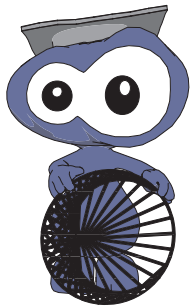
Laboratorio teorico-pratico per la preparazione alle gare di matematica

Ercole Suppa

Liceo Scientifico A. Einstein, Teramo
e-mail: ercolesuppa@gmail.com

Teramo, 10 dicembre 2014



TEORIA DEI NUMERI

- Sistemi di numerazione
- Divisibilità, numeri primi, fattorizzazione
- MCD, MCM, teorema di Bezout
- Algoritmo euclideo
- Algoritmo euclideo esteso
- Aritmetica modulare
- Funzione di Eulero
- Piccolo teorema di Fermat e teorema di Eulero
- Congruenze simultanee e teorema cinese dei resti
- Equazioni diofantee lineari
- Struttura moltiplicativa di $\mathbb{Z}_p$ (p primo)
- Equazione di Pell e equazioni diofantee di secondo grado

Teorema. Fissato un intero $b > 1$ possiamo rappresentare un numero naturale $a > 0$ in modo unico nella forma seguente

$$a = r_n b^n + r_{n-1} b^{n-1} + \cdots + r_1 b + r_0 \qquad (\star)$$

con $0 \leq r_i < b$ per ogni $i \in \{0, 1, \ldots, n\}$ e con $r_n > 0$.

La scrittura $(\star)$ è chiamata *rappresentazione di a in forma polinomiale* e viene indicata con la notazione

$$a = (r_n r_{n-1} \cdots r_1 r_0)_b$$

oppure con

$$a = (\overline{r_n r_{n-1} \cdots r_1 r_0})_b$$

Se $b = 10$ si ha la *rappresentazione decimale* e il pedice 10 viene omesso

$$a = \overline{r_n r_{n-1} \cdots r_1 r_0} = r_n 10^n + r_{n-1} 10^{n-1} + \cdots + r_1 10 + r_0$$

Algoritmo della divisione. Dati $a, b \in \mathbb{Z}$ con $b \neq 0$ esistono due unici numeri $q, r \in \mathbb{Z}$ tali che:

$$a = bq + r, \qquad 0 \leq r < |b|$$

Divisibilità. Nel caso in cui $r = 0$, ossia se $a = bq$, diciamo che b divide a e scriviamo $b \mid a$.

Numeri primi. Un *numero primo* è un intero maggiore di 1 che ha come divisori positivi soltanto 1 e se stesso.

Teorema fondamentale dell'aritmetica. Ogni intero $n > 1$ si può scrivere nella forma:

$$n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_k^{\alpha_k}$$

dove $p_1, p_2, \ldots, p_k$ sono primi distinti e $\alpha_1, \alpha_2, \ldots, \alpha_k$ sono interi maggiori o uguali a uno. Tale scrittura è detta *fattorizzazione di n in fattori primi* ed è unica a meno dell'ordine dei fattori.

Massimo comun divisore. Si dice *massimo comun divisore* di n numeri interi positivi $a_1, a_2, \cdots, a_n$ il più grande intero positivo che divide tutti gli a_i. Il massimo comun divisore di $a_1, a_2, \cdots, a_n$ si indica con $\mathrm{MCD}(a_1, a_2, \ldots, a_n)$. Il massimo comun divisore di due interi a e b si indica con la notazione abbreviata (a, b). Due interi a e b si dicono *primi fra loro* o *coprimi* se $(a, b) = 1$.

Fattorizzazione del MCD**.** La fattorizzazione del MCD contiene *tutti* e *soli* i fattori primi che compaiono in tutte le singole fattorizzazioni, ciascuno elevato al minimo esponente.

Teorema di Bezout. Se $a, b \in \mathbb{Z}$ e $d = (a, b)$, esistono $m, n \in \mathbb{Z}$ tali che:

$$d = ma + nb$$

Minimo comune multiplo. Si dice *minimo comune multiplo* di n numeri interi positivi $a_1, a_2, \cdots, a_n$ il più piccolo intero positivo che è divisibile per tutti gli a_i. Il minimo comune multiplo di $a_1, a_2, \cdots, a_n$ si indica con $\mathrm{MCM}(a_1, a_2, \ldots, a_n)$. Il minimo comune multiplo di due interi a e b si indica con $[a, b]$.

Fattorizzazione del MCM**.** La fattorizzazione del MCM contiene tutti e soli i fattori primi che compaiono in almeno una delle singole fattorizzazioni, ciascuno elevato al massimo esponente.

Relazione tra MCD e MCM. Per ogni $a, b \in \mathbb{Z}$ si ha

$$(a, b)[a, b] = ab$$

Algoritmo euclideo

Dati due interi a, b si dimostra facilmente che se $a = bq + r$ con $0 \leq r < |b|$ allora $\text{MCD}(a, b) = \text{MCD}(b, r)$. Pertanto il MCD di a e b può essere determinato con il seguente algoritmo ricorsivo:

(1) Se uno dei due numeri è uguale a 0, l'altro numero è il MCD di (a, b).

(2) Altrimenti eseguire la divisione euclidea e scrivere $a = bq + r$, con $0 \leq r < |b|$

(3) Rimpiazzare la coppia (a, b) con la coppia (b, r).

(4) Tornare al punto (1)

Ad ogni passo il secondo elemento della coppia diventa più piccolo, per cui il procedimento terminerà dopo un numero finito di passi, fornendo il MCD di a e b.

Come esempio applichiamo l'algoritmo euclideo per calcolare il massimo comun divisore tre 348 e 124:

a	b	q	r
348	124	2	100
124	100	1	24
100	24	4	4
24	4	6	0

Pertanto

$$(348, 124) = (124, 100) = (100, 24) = (24, 4) = (4, 0)$$

e quindi $\mathrm{MCD}(348, 124) = 4$.

Algoritmo euclideo esteso

E' un algoritmo più efficiente di quello euclideo che fornisce direttamente i coefficienti della rappresentazione del MCD come combinazione lineare dei due numeri.
Illustriamo tale algoritmo con un esempio, calcolando il massimo comun divisore di $a = 348$ e $b = 124$.

x	y	$ax + by$	q	r
1	0	348	-	-
0	-1	-124	2	100
1	-2	100	1	24
1	-3	-24	4	4
5	-14	4	6	0

Dall'ultima riga della tabella si evince che

$$4 = 5 \times 348 + (-14) \times 124$$

In alcuni casi, per fare in modo che il MCD sia positivo, può essere necessario moltiplicare l'ultima equazione per -1.

Relazione di conguenza. Sia $m > 1$ un numero intero fissato. Due numeri $a, b \in \mathbb{Z}$ si dicono *congrui modulo* m e si scrive:

$$a \equiv b \pmod{m}$$

se $m \mid a - b$. Si dimostra facilmente che $a \equiv b \pmod{m}$ se e solo se a e b divisi per m danno lo stesso resto.

Classe di congruenza. Si dice *classe di congruenza* (*modulo* m) di un intero a l'insieme di tutti gli interi congrui ad a modulo m:

$$[a] = \{b \in \mathbb{Z} \mid b \equiv a \pmod{m}\}$$

Ogni classe di congruenza contiene un unico elemento x, detto *rappresentante canonico*, tale che $0 \leq x < m$.

La relazione di congruenza gode delle proprietà *riflessiva*, *simmetrica*, *transitiva* ed è *compatibile* con le operazioni di somma e prodotto, ossia se

$$a \equiv b \pmod{m}, \qquad c \equiv d \pmod{m}$$

allora:

- $a + c \equiv b + d \pmod{m}$
- $a - c \equiv b - d \pmod{m}$
- $ac \equiv bd \pmod{m}$
- $a^k \equiv b^k \pmod{m}, \qquad \forall k \in \mathbb{N}$
- $ka \equiv kb \pmod{m}$ e $(k, m) = 1 \quad \Rightarrow \quad a \equiv b \pmod{m}$.

Inverso modulo m. Si dice che un intero a è *invertibile* $\pmod m$ se esiste un intero b tale che

$$ab \equiv 1 \pmod m$$

ed in tal caso b è detto l'*inverso* di $a \pmod m$.

Criterio di invertibilità.
Un intero a è *invertibile* $\pmod m$ se e solo se $(a, m) = 1$.

Dimostrazione. Per il teorema di Bezout $(a, m) = 1$ se e solo se esistono $h, k \in \mathbb{Z}$ tali che:

$$ha + km = 1 \quad \Leftrightarrow \quad ah \equiv 1 \pmod m$$

Funzione di Eulero. Si dice *funzione φ di Eulero* la funzione che ad ogni intero $n > 1$ associa il numero degli interi $0 < a < n$ che sono relativamente primi con n, ossia

$$\varphi(n) = |\{a \in \mathbb{N} : 0 < a < n, (a, n) = 1\}|$$

Proprietà della funzione di Eulero.

- φ è una funzione *moltiplicativa* ossia se $(a, b) = 1$ allora

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

- se p è un numero primo $\varphi(p) = p - 1$
- se p è un numero primo ed $\alpha \in \mathbb{N}$: $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$
- se $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ allora

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right) \cdot \left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_k}\right)$$

Piccolo teorema di Fermat. Se $a \in \mathbb{Z}$ e p è un primo tale che $p \nmid a$ si ha:

$$a^{p-1} \equiv 1 \pmod{p}$$

Corollario. Se $a \in \mathbb{Z}$ e p è un primo si ha:

$$a^{p} \equiv a \pmod{p}$$

Teorema di Eulero. Se $a \in \mathbb{Z}$ ed $(a, m) = 1$ allora

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

Sistema di congruenze. Se $m_1, \ldots, m_k, a_1, \ldots, a_k \in \mathbb{Z}$, si dice *sistema di congruenze* un sistema della forma:

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \vdots \\ x \equiv a_k \pmod{m_k} \end{cases} \qquad (\star)$$

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

Teorema cinese dei resti. Se $m_1, m_2, \ldots, m_k \in \mathbb{Z}$ a due a due coprimi, allora il sistema $(\star)$ ammette una soluzione che è *unica* modulo $m_1 m_2 \cdots m_k$.

Costruzione della soluzione del sistema ($\star$). Per ogni $i \in \{1, 2, \ldots, k\}$ poniamo

$$b_i = \prod_{j \neq i} m_j$$

e indichiamo con c_i l'inverso di b_i modulo m_i. Allora una soluzione del sistema $(\star)$ è data da

$$x_0 = \sum_{i=1}^{k} a_i b_i c_i$$

Tutte le altre soluzioni sono della forma:

$$x = x_0 + t \cdot m_1 m_2 \cdots m_k \qquad , \qquad t \in \mathbb{Z}$$

Equazioni diofantee lineari

Un'**equazione diofantea** è un'equazione in una o più incognite con coefficienti interi di cui si ricercano le soluzioni intere

Un'equazione **diofantea lineare** in due variabili è un'equazione della forma

$$ax + by = c$$

dove $a, b, c \in \mathbb{Z}$. Risolvere tale equazione significa trovare tutte le coppie (x, y) di numeri interi che la soddisfano.

L'equazione diofantea $ax + by = c$ si dice *omogenea* se $c = 0$, si dice *completa* se $c \neq 0$.

Esistenza di soluzioni. Un'equazione diofantea completa

$$ax + by = c \qquad (\star)$$

ammette soluzioni se e solo se $(a, b) \mid c$.

In tal caso, dividendo per $d = (a, b)$ ambo i membri della $(\star)$, possiamo supporre senza perdita di generalità che $(a, b) = 1$.

Teorema. Se $(a, b) = 1$ esistono $x_0, y_0 \in \mathbb{Z}$ tali che

$$ax_0 + by_0 = c$$

Dimostrazione. Per il teorema di Bezout esistono $m, n \in \mathbb{Z}$ tali che $ma + nb = 1$ quindi, posto $x_0 = mc$, $y_0 = nc$, abbiamo

$$ax_0 + by_0 = c$$

Soluzione dell'equazione completa con $(a, b) = 1$

$$ax + by = c$$

- trovare $m, n \in \mathbb{Z}$ tali che $am + bn = 1$
- una soluzione particolare è data da:

$$x_0 = cm \quad , \quad y_0 = cn$$

- la soluzione generale è data da:

$$\begin{cases} x = x_0 + bt \\ y = y_0 - at \end{cases} \quad , \quad \forall t \in \mathbb{Z}$$