) = 4$, infatti il sistema ridotto di resti mod 8 è

$$1, 3, 5, 7$$

Notiamo che $1^1 \equiv 1 (8)$, $3^2 \equiv 9 \equiv 1 (8)$, $5^2 \equiv 25 \equiv 1 (8)$ e $7^2 \equiv 49 \equiv 1 (8)$. Dunque nessun elemento del sistema ridotto di resti mod 8 ha ordine massimo, cioè $\varphi(8) = 4$. Perciò non esistono radici primitive modulo 8.

Dopo questi esempi è spontaneo domandarsi per quali moduli $m \geq 1$ esistano radici primitive. La risposta è nel seguente teorema, che ci limiteremo ad enunciare

Teorema (importante)
Esistono radici primitive solo per i moduli $m = 1, 2, 4, p^\alpha$ e $2p^\alpha$, con p primo dispari ($\alpha \geq 1$).