TEORIA DEI NUMERI
DIVISIBILITA'

Consideriamo l'insieme Z dei numeri interi. Mentre è sempre possibile sommare, sottrarre e moltiplicare due numeri interi, non sempre esiste la divisione. Introduciamo quindi un'operazione chiamata **divisione con resto** (o **euclidea**) la cui esistenza è garantita dal seguente teorema:

Teorema Siano *a*, *b* numeri interi, $a \neq 0$. Allora esistono e sono unici due numeri interi *q*, *r* tali che:

(1) $b = a \cdot q + r$

(2) $0 \leq r < |a|$

q e *r* si chiamano *quoziente* e *resto* della divisione intera di *b* per *a.*

Dato che la divisione con resto restituisce due numeri (*q* e *r*), vengono utilizzate due scritture distinte.

In particolare si scriverà;

$$q = b \; div \; a$$

$$r = b \; mod \; a$$

Esempi:

$9 = 4 \cdot 2 + 1$ quindi 9 div 4 = 2 e 9 mod 4 = 1

$-15 = 7 \cdot (-3) + 6$ quindi -15 div 7 =-3 e -15 mod 7 = 6

Definizione: Si dice che *a* è un **divisore** di *b* (scriveremo $a|b$) se la divisione di *b* per *a* ha resto uguale a zero, cioè $b \; mod \; a = 0$ oppure $b = a \cdot q$.

Ogni numero intero diverso da zero ha qualche divisore: ±1, ±*b* sono divisori di *b.* Ce *n*e possono essere altri, oppure no.

Definizione: Un numero naturale N, con $N \geq 2$ si dice:
- **primo** se gli unici divisori di N sono 1 e N
- **composto** altrimenti

Esempio: Numeri primi: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, ...

Nasce il problema di come stabilire se un numero N sia primo.

Algoritmo elementare per stabilire se N è primo (già noto agli antichi greci)
Consideriamo tutti i possibili numeri tra 2 e N-1, $2 \leq d \leq (N-1)$, e dividiamo N per d:

- se la divisione ha resto zero per qualche d, N è composto
- se la divisione non ha mai resto zero, N è primo

Possibili scorciatoie

- Basta controllare tutti i numeri d maggiori di 1 e minori di radice di N ($1<d<\sqrt{N}$): infatti se N =d·d' con 1<d, d', allora d< $\sqrt{N}$ o d'<$\sqrt{N}$ altrimenti d·d'> $\sqrt{N} \cdot \sqrt{N}$ =N (assurdo)

Esempio: per stabilire se **101** è primo, si potrebbe controllare che non sia divisibile per tutti i numeri maggiori di 1 e minori di 11, cioè 2, 3, 4,…, 8, 9, 10

- Se d non funziona, inutile controllare per 2d, 3d, …… (quindi se il numero N non è divisibile per 2, è inutile controllare che sia divisibile per 4, 6, 8,...)

  Esempio: per controllare che **101** sia primo, basta vedere che non è divisibile per 2, 3, 5, 7.

I numeri primi sono **infiniti**.

Questa proprietà è già nota a Euclide, che ne dà una dimostrazione per assurdo.

Teorema: L'insieme dei numeri primi è infinito.

Dim:

Dimostriamo per assurdo:

supponiamo che l'insieme dei numeri primi sia finito e indichiamo con I questo insieme:

I = $\{2,3,5,7,...,p\}$, dove p è il numero primo più grande di tutti... Moltiplichiamo tra loro questi numeri e aggiungiamo 1 al risultato. Otteniamo così il numero:

$$N = 2\cdot 3\cdot 5\cdot .....\cdot p+1$$

Questo numero non è divisibile per 2 perché la sua espressione ci dice che dividendolo per 2 si ottiene come resto 1 (si tenga presente il teorema del quoziente e del resto e del fatto che N = $2\cdot k+1$ dove $k = 3\cdot 5\cdot ....\cdot p$).

Analogamente N non è divisibile per 3 (si avrebbe come resto 1) e non è divisibile per ogni numero dell'insieme I.

Questo è assurdo perché N (non appartenendo a I e non essendo quindi primo) deve essere rappresentabile come prodotto di fattori primi e quindi deve essere divisibile per uno dei numeri 1, 3, 5, …p.

L'assurdo nasce dall'aver supposto che **I** comprende tutti i numeri primi.

Proprietà Se p è un numero primo e a, b sono numeri interi diversi da 0, allora

$$(1) \qquad p\,|\,(a\cdot b) \;\Rightarrow\; p\,|\,a \text{ oppure } p\,|\,b\,.$$

Questa proprietà *caratterizza* i numeri primi, ossia vale anche viceversa: se per ogni coppia di numeri interi a, b diversi da 0 vale la (1), allora p è primo.

Osservazione: Se p non è primo, (1) non è vera: per esempio $6\,|\,(15\cdot 4)$, ma 6 non è divisore di 15 né di 4.

Teorema fondamentale dell'aritmetica:

Ogni naturale N ≥ 2 si decompone in uno e un solo modo (a meno dell'ordine dei fattori) come prodotto di numeri primi.

Esempio: $168 = 2^3\cdot 3\cdot 7$

Il numero dei divisori di un numero intero.

Se N è un numero intero maggiore di 1, indichiamo con $d(N)$ il numero dei divisori di N (inclusi 1 e N). Per esempio, $d(12) = 6$; infatti, i divisori di 12 sono 1, 2, 3, 4, 6, 12, in tutto sei.

Vediamo come si calcola $d(N)$.

Un numero naturale $N \geq 2$ è prodotto di potenze di numeri primi:

$$N = 2^{r_2}\cdot 3^{r_3}\cdot 5^{r_5}\cdot ....\cdot p^{r_p}$$

dove figurano soltanto i fattori p^{r_p} in cui l'esponente r_p è maggiore di zero; sarà quindi

$$N = p_1^{r_{p_1}} \cdot p_2^{r_{p_2}} \cdot \ldots \cdot p_h^{r_{p_h}}$$

per certi numeri primi $p_1, \ldots, p_h$ e altrettanti esponenti positivi $r_{p_1}, \ldots, r_{p_h}$.

Un numero m è divisore di N se si può fattorizzare *m* con gli stessi fattori primi di N o soltanto alcuni di essi, ma nessun altro, con esponenti minori o uguali di quelli che appaiono nella fattorizzazione di N; vale a dire che un divisore di N è:

$$m = p_1^{s_{p_1}} \cdot p_2^{s_{p_2}} \cdot p_3^{s_{p_3}} \cdot \ldots \cdot p_h^{s_{p_h}}$$

in cui, per $0 \le i \le h$, s_{p_i} è un numero intero tale che $0 \le s_{p_i} \le r_{p_i}$. Per ciascun fattore primo p_i ci sono dunque $r_{p_i} + 1$ modi di scegliere il corrispondente esponente per ottenere un divisore di *n*. Segue dunque che

$$d(N) = (r_{p_1} + 1) \cdot (r_{p_2} + 1) \cdot \ldots \cdot (r_{p_h} + 1)$$

Esempio: quanti sono i divisori del numero 72?

Sapendo che $72 = 2^3 \cdot 3^2$, i divisori di 72 si otterranno moltiplicando il 2 con gli esponenti da 0 a 3 (quattro possibilità) e il 3 con gli esponenti da 0 a 2 (tre possibili scelte), quindi in tutto i divisori sono $3 \cdot 4 = 12 = d(72)$.

Infatti, 72 è divisibile per $1 = 2^0 \cdot 3^0$, $2 = 2^1 \cdot 3^0$, $3 = 2^0 \cdot 3^1$, $4 = 2^2 \cdot 3^0$, $6 = 2^1 \cdot 3^1$, $8 = 2^3 \cdot 3^0$, $9 = 2^0 \cdot 3^2$, $12 = 2^2 \cdot 3^1$, $18 = 2^1 \cdot 3^2$, $24 = 2^3 \cdot 3^1$, $36 = 2^2 \cdot 3^2$, $72 = 2^3 \cdot 3^2$ cioè ha 12 divisori.

Massimo comun divisore e minimo comune multiplo

Definizione: dati *a, b* $\in N_0$, si dice **massimo comun divisore** di *a* e *b* il numero naturale *d* tale che:
- *d* è divisore di *a* e *b*
- ogni divisore comune di *a* e *b* è minore o uguale a *d*.

Osservazione: indicheremo *d* con (*a, b*)

Definizione: dati *a, b* $\in N_0$, si dice **minimo comune multiplo** di *a* e *b* il numero naturale $m \neq 0$ tale che:
- *m* è multiplo di *a* e *b*
- ogni multiplo comune $\neq 0$ di *a* e *b* è maggiore o uguale a *m*.

Osservazione: indicheremo con [*a, b*] il minimo comune multiplo di *a* e *b*.

Per la determinazione di (*a, b*) è possibile usare il **procedimento di Euclide** che deriva dalla validità dei seguenti enunciati:
assegnati due numeri *a* e *b* (supponendo $a \ge b$), eseguendo la divisione euclidea, siano *q* e *r* rispettivamente il quoziente e il resto, cioè *a=bq+r (dove 0≤r<b) (*)*, allora:

1. un intero *d* che sia divisore di *a* e *b* è divisore anche di *r*;
2. un intero *d* che sia divisore di *b* e di *r* è divisore anche di *a*.

Dimostrazione1: se *d* divide *a* allora *a = d a'* e se *d* divide *b* allora *b = d b'*. Sostituendo nella (*) si ottiene *d a'= d b' q+r* e ricavando *r*: *r = d a' –d b'q = d (a'-b'q)*
Questa relazione mostra che *d* divide *r*.
Dimostrazione 2: se *d* divide *b* allora *b = d b'* e se *d* divide *r* allora *r = d r'*. Sostituendo nella (*) si ottiene: *a= d b' q+d r' = d (b'q+r')*.
Questa relazione mostra che *d* divide *a*.

In base alla dimostrazione appena fatta, per trovare il M.C.D. tra a e b si procede nel seguente modo:

- si divide a per b e se il resto della divisione è zero, si prende $b = (a, b)$
- se il resto è diverso da zero, si considera $(a, b) = (b, r)$ [in pratica $(a, b) = (b, a \text{ mod } b)$]
- si divide ora b per r e se il resto r' è zero, r è il numero cercato
- se r' è diverso da zero, si cerca il M.C.D. della coppia r, r' cioè $(b, r) = (r, r')$
- ….
- La ricerca termina quando si trova per la prima volta il resto della divisione uguale a zero.

Questo procedimento prende il nome di **procedimento di Euclide** o **delle divisioni successive.**
Esempi:

- $(72,22)=2$
  Infatti: $72=22\cdot 3+6$ $22=6\cdot 3+4$ $6=4\cdot 1+2$ $4=2\cdot 2+0$ quindi $(72,22)=2$
- $(1253,27)=1$
- $(12,6)=6$

Quando due numeri hanno come M.C.D. 1, si dicono **primi tra loro** (oppure **coprimi**), cioè i numeri 1253 e 27 sono primi tra loro.

Proprietà: si potrebbe dimostrare che $(a, b)\cdot[a, b] = a\cdot b$ (°).

Osservazione: se è nota la fattorizzazione del numero in numeri primi, la ricerca del M.C.D. e del m.c.m. è semplice: per il m.c.m. si moltiplicano tutti i fattori comuni e non comuni con il massimo esponente; per il M.C.D. si moltiplicano tutti i fattori in comune con il più piccolo esponente (si consideri uguale a zero l'esponente dei fattori che non compaiono.)
Esempio: $72 = 2^3\cdot 3^2$
$22 = 2\cdot 11$
Quindi $(72,22)=2$
$[72,22]= 2^3\cdot 3^2\cdot 11=792$

Si osservi che $(72,22)\cdot [72,22] = 1584 = 72\cdot 22$ (cioè la proprietà (°)).

Teorema: per ogni M>0 si possono trovare M numeri consecutivi nessuno dei quali sia primo.
Dimostrazione: è sufficiente considerare:
$1\cdot 2\cdot 3\ldots\cdot M\cdot (M+1)+2$ divisibile per 2
$1\cdot 2\cdot 3\ldots\cdot M\cdot (M+1)+3$ divisibile per 3
……
$1\cdot 2\cdot 3\ldots\cdot M\cdot (M+1)+(M+1)$ divisibile per $(M+1)$

Osservazione: Il numero $1\cdot 2\cdot 3\ldots\cdot M\cdot (M+1) = (M+1)!$ si chiama fattoriale del numero $(M+1)$ ed è uguale al prodotto tra M+1 e tutti i numeri interi positivi che lo precedono ($5!=1\cdot 2\cdot \ldots\ldots\cdot 5=120$).

Esempio: per scrivere 11 numeri consecutivi tutti composti è possibile considerare:

$1\cdot 2\cdot 3\ldots\cdot 11\cdot 12 + 2 = 12!+2 = 479001602$ che è divisibile per 2
$1\cdot 2\cdot 3\ldots\cdot 11\cdot 12 + 3 = 12!+3 = 479001603$ che è divisibile per 3
.
.

$1\cdot 2\cdot 3\ldots\cdot 11\cdot 12+12 = 12!+12 = 479001612$ che è divisibile per 12.

Teorema di Bézout Dati due numeri *a* e *b,* sia *d* il loro M.C.D. (indichiamo $d = (a, b)$); allora esistono $n,m \in \mathbf{Z}$ tali che: $ma + nb = d$

Esempio: sia a = 44 e b= 13, d (44,13) =1; come si calcolano m e n?
Metodo delle divisioni successive
$44 = [13]\cdot 3 + [5]$
$13 = [5]\cdot 2 + [3]$
$5 = [3]\cdot 1 + [2]$
$[3] = [2]\cdot 1 + 1$
Torno indietro con i resti partendo dall'ultima uguaglianza:
$1 = 3 - 2\cdot 1 = 3\text{-}(5\text{-}3\cdot 1)\cdot 1 = 3\cdot 2\text{-}5\cdot 1 = 2\,(13\text{-}5\cdot 2)\text{-}5 = 5\,(\text{-}5)+2\cdot 13 = (44\text{-}13\cdot 3)\,(\text{-}5)+2\cdot 13 =$
$44\,(\text{-}5)+13\,(17) = 1$
Quindi m= -5 n=17. Infatti $-5\cdot 44 + 17\cdot 13 = -220 + 221 = 1$.

ESERCIZI DIVISIBILITA' CON SOLUZIONE

1) Quanti interi si possono scegliere al massimo fra 2 e 20 (estremi compresi) in modo che siano a due a due primi tra loro?
   Soluzione: prendiamo i numeri primi e precisamente 2, 3, 5, 7, 11, 13, 17, 19 quindi abbiamo 8 scelte possibili.

2) Si considerino i numeri naturali *n* di 3 cifre tali che verificano la seguente proprietà: le cifre di *n* sono tre numeri consecutivi in qualunque ordine (ad esempio 435 oppure 879). Quanti di questi numeri sono primi?
   Soluzione: nessuno perché la somma di tre numeri consecutivi è sempre multipla di 3. Infatti, siano x-1, x, x+1 i tre numeri consecutivi che sono le tre cifre di *n*. La somma sarà (x-1) + x + (x+1) = 3x cioè *n* è un multiplo di 3.

3) Qual è il più piccolo numero intero positivo che possiede esattamente 15 divisori?
   Soluzione: il numero sarà $2^4\cdot 3^2$=144.

4) Trovare i due divisori di $2^{48}-1$ compresi tra 60 e 70.
   Soluzione: usando i prodotti notevoli si ha:
   $2^{48}-1 = (2^{24}+1)(2^{24}-1) = (2^{24}+1)(2^{12}+1)(2^{12}-1) = (2^{24}+1)(2^{12}+1)(2^6+1)(2^6-1)$
   essendo $2^6+1 = 65$ e $2^6-1 = 63$ si ottengono 63 e 65 come soluzioni.

5) Qual è il più grande intero positivo *n* per il quale n^3+100 è divisibile per *n*+10.
   Soluzione: eseguendo la divisione si ottiene come resto -900 e come quoziente n^2-10*n*+100. Infatti,

$$\begin{array}{rl} n^3+100 & \mid \quad n+10 \\ \underline{-n^3-10n^2} & \mid \quad n^2-10n+100 \\ -10n^2+100 & \mid \\ \underline{+10n^2+100n} & \mid \\ 100n+100 & \mid \\ \underline{-100n-1000} & \mid \\ -900 & \mid \end{array}$$

Quindi si ha $n^3+100 = (n^2-10n+100)\cdot (n+10) - 900$ quindi il numero n^3+100 sarà divisibile per $(n+10)$ se 900 è multiplo di $n+10$. Per avere il più grande positivo n sarà proprio $900 = n+10$ cioè $n = 890$.

6) Trovare tutti i numeri a e b tali che $a^2 - 4b^2 = 45$.
Soluzione: $a^2 - 4b^2 = (a - 2b)(a + 2b) = 45$.
I divisori di 45 sono: d (45) = 6, cioè 45 ha 6 divisori.
Quindi il 45 si potrà ottenere come prodotto di 1 per 45, di 3 per 15, di 5 per 9, cioè si avrà
$\begin{cases} a-2b=1 \\ a+2b=45 \end{cases}$ oppure $\begin{cases} a-2b=3 \\ a+2b=15 \end{cases}$ oppure $\begin{cases} a-2b=5 \\ a+2b=9 \end{cases}$
che forniscono le tre coppie di soluzioni: (23,11) (9,3) e (7,1).

7) Per quale valore di n l'espressione $n^2 - 14n + 24$ è un numero primo?
Soluzione: fattorizzando il trinomio si ottiene $n^2 - 14n + 24 = (n - 2)(n - 12)$ quindi per essere un numero primo uno dei due fattori deve essere 1 oppure –1.
Nel primo caso si ha $n - 2 = 1$ quindi $n = 3$ che dà come risultato –9 (non accettabile) e $n - 12 = 1$ quindi $n = 13$ che dà come risultato 11 (numero primo).
Nel secondo caso si ha $n - 2 = -1$ cioè $n = 1$ che dà come risultato 11 e $n - 12 = -1$ cioè $n = 11$ che dà come risultato –9 (non accettabile).
Le soluzioni sono quindi $n = 1, 13$.

8) I numeri a e b sono interi positivi. Qual è il minimo valore di $a + b$ affinché $21ab^2$ e $15ab$ siano entrambi quadrati perfetti?
Soluzione: Se $21ab^2$ è un quadrato, anche $21a$ deve essere un quadrato.
Poiché $21\ a = 3 \cdot 7a$ e in un quadrato tutti gli esponenti dei fattori primi devono essere pari, a contiene i fattori *3* e *7* quindi il valore minimo di a che rende $21a$ un quadrato è proprio 21. Per quanto riguarda $15ab$ sostituendo $a = 21$ e fattorizzando si ha $3^2 \cdot 5 \cdot 7 \cdot b$ quindi il minimo valore di b che lo rende un quadrato è $b = 5 \cdot 7 = 35$. Allora $a + b = 56$.

9) Per quanti valori dell'intero positivo n l'espressione $\dfrac{5n+93}{n+7}$ è un intero positivo?
Soluzione: si ha $\dfrac{5n+93}{n+7} = \dfrac{5n+35+58}{n+7} = 5 + \dfrac{58}{n+7}$ quindi l'espressione sarà un intero positivo per i valori di n tali che $n + 7$ divide 58. Essendo $58 = 2 \cdot 29$, poniamo: $n + 7 = 2$, che restituisce la soluzione non accettabile $n = -5$ (n deve essere positivo); $n + 7 = 29$, cioè $n = 22$; $n + 7 = 58$, cioè $n = 51$. Quindi le soluzioni sono due: 22 e 51.

10) Determinare tutti gli interi n tali che $n^4 + 4$ sia un numero primo.
Soluzione: $n^4 + 4 = (n^2 + 2)^2 - 4n^2 = (n^2 + 2 + 2n)\ (n^2 + 2 - 2n)$. Il numero $(n^2 + 2 + 2n)$ è

sicuramente maggiore di 1, quindi, affinché il numero $n^4 + 4$ sia primo, deve essere $n^2 + 2 – 2n = 1$. Questo si ha solo per $n = 1$, che restituisce infatti il numero $1^4 + 4 = 5$, cioè un numero primo.

11) Siano *a, b, c* tre numeri positivi, dispari, distinti e minori di 100. Quanto può essere al massimo il loro massimo comun divisore?
Soluzione: se *d* è il M.C.D. di *a, b, c,* deve essere $a = xd$, $b = yd$ e $c = zd$, con *x, y, z* tutti dispari e distinti. I più piccoli valori di *x, y, z*, sono 1, 3, 5 e poiché $c = 5d < 100$, *d* sarà 19 (cui corrispondono $a = 19$, $b = 57$, $c = 95$).

12) Un numero è composto da 77 cifre tutte uguale a 7. Qual è il resto della divisione di questo numero per 101?
Soluzione: considerando che $77 \cdot (101) = 77 \cdot (100+1) = 7700+77 = 7777$ si può concludere che 7777 è multiplo di 101. Il numero di 77 cifre tutte uguali a 7 si può scrivere come somma: $7777 \cdot 10^{73} + 7777 \cdot 10^{69} + 7777 \cdot 10^{65} + \ldots\ldots\ldots + 7777 \cdot 10^5 + 7777 \cdot 10 + 7$ quindi il resto nella divisione per 101 è 7.

13) Dimostrare che $(a, a+1) = 1$, $(2a, 2a+2) = 2$, $(a+b, b) = (a, b)$, $(5a+3b, 13a+8b) = (a, b)$
(dove al solito (x, y) indica il massimo comun divisore dei numeri *x* e *y*).
Soluzione: le prime tre uguaglianze si ottengono banalmente dall'algoritmo di Euclide (eseguendo la divisione tra i due numeri e considerando il resto…).
L'ultima si ottiene sempre applicando l'algoritmo di Euclide e cioè eseguendo le divisioni seguenti:
$13a+8b = (5a+3b) \cdot 2 + (3a+2b)$
$5a+3b = (3a+2b) \cdot 1 + (2a+b)$
$3a+2b = (2a+b) \cdot 1 + (a+b)$
$2a+b = (a+b) \cdot 1 + a$, dalla quale si deduce che il M.C.D. cercato è $(a+b, a) = (a, b)$ (come risulta dalla terza relazione). Quindi $(5a+3b, 13a+8b) = (a, b)$.

Equazioni diofantee

Un'equazione diofantea è un'equazione algebrica a coefficienti interi in una o più incognite di cui si cercano soluzioni intere.

1. Equazioni diofantee di primo grado

a) In due incognite

Consideriamo l'equazione

$$123\,x + 57\,y = 8. \qquad (1)$$

Il luogo dei punti del piano di coordinate x e y descritto dalla (1) è una retta. Cerchiamo, se esistono, soluzioni x, y della (1) intere, cioè punti sulla retta che abbiano entrambe le coordinate intere.

In tale caso i coefficienti 123 e 57 sono entrambi divisibili per 3, quindi il membro di sinistra dell'equazione è divisibile per 3, per ogni valore intero di x e y. Invece il membro di destra è 8, che non è divisibile per 3. Quindi non esistono soluzioni intere della (1).

Più in generale, consideriamo l'equazione diofantea

$$\mathbf{ax + by = c, \quad (2)}$$

con *a, b, c* numeri interi. Un'equazione di questa forma si dice di *primo grado*. Se questa equazione possiede soluzioni, ogni numero *d* che divida[1] sia *a* che *b,* deve dividere anche *c*. In particolare, questo deve valere per il più grande tra i divisori comuni di *a* e *b*, cioè per il loro massimo comun divisore, indicato generalmente con (*a, b*). Abbiamo quindi scoperto che, affinché l'equazione (2) abbia soluzione, è necessario che *c* sia un multiplo di (*a, b*).

[1. Si dice che un numero *d* divide *a* se *a* è un multiplo intero di *d*; in formula $a = qd$, con *q* intero.]

Modifichiamo l'equazione (1) affinché possa avere soluzioni. Consideriamo ad esempio

$$123\,x + 57\,y = 9. \qquad (3)$$

Dato che (123, 57) = 3 e 9 è un multiplo di 3, questa equazione può avere soluzioni. Per vedere se effettivamente ne ha, è utile il seguente teorema:

TEOREMA DI BEZOUT

Se *A, B* sono interi e (*A, B*) è il loro massimo comun divisore, allora esistono due interi *h*, *k* tali che

$$hA + kB = (A, B).$$

Il Teorema di Bezout garantisce che esistono due interi *h*, *k* tali che $123h + 57k = 3$; moltiplicando questa equazione per 3, troviamo che $x = 3h$ e $y = 3k$ sono una soluzione della (3).

Il problema si riduce quindi a dimostrare il teorema di Bezout, con una dimostrazione che fornisca un metodo per calcolare *h* e *k*, basata sul seguente algoritmo:

L'Algoritmo di Euclide

Dati due interi positivi *a, b*, l'algoritmo di Euclide determina il loro massimo comun divisore (*a, b*). Si basa sulla divisione con resto di numeri interi.

Applichiamo l'algoritmo nel nostro caso, cioè agli interi $a = 123$ e $b = 57$.

Iniziamo con lo scrivere la divisione con resto del più grande tra i due per il più piccolo: il 57 nel 123 ci sta 2 volte e resta 9, in formula:

$$123 = 2 \cdot 57 + 9.$$

Nel caso generale (supponendo *a* maggiore di *b*): $a = q \cdot b + r$,

dove *q* è il quoziente della divisione e *r* il resto, ossia un intero compreso tra 0 e $b - 1$. L'identità appena scritta mostra che se un intero *d* divide sia *a* che *b*, deve dividere anche *r* (infatti $r = a - q \cdot b$). Analogamente, se un intero *d* divide sia *b* che *r*, deve dividere anche *a*. Quindi un numero è divisore comune di *a* e *b* se e solamente se è divisore comune di *b* e *r*.

Applicando questo ragionamento al più grande dei divisori comuni, deduciamo che (*a, b*) = (*b*, *r*), quindi ci siamo ricondotti a trovare il massimo comun divisore tra *b* e *r*, operazione più semplice, visto che si tratta di due numeri più piccoli dei precedenti. Inoltre l'argomento si può iterare, con *b*, *r* al posto di *a, b.*

Nel nostro caso, abbiamo che (123, 57) = (57, 9), e ripetendo la divisione con resto con questi nuovi numeri troviamo: $57 = 6 \cdot 9 + 3$, e proseguendo allo stesso modo $9 = 3 \cdot 3 + 0$.
L'algoritmo è concluso quando una divisione non ha resto; infatti, nelle divisioni successive i resti diminuiscono, quindi prima o poi deve comparire il resto 0. Dalle considerazioni fatte sopra sappiamo che (123, 57) = (57, 9) = (9, 3) = (3, 0) = 3, quindi il M.C.D. tra 123 e 57 è 3, cioè l'ultimo resto non nullo generato dall'algoritmo di Euclide.
Ovviamente il M.C.D. di due numeri si può trovare anche fattorizzandoli, ma in presenza di numeri molto grandi è molto difficile, mentre l'algoritmo di Euclide è piuttosto veloce.
L'algoritmo di Euclide è interessante non tanto come metodo per determinare il M.C.D., ma perché riscrivendo i passaggi al contrario è possibile risalire agli interi h e k del Teorema di Bezout.
Riscriviamo di seguito i passaggi dell'algoritmo, tralasciando l'ultimo:

$$(P1)\ 123 = 2 \cdot 57 + 9$$
$$(P2)\ 57 = 6 \cdot 9 + 3$$

Il nostro scopo è scrivere 3 come combinazione intera di 123 e 57, cioè come somma dei numeri 123 e 57 moltiplicati per opportuni coefficienti interi. Dalla seconda equazione possiamo scrivere 3 come combinazione intera di 57 e 9. Dalla prima possiamo ricavare 9 come combinazione intera di 123 e 57. Mettendole insieme, troviamo 3 come combinazione intera di 123 e 57. Vediamo i passaggi (vicino ad alcune delle uguaglianze è indicata la riga dell'algoritmo di Euclide utilizzata):

$$3 =_{(P2)} 57 - 6 \cdot 9 =_{(P1)} 57 - 6 \cdot (123 - 2 \cdot 57) = -6 \cdot 123 + 13 \cdot 57.$$

In conclusione,

$$3 = -6 \cdot 123 + 13 \cdot 57, \qquad (4)$$

quindi nel nostro caso i coefficienti di Bezout sono $h = -6$ e $k = 13$.

Soluzione generale. Moltiplicando per 3 l'uguaglianza (4) fornita dal Teorema di Bezout, troviamo che $x^* = -18$, $y^* = 39$ è una soluzione dell'equazione (3). Vediamo se ve ne sono altre e, in caso affermativo, determiniamole.
Se facciamo la sostituzione $x = x^* + x' = -18 + x'$, $y = y^* + y' = 39 + y'$, il primo membro dell'equazione (3) diventa

$$123x + 57y = 123(x^* + x') + 57(y^* + y') = 123x^* + 57y^* + 123x' + 57y' = 9 + 123x' + 57y',$$

dove abbiamo usato il fatto che x^*, y^* è una soluzione. Questa espressione deve essere uguale a 9, quindi troviamo che le nuove incognite x', y' devono risolvere l'equazione

$$123\,x' + 57\,y' = 0.$$

Poiché a secondo membro c'è lo zero, è semplice determinare le soluzioni intere di questa equazione. Infatti, ricaviamo la y' in funzione della x':

$$y' = -\frac{123}{57}x' = -\frac{41}{19}x'$$

dove abbiamo ridotto la frazione in modo da avere numeratore e denominatore primi tra loro. Il fatto che 41 e 19 siano primi tra loro implica che y' è un intero se e solamente se x' è un multiplo di 19 (questo è l'unico modo per semplificare il denominatore). Quindi $x' = 19n$, dove n è un intero arbitrario, da cui ricaviamo $y' = -41n$. Concludiamo che le soluzioni di (3) sono esattamente le coppie x, y della forma

$$x = -18 + 19n,\ y = 39 - 41n,$$

al variare di n fra tutti gli interi. Geometricamente, si tratta dei punti sulla retta di equazione $123x + 57y = 9$ ottenuti partendo dal punto $(-18, 39)$ e facendo n passi di lunghezza 19 verso destra (rispettivamente, verso sinistra) e n passi di lunghezza 41 verso il basso (rispettivamente, verso l'alto).
VERIFICA: $123(-18+19n)+57(39-41n) = -2214+2337n+2223-2337n = 9$.

Riassunto:

L'equazione diofantea di primo grado $\boldsymbol{ax + by = c}$, (5)

con *a, b, c* interi, possiede soluzioni se e solamente se *c* è un multiplo di (*a, b*). In questo caso, posto *c* = (*a, b*)·*q*, si usa l'algoritmo di Euclide per trovare le soluzioni *h*, *k* di *ha* + *kb* = (*a, b*), e si ha che *x** = *qh*, *y** = *qk* è una soluzione particolare di (5). Tutte le soluzioni sono date dalla formula

$$x = x^* + \frac{b}{(a,b)}n, \quad y = y^* - \frac{a}{(a,b)}n,$$

al variare di *n* tra tutti gli interi.

Esercizio 1
Risolvere, se è possibile, le seguenti equazioni diofantee:
3x + 6y = 22, 7x + 11y = 13, 3x − 4y = 29, 11x + 12y = 58, 153x − 34y = 51.

b) In tre incognite
Consideriamo l'equazione diofantea lineare in tre incognite

$$\boldsymbol{ax + by + cz = d} \qquad \textbf{(6)}$$

dove (*a*, *b*, *c*) divide *d*. [Ricorda: (*a*, *b*, *c*) = M.C.D. (*a*, *b*, *c*)]
Sotto la condizione scelta, la (6) è risolvibile; determiniamo le sue soluzioni associandole due equazioni diofantee lineari ciascuna in due incognite:

$$ax_1 + (b,c)x_2 = d, \quad (6_1)$$

$$by_1 + cy_2 = (b,c) \quad (6_2).$$

Essendo (*a*, (*b*, *c*)) = (*a*, *b*, *c*), la (6) è risolvibile se e solo se la (6_1) lo è. Inoltre, abbiamo già trovato che, se x_1^*, x_2^* è una soluzione di (6_1), allora tutte le sue soluzioni sono del tipo:

$$x_1 = x_1^* + \frac{(b,c)}{(a,b,c)}t, \quad x_2 = x_2^* - \frac{a}{(a,b,c)}t, \text{ al variare di t in } \boldsymbol{Z}.$$

Ma anche (6_2) è sempre risolvibile; sia y_1^*, y_2^* una sua soluzione; allora si può dimostrare che tutte le soluzioni di (6) sono del tipo:

$$x = x_1^* + \frac{(b,c)}{(a,b,c)}t,$$

$$y = y_1^* x_2^* - y_1^* \frac{a}{(a,b,c)}t + \frac{c}{(b,c)}s, \text{ al variare di } t, s \text{ in } \boldsymbol{Z}.$$

$$z = y_2^* x_2^* - y_2^* \frac{a}{(a,b,c)}t - \frac{b}{(b,c)}s,$$

Esempio
Determiniamo tutte le soluzioni dell'equazione diofantea x + 2y + 3z = 4.
Poiché (1, 2, 3) = 1 e 1 divide 4, l'equazione è risolvibile. Consideriamo le seguenti due equazioni diofantee lineari in due indeterminate: $x_1 + (2, 3)\, x_2 = 4$, ovvero $x_1 + x_2 = 4$, e $2y_1 + 3y_2 = 1$. Notiamo istantaneamente che (4, 0) è una soluzione della prima equazione e (–1, 1) una soluzione della seconda; pertanto le soluzioni dell'equazione data sono:

$$x = 4 + t,$$

$$y = t + 3s, \quad \text{al variare di } t, s \text{ in } \boldsymbol{Z}.$$

$$z = -t - 2s,$$

Ad esempio, per *s* = *t* = 0, abbiamo (4, 0, 0); per *s* = 0 e *t* = 1, (5, 1, -1); per *s* = 1 e *t* = 0, (4, 3, -2)….

Esercizio 2
Risolvere, se è possibile, le equazioni diofantee 3x + 12y − 9z = 15, 6x – 4y +8z = 12.

2. Equazioni diofantee di secondo grado

Per quanto riguarda le equazioni diofantee di secondo grado, e più in generale di grado superiore al primo, purtroppo, a differenza del primo grado, non esistono metodi generali di risoluzione; si può ricorrere a tecniche e a trucchi per risolvere casi particolari.

Eliminazione di un'incognita.

Consideriamo l'equazione diofantea

$$2x^2 - xy - 9x + 5y + 2001 = 0. \qquad (7)$$

È un'equazione di secondo grado in cui l'incognita y compare solo al primo grado. Quindi possiamo facilmente ricavare la y in funzione della x: $(5 - x)\, y = -2x^2 + 9x - 2001$, da cui

$$y = \frac{2x^2 - 9x + 2001}{x - 5}. \qquad (8)$$

Facciamo ora la divisione con resto del polinomio al numeratore con il polinomio al denominatore, ottenendo: $2x^2 - 9x + 2001 = (2x + 1)(x - 5) + 2006$.

Dalla (8) ricaviamo quindi

$$y = \frac{2x^2 - 9x + 2001}{x + 5} = \frac{(2x+1)(x-5)}{x-5} + \frac{2006}{x-5} = 2x + 1 + \frac{2006}{x-5}. \qquad (9)$$

Poiché x è un intero, la (9) fornisce un valore intero per y se e solo se $x - 5$ divide 2006.

Determiniamo tutti i divisori di 2006. Dato che $2006 = 2 \cdot 17 \cdot 59$, i divisori di 2006 sono

$$\pm 1, \pm 2, \pm 17, \pm 34, \pm 59, \pm 118, \pm 1003, \pm 2006.$$

Perciò $x - 5$ deve assumere uno dei 16 valori elencati sopra, da cui x deve assumere uno dei 16 valori seguenti:

$$-2001, -998, -113, -54, -29, -12, 3, 4, 6, 7, 22, 39, 64, 123, 1008, 2011.$$

Ricaviamo infine la y dalla (9) e concludiamo che l'equazione (7) ha esattamente 16 soluzioni, ossia

x	-2001	-998	-113	-54	-29	-12	3	4	6	7	22	39	64	123	1008	2011
y	-4002	-1997	-242	-141	-116	-141	-996	-1997	2019	1018	163	138	163	264	2019	4024

Esercizio 3

Trovare le soluzioni intere delle equazioni diofantee seguenti:

$3x^2 + xy - 2x + 5y + 7 = 0$, $y^2 - xy + 5x + 1 = 0$, $(x + 1)(y + 1) = 2xy$.

Punti razionali su una conica.

Si dice *conica* il luogo degli zeri di un polinomio di secondo grado nelle variabili x, y. Le coniche più famose sono l'iperbole, la parabola e l'ellisse (la circonferenza è una particolare ellisse). Vi sono però anche i casi degeneri, in cui la conica è vuota (ad esempio $x^2 + y^2 = -1$) o si riduce a un solo punto (ad esempio $x^2 + y^2 = 0$), o è una retta (ad esempio $x^2 = 0$), o l'unione di due rette (ad esempio $xy = 0$).

Consideriamo la circonferenza di centro O (0, 0) e raggio 1, descritta dall'equazione

$$x^2 + y^2 = 1. \qquad (10)$$

Le soluzioni intere di questa equazione sono ovviamente solo le coppie (1, 0), (0, 1), (−1, 0), (0, −1). Vogliamo determinare tutte le soluzioni razionali di (10), ossia l'insieme dei punti (x, y) aventi per ascissa x e per ordinata y due frazioni. Procediamo così: fissiamo un punto razionale sul cerchio, ad esempio (−1, 0), e tracciamo la retta passante per questo punto di coefficiente angolare t. Questa retta intersecherà il cerchio in un secondo punto (x, y), oltre a (−1, 0). Dimostriamo che se t è un numero razionale, allora (x, y) ha coordinate razionali. Infatti, l'ascissa di questo secondo punto d'intersezione è soluzione di un polinomio di secondo grado i cui coefficienti sono razionali (dipendono dai coefficienti dell'equazione (10) e da t).

In generale, un polinomio di secondo grado con coefficienti razionali non ha radici razionali, perché nella formula risolutiva compare una radice quadrata. Nel nostro caso però sappiamo che $x = -1$ è soluzione (poiché $(-1, 0)$ è un'intersezione), quindi, per il Teorema di Ruffini, il polinomio in questione è divisibile per $x + 1$. Effettuando la divisione tra polinomi a coefficienti razionali si ottiene un polinomio a coefficienti razionali, che in questo caso è un polinomio di grado uno a coefficienti razionali, che pertanto ha una radice razionale. D'altra parte, tutti i punti razionali sul cerchio si trovano in questo modo. Infatti, se (x, y) è un punto razionale sul cerchio diverso da $(-1, 0)$, allora la retta passante per $(-1, 0)$ e per (x, y) ha coefficiente angolare $\frac{y}{x+1}$, che è un numero razionale.

Questo ragionamento ha validità generale: se C è una conica, tutti punti razionali su C si trovano fissando un qualunque punto razionale P e individuando le seconde intersezioni di C con una qualunque retta passante per P e avente coefficiente angolare razionale.

Vediamo di attuare quanto detto nel caso dell'equazione (10), avendo fissato il punto $(-1, 0)$. Si tratta di trovare le soluzioni del sistema $\begin{cases} x^2 + y^2 = 1 \\ y = t(x+1) \end{cases}$. (11)

Sostituendo l'espressione per y dalla seconda equazione nella prima otteniamo

$$x^2 + t^2(x + 1)^2 = 1,$$

ossia

$$(1 + t^2)x^2 + 2t^2x + t^2 - 1 = 0. \qquad (12)$$

Sappiamo già che $x = -1$ è soluzione di questa equazione, quindi il polinomio sopra è divisibile per $x + 1$. Infatti,

$$(1 + t^2)\, x^2 + 2t^2x + t^2 - 1 = (x + 1)\, ((1 + t^2)\, x + t^2 - 1).$$

Perciò l'altra soluzione di (12) è soluzione di

$$(1 + t^2)\, x + t^2 - 1 = 0,$$

cioè

$$x = \frac{1-t^2}{1+t^2}$$

Sostituendo questo valore di x nella seconda equazione del sistema (11), troviamo

$$y = \frac{2t}{1+t^2}.$$

Concludiamo che tutti i punti razionali sul cerchio sono quelli della forma

$$(x, y) = \left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2} \right), \qquad (13)$$

al variare di t tra tutti i numeri razionali. Si osservi che questa è la parametrizzazione del cerchio che si trova associando a un punto P sul cerchio il numero $t = \tan\left(\frac{\theta}{2}\right)$, dove θ è l'angolo $A\hat{O}P$, con A= (1, 0).

Esercizio 4

Determinare i punti razionali sull'iperbole di equazione

$$x^2 - y^2 = 1,$$

e sull'ellisse di equazione

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

dove a, b sono numeri razionali non nulli.

Terne pitagoriche

Una delle equazioni diofantee più famose è:

$$\boldsymbol{a^2 + b^2 = c^2}, \quad (14)$$

come equazione nelle incognite *a, b, c*. Per il Teorema di Pitagora, le soluzioni intere e positive di questa equazione sono le terne (*a, b, c*) per cui esiste un triangolo rettangolo di cateti *a, b* e d'ipotenusa *c*. Per questo motivo, tali terne si dicono *terne pitagoriche*: corrispondono ai triangoli rettangoli con tutti i tre lati interi. Mostriamo come la conoscenza dei punti razionali sul cerchio permetta di determinare tutte le possibili terne pitagoriche.

Iniziamo con l'osservare che se (*a, b, c*) è una terna pitagorica con un fattore comune *d*, allora la terna (*a/d, b/d, c/d*) è ancora pitagorica. Quindi è sufficiente determinare tutte le terne pitagoriche primitive, ossia quelle per cui il massimo comun divisore tra *a, b, c* è 1; tutte le altre si otterranno moltiplicando i tre numeri di una terna primitiva per lo stesso intero positivo. Se poniamo

$$x = \frac{a}{c}, \quad y = \frac{b}{c},$$

e dividiamo l'equazione (14) per c^2, troviamo l'equazione

$$x^2 + y^2 = 1.$$

Ci interessano quindi le soluzioni razionali di questa equazione, che per quanto visto prima sono date dalla formula (13). Scrivendo il numero razionale *t* in (13) come *t = m/n*, con *m, n* interi primi tra loro, otteniamo

$$x = \frac{a}{c} = \frac{n^2 - m^2}{n^2 + m^2}, \quad y = \frac{b}{c} = \frac{2mn}{n^2 + m^2}. \quad (15)$$

Sia *p* un numero primo diverso da 2 che divide sia $2mn$ che $n^2 + m^2$. Dato che $p \neq 2$ divide $2mn$, necessariamente divide almeno uno tra *m* e *n*. Ma dovendo dividere anche $n^2 + m^2$, divide anche il quadrato dell'altro, e quindi l'altro. Questo contraddice il fatto che *m, n* fossero primi tra loro. Quindi i numeri $2mn$ e $m^2 + n^2$ hanno al più il fattore 2 in comune, e questo avviene se e solamente se *n* e *m* sono entrambi dispari (non possono essere entrambi pari, essendo primi tra loro). Consideriamo il caso in cui *m* e *n* abbiano parità diversa. Allora se (*a, b, c*) è una terna di interi positivi con M.C.D. = 1 che verifica (14), necessariamente $a = n^2 - m^2$, $b = 2mn$, $c = n^2 + m^2$.

Se invece *n* e *m* sono entrambi dispari, (15) implica

$$a = \frac{n^2 - m^2}{2}, \quad b = mn, \quad c = \frac{n^2 + m^2}{2}.$$

Ma essendo numeri dispari, $n = 2k + 1$ e $m = 2h - 1$, da cui

$$a = 2(k + h)(k - h + 1),\ b = (k + h)^2 - (k - h + 1)^2,\ c = (k + h)^2 + (k - h + 1)^2.$$

Dato che $k + h$ e $k - h + 1$ hanno parità diversa, questo caso si riduce al precedente, ma si è scambiato *a* con *b*. Concludiamo che le terne pitagoriche (*a, b, c*) con massimo comun divisore 1 sono tutte e sole le terne $a = n^2 - m^2$, $b = 2mn$, $c = n^2 + m^2$, con $n > m$ interi positivi primi tra loro, di parità diversa, e le terne ottenute scambiando *a* con *b*.

ESERCIZI EQUAZIONI DIOFANTEE CON SOLUZIONI

1. Determinare tutte le coppie (x, y) di numeri interi che 7x – 5y = 2.

Risposta: $\begin{cases} x = -4 + 5 \cdot n \\ y = -6 + 7 \cdot n \end{cases}$ *con n* int*ero*.

SOLUZIONE

Il problema consiste nel trovare tutte le soluzioni intere di 7x – 5y = 2. (1)

A tale scopo, se applichiamo l'algoritmo di Euclide alla coppia (7, 5), otteniamo:

(I) $7 = 1 \cdot 5 + 2$ quindi (I') $2 = 7 - 1 \cdot 5$

(II) $5 = 2 \cdot 2 + 1$ quindi (II') $1 = 5 - 2 \cdot 2$

(III) $2 = 1 \cdot 2 + 0$.

A questo punto riusciamo a esprimere 1 come combinazione intera dei numeri 7 e 5 nel modo seguente:

$1 = 5 - 2 \cdot 2 = 5 - 2 (7 - 5 \cdot 1) = -2 \cdot 7 + 3 \cdot 5$.

Abbiamo quindi trovato che:

$7 \cdot (-2) + 5 \cdot 3 = 1$

e quindi, moltiplicando ambo i membri per 2, otteniamo

$7 \cdot (-4) + 5 \cdot 6 = 2$

cioè (−4, −6) è una soluzione di (1).

Per trovare tutte le soluzioni intere di (1), osserviamo che, prese due qualsiasi coppie di interi (x_1, y_1) e (x_2, y_2) che la soddisfino, si avrà (ovviamente) che $7x_1 - 5y_1 = 2$ e $7x_2 - 5y_2 = 2$, quindi, sottraendo membro a membro, si otterrà: $7 (x_1 - x_2) - 5 (y_1 - y_2) = 0$.

Detto in altre parole, se (x_1, y_1) e (x_2, y_2) sono entrambe soluzioni di (1), allora la loro differenza è una soluzione intera dell'equazione diofantea 7x – 5y = 0. (2)

Ciò significa che per trovare tutte le soluzioni intere di (1) basterà trovarne una sola (x_0, y_0), dopodiché tutte le altre si troveranno aggiungendo a (x_0, y_0) una soluzione di (2).

Notiamo che se (x', y') è una soluzione di (2), si avrà 7x' = 5y', ed essendo 7 e 5 primi tra loro, necessariamente x' sarà un multiplo di 5 e y' un multiplo di 7.

Di conseguenza le soluzioni di (2) sono tutte e sole le coppie (x*, y*) del tipo:

$$(3) \begin{cases} x^* = 5 \cdot n \\ y^* = 7 \cdot n \end{cases}, \text{ con } n \text{ intero.}$$

Infine, le soluzioni di (1) sono tutte e sole le coppie (x, y) tali che

$$(4) \begin{cases} x = -4 + 5 \cdot n \\ y = -6 + 7 \cdot n \end{cases}, \text{ con } n \text{ intero.}$$

[VERIFICA: $7(-4+5n)-5(-6+7n) = -28 +35n + 30 -35n = 2$ (c.v.d.)]

2. Quante sono le terne ordinate (a, b, c) di interi positivi verificanti l'equazione $a^2 + b^2 + c^2 = 110$?

Risposta: 3

SOLUZIONE

Notiamo innanzitutto che a, b, c non possono essere tutti pari, poiché la somma dei quadrati dei numeri pari compresi tra 1 e 10 non dà come risultato 110. Quindi si può avere solo il caso in cui un numero è pari e gli altri due sono dispari. Sia c pari; allora $a^2 + b^2 = 110 - c^2$, ma essendo il più grande quadrato di un numero pari, prossimo a 110, 100, si avrà:

$110 - 100 = 10 = 1 + 9 = 1^2 + 3^2 \longrightarrow$ I terna soluzione (1, 3, 10)

Ora procediamo utilizzando i quadrati dei pari più piccoli di 100:

$110 - 64 = 46$, che però non è possibile esprimere come somma di due quadrati di numeri dispari;

$110 - 36 = 74 = 25 + 49 = 5^2 + 7^2 \longrightarrow$ II terna soluzione (5, 6, 7);

$110 - 16 = 94$, che però non è possibile esprimere come somma di due quadrati di numeri dispari;

$110 - 4 = 106 = 25 + 81 = 5^2 + 9^2 \longrightarrow$ III terna soluzione (2, 5, 9).

In totale le terne sono quindi 3.

3. Determinare tutte le soluzioni dell'equazione 15x – 21y + 9z = 3.

Risposta: $x = t; \quad y = -1 + 5t + 3s; \quad z = -2 + 10t + 7s.$

SOLUZIONE

Poiché (15, 21, 9) = 3 e 3 divide 3, l'equazione è risolvibile. Consideriamo le seguenti due equazioni diofantee lineari in due indeterminate: $15x_1 + (21, 9)\, x_2 = 3$, ovvero $5x_1 + x_2 = 1$, e $-21y_1 + 9y_2 = (21, 9)$, ovvero $-7y_1 + 3y_2 = 1$. Notiamo istantaneamente che (0, 1) è una soluzione della prima equazione e (-1, -2) una soluzione della seconda; pertanto le soluzioni dell'equazione data sono:

$$x = t,$$
$$y = -1 + 5t + 3s,$$
$$z = -2 + 10t + 7s,$$ al variare di t, s in Z.

Ad esempio, per s = t = 0, abbiamo (0, -1, -2); per s = 0 e t = 1, (1, 4, 8); per s=1 e t = 0, (0, 2, 5)….

4. Data l'equazione $-4x^2 + 6x + 2xy - y + 13 = 0$, determinare il valore assoluto della somma dei prodotti dei valori soluzione di x che hanno uguali i corrispondenti valori di y.

Risposta: 14

SOLUZIONE

Consideriamo l'equazione data: $-4x^2 + 2xy + 6x - y + 13 = 0$. Possiamo esplicitarla rispetto a y:

$(2x - 1)\, y = 4x^2 - 6x - 13$, da cui $y = \dfrac{4x^2 - 6x - 13}{2x - 1}$. Facciamo ora la divisione con resto del polinomio al numeratore con il polinomio al denominatore, ottenendo: $4x^2 - 6x - 13 = (2x - 2)(2x - 1) - 15$.

Ricaviamo quindi

$$y = \frac{4x^2 - 6x - 13}{2x - 1} = \frac{(2x - 1)(2x - 2)}{2x - 1} - \frac{15}{2x - 1} = 2x - 2 - \frac{15}{2x - 1}.$$

Poiché x è un intero, la funzione sopra fornisce un valore intero per y se e solo se 2x – 1 divide 15. Determiniamo tutti i divisori di 15. Dato che $15 = 3 \cdot 5$, i divisori di 15 sono ±1, ±3, ±5, ±15.

Perciò 2x – 1 deve assumere uno degli 8 valori elencati sopra, cioè uno degli 8 valori seguenti:

$$-7, -2, -1, 0, 1, 2, 3, 8.$$

Ricaviamo infine la y:

x	-7	-2	-1	0	1	2	3	8
y	-15	-3	1	13	-15	-3	1	13

La soluzione al problema è data da: $|(-7 \cdot 1) + (-2 \cdot 2) + (-1 \cdot 3) + (0 \cdot 8)| = |-7 - 4 - 3| = |-14| = 14.$

5. Quante sono le coppie di interi non negativi x e y che risolvono 17x + 43y = 9999.

Risposta: 14

SOLUZIONE

Il problema consiste nel trovare tutte le soluzioni intere di

$$(1)\ 17x + 43y = 9999.$$

A tale scopo, se applichiamo l'algoritmo di Euclide alla coppia (17, 43), otteniamo:

(I) $43 = 2 \cdot 17 + 9$ quindi (I') $9 = 43 - 2 \cdot 17$

(II) $17 = 1 \cdot 9 + 8$ quindi (II') $8 = 17 - 1 \cdot 9$

(III) $9 = 1 \cdot 8 + 1$ quindi (III') $1 = 9 - 1 \cdot 8$.

A questo punto riusciamo a esprimere 1 come combinazione intera dei numeri 17 e 43 nel modo seguente:

$1 =_{(III')} 9 - 1 \cdot 8 =_{(II')} 9 - 1\,(17 - 1 \cdot 9) = -1 \cdot 17 + 2 \cdot 9 =_{(I')} -1 \cdot 17 + 2(43 - 2 \cdot 17) =$
$-5 \cdot 17 + 2 \cdot 43.$

Abbiamo quindi trovato che (−5, 2) è una soluzione di (1) e quindi, moltiplicando ambo i membri per 9999, otteniamo: $17 \cdot (-49995) + 43 \cdot (19998) = 9999.$

A questo punto, scrivendo l'equazione omogenea associata alla (1):

$$(2) \qquad 17x + 43y = 0,$$

se (x', y') è una soluzione di (2), avremo che $17x' = -43y'$, ed essendo 17 e 43 primi tra loro, necessariamente x' sarà un multiplo di 43 e y' un multiplo di 17.

Di conseguenza le soluzioni di (2) sono tutte e sole le coppie (x*, y*) del tipo:

$$(3) \begin{cases} x^* = 43 \cdot n \\ y^* = -17 \cdot n \end{cases}, \text{ con } n \text{ intero.}$$

Infine, le soluzioni di (1) sono tutte e sole le coppie (x, y) tali che

$$(4) \begin{cases} x = -49995 + 43 \cdot n \\ y = 19998 - 17 \cdot n \end{cases} \quad con\ n\ \text{int}\,ero.$$

[VERIFICA: $17(-49995+43n)+43(19998-17n) = -849915+17 \cdot 43n + 859914 - 17 \cdot 43n = 9999$ (c.v.d.)]

Per trovare le soluzioni intere <u>non negative</u>, dobbiamo risolvere il sistema:

$$\begin{cases} x \geq 0 \\ y \geq 0 \end{cases} \Rightarrow \begin{cases} -49995 + 43n \geq 0 \\ 19998 - 17n \geq 0 \end{cases} \Rightarrow \begin{cases} n \geq 1163 \\ n \leq 1176 \end{cases} \Rightarrow \quad 1163 \leq n \leq 1176$$

In definitiva abbiamo 14 soluzioni, date dalle coppie seguenti:

1163	1164	1165	1166	1167	1168	1169	1170	1171	1172	1173	1174	1175	1176
x=14	x=57	x=100	x=143	x=186	x=229	x=272	x=315	x=358	x=401	x=444	x=487	x=530	x=573
y=227	y=210	y=193	y=176	y=159	y=142	y=125	y=108	y=91	y=74	y=57	y=40	y=23	y=6

6. Un falegname ha bisogno di misurare una lunghezza di 30 cm, ma ha dimenticato il metro. Ha con sé una tavola che misura 70 cm × 50 cm. Qual è il numero minimo di misurazioni che deve fare?

Risposta: 3

SOLUZIONE: il problema è estremamente semplice, basta infatti considerare che sottraendo 50 cm da 70 cm, si ottiene 20 cm, sottraendo 20 cm da 50 cm si ottiene 30 cm; basta confrontare la lunghezza con quest'ultima misura e il gioco è fatto! In alternativa basta risolvere l'equazione diofantea 50x + 70y = 30, che ha per soluzioni x = 2 e y = -1, quindi in totale le operazioni sono tre.

7. Una vecchia signora ricama 35 tovaglioli al giorno e li confeziona in scatole da 6 tovaglioli ciascuna. Qual è il numero minimo di giorni che deve lavorare per averne alla fine della giornata esattamente uno in più?

Risposta: 5

SOLUZIONE

Posto x = numero dei giorni, y = numero delle scatole, il problema consiste nel trovare tutte le soluzioni intere di $(1)\ 35x - 6y = 1.$

A tale scopo, se applichiamo l'algoritmo di Euclide alla coppia (35, 6), otteniamo:

(I) $35 = 5 \cdot 6 + 5$ quindi (I') $5 = 35 - 5 \cdot 6$

(II) $6 = 1 \cdot 5 + 1$ quindi (II') $1 = 6 - 1 \cdot 5.$

A questo punto riusciamo a esprimere 1 come combinazione intera dei numeri 35 e 6 nel modo seguente:

$1 =_{(II')} 6 - 1 \cdot 5 =_{(I')} 6 - 1\,(35 - 5 \cdot 6) = -1 \cdot 35 + 6 \cdot 6.$
Abbiamo quindi trovato che: $35 \cdot (-1) + 6 \cdot 6 = 1.$
A questo punto, scrivendo l'equazione omogenea associata alla (1):
(2) $35x - 6y = 0,$
se (x', y') è una soluzione di (2), avremo che $35x' = 6y'$, ed essendo 35 e 6 primi tra loro, necessariamente x' sarà un multiplo di 6 e y' un multiplo di 35.
Di conseguenza le soluzioni di (2) sono tutte e sole le coppie (x*, y*) del tipo:

$$(3)\ \begin{cases} x^* = 6 \cdot n \\ y^* = 35 \cdot n \end{cases} \quad con\ n\ \text{int}\, ero.$$

Infine, le soluzioni di (1) sono tutte e sole le coppie (x, y) tali che

$$(4)\ \begin{cases} x = -1 + 6 \cdot n \\ y = -6 + 35 \cdot n \end{cases} \quad con\ n\ \text{int}\, ero.$$

[VERIFICA: $35(-1+6n)-6(-6+35n) = -35 +210n + 36 -210n = 1$ (c.v.d.)]

Per n = 1 abbiamo: $\begin{cases} x = 5 \\ y = 29 \end{cases}$, quindi il numero minimo di giorni che la signora deve lavorare è 5.

8. Un venditore acquista 40 rose alla volta per poi rivenderle a mazzi di 7. Vorrebbe portarne una a sua moglie senza però farne avanzare di più. Quante ne deve acquistare e quanti mazzi deve riuscire a vendere entro la fine della giornata?

Risposta: 120 rose e 17 mazzi
SOLUZIONE
Posto x = numero di rose, y = numero di mazzi, il problema consiste nel trovare tutte le soluzioni intere di (1) $40x - 7y = 1.$
A tale scopo, se applichiamo l'algoritmo di Euclide alla coppia (40, 7), otteniamo:
(I) $40 = 5 \cdot 7 + 5$ quindi (I') $5 = 40 - 5 \cdot 7$
(II) $7 = 1 \cdot 5 + 2$ quindi (II') $2 = 7 - 1 \cdot 5$
(III) $5 = 2 \cdot 2 + 1$ quindi (III') $1 = 5 - 2 \cdot 2.$
A questo punto riusciamo a esprimere 1 come combinazione intera dei numeri 40 e 7 nel modo seguente:
$1 =_{(III')} 5 - 2 \cdot 2 =_{(II')} 5 - 2(7 - 1 \cdot 5) = -2 \cdot 7 + 3 \cdot 5 =_{(I')} -2 \cdot 7 + 3(40 - 5 \cdot 7) = -17 \cdot 7 + 3 \cdot 40.$
Abbiamo quindi trovato che: $40 \cdot 3 - 17 \cdot 7 = 1.$
A questo punto, scrivendo l'equazione omogenea associata alla (1):
(2) $40x - 7y = 0,$
se (x', y') è una soluzione di (2), avremo che $40x' = 7y'$, ed essendo 40 e 7 primi tra loro, necessariamente x' sarà un multiplo di 7 e y' un multiplo di 40.
Di conseguenza le soluzioni di (2) sono tutte e sole le coppie (x*, y*) del tipo:

$$(3)\ \begin{cases} x^* = 7 \cdot n \\ y^* = 40 \cdot n \end{cases} \quad con\ n\ \text{int}\, ero.$$

Infine, le soluzioni di (1) sono tutte e sole le coppie (x, y) tali che

$$(4)\ \begin{cases} x = 3 + 7 \cdot n \\ y = 17 + 40 \cdot n \end{cases} \quad con\ n\ \text{int}\, ero.$$

[VERIFICA: $40(3+7n)-7(17+40n) = 120 +280n - 119 -280n = 1$ (c.v.d.)]

Per n = 0 abbiamo: $\begin{cases} x = 3 \\ y = 17 \end{cases}$, quindi il numero di rose che il venditore deve acquistare è 120 e il numero di mazzi che deve vendere è 17.

9. Marta ha bisogno di pesare 330 g di farina per fare un dolce, ma non ha una bilancia a disposizione. Su internet legge che un cucchiaio di farina corrisponde circa a 25 g e un bicchiere di plastica ne contiene 90 g. Qual è il numero minimo di operazioni che deve compiere per pesare 330 g di farina?

Risposta: 8

SOLUZIONE

Posto x = numero di cucchiai, y = numero di bicchieri, il problema consiste nel trovare tutte le soluzioni intere di (1) $25x + 90y = 330$,

da cui, dividendo tutto per 5: (1bis) $5x + 18y = 66$.

A tale scopo, se applichiamo l'algoritmo di Euclide alla coppia (5, 18), otteniamo:

(I) $18 = 3 \cdot 5 + 3$ quindi (I') $3 = 18 - 3 \cdot 5$

(II) $5 = 1 \cdot 3 + 2$ quindi (II') $2 = 5 - 1 \cdot 3$

(III) $3 = 1 \cdot 2 + 1$ quindi (III') $1 = 3 - 1 \cdot 2$.

A questo punto riusciamo a esprimere 1 come combinazione intera dei numeri 5 e 18 nel modo seguente:

$1 =_{(III')} 3 - 1 \cdot 2 =_{(II')} 3 - 1(5 - 1 \cdot 3) = -1 \cdot 5 + 2 \cdot 3 =_{(I')} -1 \cdot 5 + 2(18 - 3 \cdot 5) = -7 \cdot 5 + 2 \cdot 18.$

Abbiamo quindi trovato che: $-7 \cdot 5 + 2 \cdot 18 = 1$.

A questo punto, scrivendo l'equazione omogenea associata alla (1bis):

(2) $5x + 18y = 0$,

se (x', y') è una soluzione di (2), avremo che $5x' = -18y'$, ed essendo 5 e 18 primi tra loro, necessariamente x' sarà un multiplo di 18 e y' un multiplo di 5.

Di conseguenza le soluzioni di (2) sono tutte e sole le coppie (x*, y*) del tipo:

$$(3)\ \begin{cases} x^* = 18 \cdot n \\ y^* = -5 \cdot n \end{cases} \quad con\ n\ \text{int}\, ero.$$

Moltiplicando $-7 \cdot 5 + 2 \cdot 18 = 1$ per 66, otteniamo:

$-462 \cdot 5 + 132 \cdot 18 = 66$.

Infine, le soluzioni di (1) sono tutte e sole le coppie (x, y) tali che

$$(4)\ \begin{cases} x = -462 + 18 \cdot n \\ y = 132 - 5 \cdot n \end{cases} \quad con\ n\ \text{int}\, ero.$$

[VERIFICA: $5(-462 + 18n) + 18(132 - 5n) = -2310 + 90n + 2376 - 90n = 66$ (c.v.d.)]

Dobbiamo trovare le soluzioni intere non negative, quindi dobbiamo risolvere il sistema:

$$\begin{cases} x \geq 0 \\ y \geq 0 \end{cases} \Rightarrow \begin{cases} -462 + 18n \geq 0 \\ 132 - 5n \geq 0 \end{cases} \Rightarrow \begin{cases} n \geq 25,7 \\ n \leq 26,4 \end{cases} \Rightarrow \quad n = 26$$

Per n = 26 abbiamo: $\begin{cases} x = 6 \\ y = 2 \end{cases}$, quindi il numero minimo di operazioni che Marta deve compiere è 6 + 2 = 8.

10. Nel piano cartesiano una pulce parte dall'origine e può fare solo salti in orizzontale lunghi 17 o 11 (in avanti o indietro) e in verticale lunghi 41 o 37 (in avanti o indietro). Come può arrivare nel punto di coordinate (10, 10)? Può farlo con un numero di salti in orizzontale che sia uguale al numero di salti in verticale?

Risposta: 40; Sì.

SOLUZIONE

Siano x_O, y_O i salti orizzontali; x_V, y_V i salti verticali. Deve essere:

$$(1)\ 17x_O + 11y_O = 10 \text{ e } (2)\ 41x_V + 37y_V = 10.$$

Risolviamo la (1):

applichiamo l'algoritmo di Euclide alla coppia (17, 11):

(I) $17 = 1 \cdot 11 + 6$ quindi (I') $6 = 17 - 1 \cdot 11$

(II) $11 = 1 \cdot 6 + 5$ quindi (II') $5 = 11 - 1 \cdot 6$

(III) $6 = 1 \cdot 5 + 1$ quindi (III') $1 = 6 - 1 \cdot 5$.

A questo punto esprimiamo 1 come combinazione intera dei numeri 11 e 17:

$1 =_{(III')} 6 - 1 \cdot 5 =_{(II')} 6 - 1(11 - 1 \cdot 6) = -1 \cdot 11 + 2 \cdot 6 =_{(I')} -1 \cdot 11 + 2(17 - 1 \cdot 11) = -1 \cdot 11 + 2 \cdot 17 - 2 \cdot 11 = -3 \cdot 11 + 2 \cdot 17$.

Moltiplicando l'uguaglianza sopra per 10 si ha:

$20 \cdot 17 - 30 \cdot 11 = 10$.

A questo punto, scrivendo l'equazione omogenea associata alla (2):

$$(3)\quad 17x_O + 11y_O = 0,$$

se (x', y') è una soluzione di (2), avremo che $17x'_O = -11y'_O$, ed essendo 17 e 11 primi tra loro, necessariamente x' sarà un multiplo di 11 e y' un multiplo di 17.

Di conseguenza le soluzioni di (2) sono tutte e sole le coppie (x*, y*) del tipo:

$$(3)\ \begin{cases} x^* = 11 \cdot n \\ y^* = -17 \cdot n \end{cases} \quad con\ n\ \text{intero}.$$

Infine, le soluzioni di (1) sono tutte e sole le coppie (x, y) tali che

$$(4)\ \begin{cases} x_O = 20 + 11 \cdot n \\ y_O = -30 - 17 \cdot n \end{cases} \quad con\ n\ \text{intero}.$$

Analogamente, risolviamo la (2):

applichiamo l'algoritmo di Euclide alla coppia (37, 41):

(I) $41 = 1 \cdot 37 + 4$ quindi (I') $4 = 41 - 1 \cdot 37$

(II) $37 = 9 \cdot 4 + 1$ quindi (II') $1 = 37 - 9 \cdot 4$

A questo punto esprimiamo 1 come combinazione intera dei numeri 41 e 37:

$1 =_{(II')} 37 - 9 \cdot 4 =_{(I')} 37 - 9(41 - 1 \cdot 37) = 37 - 9 \cdot 41 + 9 \cdot 37 = -9 \cdot 41 + 10 \cdot 37$.

Moltiplicando l'uguaglianza sopra per 10 si ha:

$-90 \cdot 41 + 100 \cdot 37 = 10$.

A questo punto, scrivendo l'equazione omogenea associata alla (1):

$$(2)\quad 41x_V + 37y_V = 0,$$

se (x', y') è una soluzione di (2), avremo che $41x'_V = -37y'_V$, ed essendo 37 e 41 primi tra loro, necessariamente x' sarà un multiplo di 37 e y' un multiplo di 41.

Di conseguenza le soluzioni di (2) sono tutte e sole le coppie (x*, y*) del tipo:

$$(3)\ \begin{cases} x^* = 37 \cdot k \\ y^* = -41 \cdot k \end{cases} \quad con\ k\ \text{intero}.$$

Infine, le soluzioni di (2) sono tutte e sole le coppie (x, y) tali che

$$(4)\quad \begin{cases} x_V = -90 + 37 \cdot k \\ y_V = 100 - 41 \cdot k \end{cases} \quad con\ k\ \text{int}ero.$$

Ora costruiamo una tabella per calcolare come variano le soluzioni al variare di n e k:

n	-5	-4	-3	-2	-1	0	1	2	3
x_O	-35	-24	-13	-2	9	20	33	42	53
y_O	55	38	21	4	-13	-30	-47	-54	-81
$\lvert x_O\rvert+\lvert y_O\rvert$	90	62	34	6	22	50	80	96	134

k	-5	-4	-3	-2	-1	0	1	2	3
x_V	-275	-238	-201	-164	-127	-90	-53	-16	21
y_V	305	264	223	182	141	100	59	18	-23
$\lvert x_V\rvert+\lvert y_V\rvert$	580	502	424	346	268	190	112	34	44

La pulce arriva in P con 40 salti (6 + 34) corrispondenti a n= –2, k=2.
Per n= –3, k=2, il numero dei salti orizzontali è uguale al numero di salti verticali.

La Struttura Moltiplicativa del gruppo Z_n

Analizziamo qualche aspetto collegato alla struttura moltiplicativa degli insiemi Z_n delle classi di resto modulo *n*. Nel seguito indicheremo con $\equiv_n$ le congruenze modulo *n*.

Consideriamo innanzitutto il caso in cui $n = p$ sia un numero primo; citiamo le definizioni e i risultati fondamentali.

Teorema di Fermat. Siano p primo e a intero non divisibile per p allora

$$a^{p-1} \equiv_p 1 .$$

Corollario. Siano p primo e a intero qualsiasi allora

$$a^p \equiv_p a.$$

Definizione. Siano p primo e a intero non divisibile per p allora si definisce l'ordine moltiplicativo di a modulo p come il più piccolo intero positivo n tale che $a^n \equiv_p 1$ e si scrive:

$$ord_p(a) := \min\{n \geq 1 \mid a^n \equiv_p 1\}.$$

Teorema. Siano p primo e a intero non divisibile per p allora

$$ord_p(a) \mid (p-1) .$$

Corollario. Siano p primo, a intero non divisibile per p e $a^n \equiv_p 1$ allora

$$ord_p(a) \mid n .$$

Corollario. Siano p primo, a intero non divisibile per p e $a^n \equiv_p a^m$ allora

$$ord_p(a) \mid (n-m).$$

Corollario. Siano p primo e a intero non divisibile per p allora esiste un intero n tale che $a^n \equiv_p -1$ se e solo se $ord_p(a)$ è un numero pari. Il più piccolo di tali n positivi sarà $ord_p(a)/2$ e tutti gli altri n buoni saranno un multiplo dispari di tale minimo.

Definizione. Un intero a si dice un generatore modulo p se $ord_p(a) = p-1$.

Osservazione. Se a è un generatore modulo p, allora $a^1, a^2, ..., a^{p-1}$ rappresentano tutte le classi di congruenza modulo p tranne la classe nulla.

Teorema. Per ogni numero primo p esiste un generatore modulo p.

Teorema. Se a è un generatore modulo p e se k e $p-1$ sono relativamente primi tra loro, allora a^k sono tutti e soli i generatori moduli p.

Introduciamo ora una funzione assai importante in teoria dei numeri: la Φ di Eulero.

Definizione. Sia m un intero maggiore di 1, la funzione Φ di Eulero è quella mappa che associa a ogni m il numero degli interi compresi tra 0 e m (estremi esclusi) che sono primi con m. In formule:
$\Phi(m) := card\{a \in N \mid 0 < a < m \text{ e } (a,m) = 1\}$.

Teorema. Sia $m = p_1^{\alpha_1} \cdot \ldots \cdot p_k^{\alpha_k}$ la fattorizzazione in numeri primi di m. Allora vale

$$\Phi(m) = m\left(1-\frac{1}{p_1}\right)\cdot\ldots\cdot\left(1-\frac{1}{p_k}\right)$$

Esercizio 1. Determinare il resto della divisione per 13 di $a = 2^{2016}+5^{2016}+7^{2016}+11^{2016}$.
Soluzione: innanzitutto osserviamo che $2016 = 168\cdot 12$, quindi per il teorema di Fermat se $(x,13)=1$ si ha $x^{12} \equiv_{13} 1$ e dunque $x^{2016} = \left(x^{12}\right)^{168} \equiv_{13} 1^{168} \equiv_{13} 1$; nel caso in questione (essendo 2, 5, 7 e 11 relativamente primi con 13) si ha:

$$a = 2^{2016}+5^{2016}+7^{2016}+11^{2016} \equiv_{13} 1+1+1+1 \equiv_{13} 4$$

in conclusione il resto della divisione di a per 13 è 4.

Esercizio 2. Dimostrare che per ogni numero naturale n il termine $2n^{41}+11n^{23}+24n^3+13n$ è divisibile per 5.
Soluzione: se n è un multiplo di 5 siamo già arrivati. Supponiamo quindi che $(n,5)=1$ allora per il teorema di Fermat si ha $n^4 \equiv_5 1$ quindi $n^{41} \equiv_5 \left(n^4\right)^{10}\cdot n^1 \equiv_5 n$ e $n^{23} \equiv_5 \left(n^4\right)^5 \cdot n^3 \equiv_5 n^3$ da cui

$$2n^{41}+11n^{23}+24n^3+13n \equiv_5 2n+11n^3+24n^3+13n \equiv_5 15n+35n^3 \equiv_5 0.$$

Esercizio 3. (Senior Camp 2007) Determinare tutte le cifre con cui può terminare in base dieci x^{2008} dove *x* è un qualsiasi numero naturale.
Soluzione: sia *k* la cifra in questione, consideriamo le congruenze modulo 5 e supponiamo inizialmente che 5 non divida *x*. Poiché $\Phi(5)=4$, si può applicare il teorema di Fermat: $x^4 \equiv_5 1$ da cui $k \equiv_5 x^{2008} \equiv_5 \left(x^4\right)^{502} \equiv_5 1$ e quindi $k=1$ oppure $k=6$. Supponiamo ora che $(5,x)=5$ allora $k=0$ oppure $k=5$. In definitiva le cifre possibili sono 1,6,0,5 e sono tutte effettivamente ottenibili, basta osservare, infatti, che $1^2 \equiv_{10} 1$, $6^2 \equiv_{10} 6$, $0^2 \equiv_{10} 0$ e $5^2 \equiv_{10} 5$ e quindi $1^n \equiv_{10} 1$, $6^n \equiv_{10} 6$, $0^n \equiv_{10} 0$ e $5^n \equiv_{10} 5$ per ogni numero naturale *n*, quindi anche per $n = 2008$.

Ritroviamo ora alcuni dei risultati precedentemente visti nel caso $n = p$ primo, nell'ambito più generale di un numero intero m qualsiasi.

Teorema di Eulero. Siano a e m interi primi tra loro, allora

$$a^{\Phi(m)} \equiv_m 1.$$

Definizione. Siano a e m interi primi tra loro allora si definisce l'ordine moltiplicativo di a modulo m come il più piccolo intero positivo n tale che $a^n \equiv_m 1$ e si scrive:
$ord_m(a) := \min\{n \geq 1 \mid a^n \equiv_m 1\}$.
Teorema. Siano a e m interi primi tra loro allora
$ord_m(a) \mid \Phi(m)$.
Corollario. Siano a e m interi primi tra loro e $a^n \equiv_m 1$ allora
$ord_m(a) \mid n$.
Corollario. Siano a e m interi primi tra loro e $a^n \equiv_m a^h$ allora

$ord_m(a) \mid (n-h)$.

Definizione. Un intero a si dice un generatore modulo m se $ord_m(a) = \Phi(m)$.

Osservazione. Se a è un generatore modulo m, allora $a^1, a^2, ..., a^{\Phi(m)}$ rappresentano tutte le classi di congruenza modulo m che contengono un rappresentante relativamente primo con m.

Corollario. Siano a e m interi primi tra loro, se esiste un intero n tale che $a^n \equiv_m -1$ allora $ord_m(a)$ è un numero pari. Se esiste un generatore modulo m allora vale anche il viceversa e il più piccolo di tali n positivi sarà $ord_m(a)/2$ e tutti gli altri n buoni saranno un multiplo dispari di tale minimo.

Teorema. Gli unici interi m per cui esiste un generatore modulo m sono 2, 4, una qualsiasi potenza naturale di un primo dispari p^n e un qualsiasi numero del tipo $2 \cdot p^n$ con *n* naturale e *p* primo dispari.

Esercizio 4. (Senior Camp 2007) Si determini il più piccolo intero positivo n tale che $125 \mid 7^n - 1$.

Soluzione: osserviamo che se $7^n \equiv_{125} 1$ allora $7^n \equiv_5 1$ ovvero $7^n \equiv_5 2^n \equiv_5 1$. Ora le potenze di 2 modulo 5 sono cicliche di periodo 4, infatti, $2^1, 2^2, 2^3 \equiv_5 2,4,3$ rispettivamente mentre $2^4 \equiv_5 1$; allora $n = 4m$ per qualche naturale m. Ora $7^4 = 2401 \equiv_{25} 1$ quindi $7^{4m} = \left(7^4\right)^m \equiv_{25} 1$ allora $7^4 = 25k + 1$ con *k* non divisibile per 5 poiché 7^4 non è congruo a 1 modulo 125. Ora dobbiamo avere $(25k+1)^m \equiv_{125} 1$, sviluppando la potenza usando i coefficienti binomiali di Newton si ha $\sum_{i=0}^{m} \binom{m}{i} 25^{m-i}$ i cui unici addendi non multipli di 125 sono gli ultimi due: $25km + 1$. Affinché quest'ultimo termine sia congruo a 1 modulo 125, il minimo *m* deve essere 5, quindi il più piccolo intero positivo che stavamo cercando sarà $n = 4 \cdot 5 = 20$.

Esercizio 5. Determinare il resto della divisione per 25 di $919^{919} + 9191^{9191}$.

Soluzione: volendo usare il teorema di Eulero andiamo a trovare $\Phi(25) = 25\left(1 - \frac{1}{5}\right) = 20$ e scomponiamo 919 e 9191 in: $919 = 900 + 19 = 45 \cdot 20 + 19$ e $9191 = 9180 + 11 = 459 \cdot 20 + 11$. Sappiamo inoltre che $919 \equiv_{25} -6$ e $9191 \equiv_{25} -9$, quindi:

$$919^{919} + 9191^{9191} \equiv_{25} (-6)^{919} + (-9)^{9191} = \left[(-6)^{20}\right]^{45} \cdot (-6)^{19} + \left[(-9)^{20}\right]^{459} \cdot (-9)^{11} \equiv_{25} -6^{19} - 9^{11}$$

(essendo per il teorema di Eulero $(-6)^{20} \equiv_{25} 1 \equiv_{25} (-9)^{20}$). Ora

$$6^{19} = 6 \cdot 36^9 \equiv_{25} 6 \cdot 11^9 = 6 \cdot 11 \cdot 121^4 \equiv_{25} 6 \cdot 11 \cdot (-4)^4 = 16896 \equiv_{25} -4$$

ed anche

$$9^{11} = 9 \cdot 81^5 \equiv_{25} 9 \cdot 6^5 = 9 \cdot 6 \cdot 36^2 \equiv_{25} 9 \cdot 6 \cdot 11^2 = 9 \cdot 6 \cdot 121 = 6534 \equiv_{25} 9;$$

quindi

$919^{919} + 9191^{9191} \equiv_{25} -6^{19} - 9^{11} \equiv_{25} 4 - 9 = -5 \equiv_{25} 20$. Quindi il resto della divisione per 25 di $919^{919} + 9191^{9191}$ è 20.

CONGRUENZE

I)*Definizione*: due numeri naturali *a* e *b* si dicono *congrui modulo un numero naturale p* se hanno lo stesso resto nella divisione intera per *p*. Si scrive $a \equiv b \ mod\ p$ oppure $a \equiv b\ (p)$.
Proprietà delle congruenze: la congruenza è una relazione di equivalenza; inoltre:

$$a \equiv b \mod p \quad c \equiv d \mod p \quad allora \quad \begin{matrix} a+c \equiv b+d & (I) \\ a \cdot c \equiv b \cdot d & (II) \end{matrix}$$

Criteri di divisibilità

- Un numero è congruo modulo 2 alla sua cifra delle unità
- Un numero è congruo modulo 3 alla somma delle sue cifre
- Un numero è congruo modulo 4 al numero intero formato dalle sue due ultime cifre
- Un numero è congruo modulo 5 alla sua cifra delle unità
- Un numero è congruo modulo 8 al numero intero formato dalle sue tre ultime cifre
- Un numero è congruo modulo 9 alla somma delle sue cifre
- Un numero è congruo modulo 10 alla sua cifra delle unità
- Un numero è congruo modulo 11 alla somma a segno alterno delle sue cifre (i segni devono essere messi in modo che la cifra delle unità abbia segno negativo)
- Un numero è divisibile per 7 se e solo se è divisibile per 7 l'intero costruito nel seguente modo: si prende l'intero iniziale privato della cifra delle unità e gli si sottrae due volte la cifra delle unità.

Esempio 1: quanto è il resto nella divisione per tre del numero 2008^{2008}?
Soluzione:

$$2008^{2008} \equiv \underbrace{2008 \cdot \ 2008 \cdot \ \cdot \ \cdot 2008}_{2008 \quad volte}$$

$2008 \equiv 1 \quad (3)$. Quindi $2008^{2008} \equiv 1 \ (\text{mod } 3)$.

II) Con le congruenze possiamo caratterizzare i quadrati perfetti: se un numero *a* è un quadrato perfetto allora $a \equiv 0 \quad oppure \quad a \equiv 1 \quad (4)$
Quindi:

- il quadrato di un intero pari è sempre congruo a 0 modulo 4;
- il quadrato di un intero dispari è sempre congruo a 1 modulo 4.

Si può dare una caratterizzazione anche modulo 8. Se un numero *a* è un quadrato perfetto, allora $a = n^2$
e *n* pari $a \equiv \begin{matrix} 0 \\ 4 \end{matrix} \quad (8)$ *n* dispari $a \equiv 1 \quad (8)$
Si possono caratterizzare nello stesso modo le quarte potenze:

- La quarta potenza di un intero pari è sempre congrua a 0 modulo 16;
- La quarta potenza di un intero dispari è sempre congrua a 1 modulo 16.

Attenzione! Non sono vere le proprietà inverse; ad esempio $8 \equiv 0 \ \text{mod } 4$ ma 8 non è un quadrato perfetto.

Esempio 2: consideriamo un numero formato concatenando un po' di scritture decimali di 2006. Quante cifre ha il più piccolo quadrato perfetto tra tali numeri?
Soluzione
Consideriamo un numero del tipo 200620002……2006. Esso è congruo a 2 mod 4 quindi non può mai essere un quadrato perfetto.

III) Sistemi di congruenze: siano $m_1,\ldots m_k$ k numeri interi e $a_1,\ldots a_k$ altri k numeri interi; si dice sistema di congruenze un sistema della forma

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ &\vdots \\ x &\equiv a_n \pmod{m_k} \end{aligned}$$

Risolvere tale sistema significa trovare gli interi x che verificano contemporaneamente le k congruenze.

Esempio 3
Sono dati sette numeri interi positivi a, b, c, d, e, f, g tali che i prodotti ab, bc, cd, de, ef, fg, ga sono tutti cubi perfetti. Dimostrare che anche a, b, c, d, e, f, g sono cubi perfetti.
Soluzione
Osservazione: se un numero è un cubo perfetto, allora ogni esponente che compare nella sua fattorizzazione in fattori primi è multiplo di 3.
Sia p un numero primo e siano $k_a, k_b, k_c,\ldots, k_g$ gli esponenti con cui compare rispettivamente nella fattorizzazione dei numeri a, b, …., g; dalle condizioni iniziali del problema ricaviamo che k_a+k_b, k_b+k_c, k_c+k_d, k_d+k_e, k_e+k_f, k_f+k_g, k_g+k_a sono tutti multipli di 3, quindi si può scrivere il sistema lineare nel campo dei numeri modulo 3:

$$\begin{aligned} k_a+k_b &\equiv 0 \pmod 3 \\ k_a+k_b &\equiv 0 \pmod 3 \\ k_c+k_d &\equiv 0 \pmod 3 \\ k_d+k_e &\equiv 0 \pmod 3 \\ k_e+k_f &\equiv 0 \pmod 3 \\ k_f+k_g &\equiv 0 \pmod 3 \\ k_g+k_a &\equiv 0 \pmod 3. \end{aligned}$$

La matrice associata a tale sistema ha determinante diverso da zero e quindi è invertibile. Il sistema ha come soluzione la sola soluzione banale $k_i= 0$ per ogni i quindi ogni esponente è multiplo di 3.

Esercizi Congruenze

Esercizio 1. Qual è il resto nella divisione per 3 del numero 2014^{2014}?
Soluzione: si ha, ovviamente, $2014 \equiv 1(3)$. Dal fatto che se $a_1 \equiv b_1(m)$ e $a_2 \equiv b_2(m)$ si ha $a_1a_2 \equiv b_1b_2(m)$, consegue anche $a_1^n \equiv b_1^n(m)$. Quindi nel nostro caso $2014^{2014} \equiv 1^{2014} \equiv 1(3)$.

Esercizio 2. Dimostrare che, se n è un numero naturale non multiplo di 3, allora il numero $3^{2n} + 3^n + 1$ è multiplo di 13. Determinare inoltre il resto della divisione per 13 di tale numero, se n è multiplo di 3.
Soluzione: studiamo per esempio le congruenze modulo 13 di questa espressione nel caso in cui n = 3k+1, ricordando che $3^3 = 27 \equiv 1(13)$. Si ha: $3^{2(3k+1)} \equiv 3^2\left(3^3\right)^{2k} \equiv 9 \cdot 1^{2k} \equiv 9$; analogamente $3^{3k+1} \equiv 3(13)$. In definitiva, $3^{2n} + 3^n + 1 \equiv 9 + 3 + 1 \equiv 0(13)$. Il calcolo per n = 3k + 2 è simile, mentre per n = 3k si trova resto uguale a 3.

Esercizio 3. Calcolare $4931^{4931}(9)$, $2^{546321}(12)$.
Soluzione: primo caso: $4931 \equiv 4+9+3+1 \equiv -1(9)$. Quindi $4931^{4931} \equiv (-1)^{4931} \equiv -1 \equiv 8(9)$.
Secondo caso: in assenza di altre idee, proviamo a iniziare a calcolare le congruenze delle potenze di 2 modulo 12. Otteniamo 1, 2, 4, 8, 4, 8, 4, 8 . . . A regime, si alternano soltanto due resti. Risulta ormai evidente che la risposta è $2^{546321} \equiv 8(12)$.

Esercizio 4. Calcolare $3^{105} + 4^{105}(11)$.
Soluzione: anche in questo caso sarebbe ottimo trovare delle periodicità semplici da individuare, oppure degli 1 o -1. Cominciamo a calcolare le congruenze delle potenze di 3 modulo 11. Otteniamo 1, 3, −2, 5, 4, 1. Quindi $3^5 \equiv 1(11)$ e di conseguenza $3^{105} = 3^{5 \cdot 21} \equiv 1^{21} \equiv 1(11)$. Un calcolo analogo conduce a $4^{105} \equiv 1(11)$ e dunque infine $3^{105} + 4^{105} \equiv 2(11)$.

Esercizio 5. Trovare tutte le coppie di numeri primi *p, q* tali che $p^2 - 2q^2 = 1$. (suggerimento: una volta trovate due soluzioni al problema, mostrare che non ce ne sono altre ragionando modulo 6)
Soluzione: innanzitutto, p dev'essere dispari; p = 3 funziona con q = 2; p = 5 funziona con q = 3. Seguendo ora il suggerimento e supponendo sia p che q maggiori di 3, ogni altro primo sarà congruo a ±1 modulo 6. In entrambi i casi, il primo membro dell'equazione è congruo a -1, mentre il secondo è congruo a 1.

Esercizio 6. Dimostrare che, per n pari, $323 | 20^n + 16^n - 3^n - 1$.
Soluzione: si ha $323 = 17 \cdot 19$. Studiamo per esempio le congruenze modulo 19:
$20^n \equiv 1^n \equiv 1(19)$; $16^n \equiv (-3)^{2k} \equiv 9^k(19)$. D'altronde $3^{2k} \equiv 9^k(19)$, quindi
$20^n + 16^n - 3^n - 1 \equiv 1 + 9^k - 9^k + 1 \equiv 0(19)$. In maniera analoga si trova $20^n + 16^n - 3^n - 1 \equiv 0(17)$ e quindi $20^n + 16^n - 3^n - 1 \equiv 0(323)$.

Esercizio 7. Trovare i residui quadratici dei numeri primi maggiori di 5 modulo 30.
Soluzione: scriviamo p nella forma 30q+r, con r appartenente all'insieme {1, 7, 11, 13, 17, 19, 23, 29}. Chiaramente $p^2 \equiv r^2(30)$. Semplici calcoli mostrano che gli unici residui quadratici possibili per numeri primi maggiori di 5 sono 1 e 19.

Esercizio 8. Dimostrare che in ogni terna pitagorica almeno un termine è multiplo di 3, almeno uno è multiplo di 4, almeno uno è multiplo di 5.
Soluzione: i residui quadratici modulo 3 sono 0 e 1. Se nessuno dei tre quadrati dell'equazione fosse multiplo di 3, si avrebbe $a^2 + b^2 \equiv 1 + 1(3)$ e d'altro canto $c^2 \equiv 1(3)$, il che chiaramente non è possibile. Osservazioni analoghe permettono di dimostrare i casi modulo 4 e 5.

Esercizio 9. Trovare il più piccolo numero naturale k tale che in Z_{2013} si abbia 700k = 11.
Soluzione: questo è il classico esercizio su Teorema di Bezout e algoritmo euclideo. Dopo qualche calcolo si trova come inverso moltiplicativo di 700 la classe -509, che moltiplicata per 11 e riportata al rappresentante privilegiato diventa 440.