FORMULARIO: TEORIA DEI NUMERI

In ogni riquadro: il teorema con le sue ipotesi e un esempio con i numeri.

1 Divisibilità, MCD, Bézout

1.1 Divisibilità

$$a \mid b \iff \exists k \in \mathbb{Z} : b = ak$$

La **cosa piccola sta a sinistra**. Proprietà chiave (combinazioni lineari): se $a \mid b$ e $a \mid c$, allora $a \mid (bx + cy)$ per ogni x, y.

ESEMPIO

$3 \mid 12$ vero, $12 \mid 3$ falso. $5 \mid 15$ e $5 \mid 20 \Rightarrow 5 \mid (15 \cdot 2 + 20 \cdot 3)$.

1.2 Divisione euclidea

$$a = dq + r \qquad \text{con } 0 \le r < d$$

Quoziente e resto sono **unici**, e il resto non è mai negativo — nemmeno con a negativo.

ESEMPIO

$47 = 5 \cdot 9 + 2$ $\qquad -47 = 5 \cdot (-10) + 3$ (non -2)

1.3 Algoritmo di Euclide

Si divide, si tiene il resto, si ripete: l'**ultimo resto non nullo** è il MCD. Si regge su

$$\text{MCD}(a, d) = \text{MCD}(d, r) \quad \text{se } a = dq + r$$

ESEMPIO

$1071 = 2 \cdot 462 + 147$; $462 = 3 \cdot 147 + 21$; $147 = 7 \cdot 21 + 0 \Rightarrow \text{MCD} = 21$.

1.4 MCD e mcm

$$\text{MCD}(a, b) \cdot \text{mcm}(a, b) = a \cdot b$$

Trovato il MCD con Euclide, il mcm viene gratis.

ESEMPIO

$\text{MCD}(12, 18) = 6 \Rightarrow \text{mcm} = \dfrac{12 \cdot 18}{6} = 36$.

1.5 Identità di Bézout

Esistono sempre x, y interi con

$$ax + by = \text{MCD}(a, b)$$

Si trovano con **Euclide esteso**: si risale l'algoritmo sostituendo i resti, senza mai moltiplicare a e b.

ESEMPIO

$21 = 1071 \cdot (-3) + 462 \cdot 7$ (controllo: $-3213 + 3234 = 21$)

1.6 Coprimi

$$\text{MCD}(a, b) = 1 \iff \exists\, x, y : ax + by = 1$$

È la chiave dell'inverso modulare.

ESEMPIO

7 e 26: $26 \cdot 3 - 7 \cdot 11 = 1$, quindi sono coprimi.

1.7 Equazioni diofantee $ax + by = c$

Ha soluzioni **se e solo se** $\text{MCD}(a, b) \mid c$, e allora sono infinite:

$$x = x_0 + \frac{b}{d}\,t, \qquad y = y_0 - \frac{a}{d}\,t, \qquad t \in \mathbb{Z}$$

ESEMPIO

$6x + 15y = 9$: $d = 3 \mid 9$ sì. $x = -1 + 5t,\ y = 1 - 2t$.
$6x + 15y = 7$: $3 \nmid 7 \Rightarrow$ nessuna soluzione.

2 Primi e divisori

2.1 Teorema fondamentale e lemma di Euclide

Ogni $n > 1$ si fattorizza in primi in modo **unico**. E se p è primo:

$$p \mid ab \ \Rightarrow\ p \mid a \text{ oppure } p \mid b$$

Falso per i non primi: $6 \mid 4 \cdot 9$ ma $6 \nmid 4$ e $6 \nmid 9$.

ESEMPIO

$360 = 2^3 \cdot 3^2 \cdot 5$

2.2 Fino a dove provare

Per sapere se n è primo bastano i divisori fino a $\sqrt{n}$: se $n = ab$ con $a \leq b$, allora $a \leq \sqrt{n}$.

ESEMPIO

211: si prova fino a 14 $(2, 3, 5, 7, 11, 13)$. Nessuno divide: è primo.

2.3 Numero dei divisori

Se $n = p_1^{a_1} \cdots p_k^{a_k}$:

$$d(n) = (a_1 + 1)(a_2 + 1) \cdots (a_k + 1)$$

Ogni divisore si costruisce scegliendo un esponente per ogni primo, da 0 ad a_i.

ESEMPIO

$360 = 2^3 3^2 5 \Rightarrow d(360) = 4 \cdot 3 \cdot 2 = 24$

2.4 Somma dei divisori

$$\sigma(n) = \prod_i (1 + p_i + p_i^2 + \cdots + p_i^{a_i}) = \prod_i \frac{p_i^{a_i+1} - 1}{p_i - 1}$$

ESEMPIO

$\sigma(360) = (1{+}2{+}4{+}8)(1{+}3{+}9)(1{+}5) = 15 \cdot 13 \cdot 6 = 1170$

2.5 Quando $d(n)$ è dispari

I divisori si accoppiano (a con n/a), e coincidono solo se $n = a^2$:

$$d(n) \text{ dispari} \iff n \text{ è un quadrato perfetto}$$

ESEMPIO

$d(36) = 9$ (dispari, e $36 = 6^2$); $d(35) = 4$ (pari).

2.6 Funzione di Eulero

$\varphi(m)$ = quanti numeri da 1 a m sono coprimi con m:

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

Per p primo: $\varphi(p) = p - 1$ e $\varphi(p^a) = p^a - p^{a-1}$.

ESEMPIO

$\varphi(100) = 100 \cdot \frac{1}{2} \cdot \frac{4}{5} = 40 \qquad \varphi(7) = 6$

3 Congruenze

3.1 Definizione

$$a \equiv b \pmod{m} \iff m \mid (a-b)$$

cioè a e b danno lo **stesso resto** diviso m.

ESEMPIO

$17 \equiv 2 \pmod{5}$ perché $5 \mid 15$.

3.2 Le regole che valgono

Da $a \equiv b$ e $c \equiv e \pmod{m}$:

$$a+c \equiv b+e, \qquad ac \equiv be, \qquad a^n \equiv b^n$$

Somma, prodotto e potenza sì. **La divisione no.**

ESEMPIO

$17 \cdot 23 \equiv 2 \cdot 3 = 6 \equiv 1 \pmod{5}$ (e infatti $391 = 5 \cdot 78 + 1$).

3.3 Semplificare: quando si può

Da $ac \equiv bc \pmod{m}$ si toglie c **solo se** $\text{MCD}(c, m) = 1$; se no si divide anche il modulo.

ESEMPIO

$6 \equiv 2 \pmod{4}$ **non** dà $3 \equiv 1 \pmod{4}$ (falso): qui $\text{MCD}(2,4) = 2$, e si passa a modulo 2.

3.4 Criteri di divisibilità, dimostrati

$$10 \equiv 1 \pmod{3), 9} \Rightarrow n \equiv \text{somma delle cifre}$$

$$10 \equiv -1 \pmod{11} \Rightarrow n \equiv \text{somma a segni alterni}$$

ESEMPIO

4725: somma cifre 18, divisibile per 9. 918082: $2-8+0-8+1-9 = -22$, divisibile per 11.

3.5 Inverso modulare

$$a\,a^{-1} \equiv 1 \pmod{m} \quad \text{esiste} \iff \text{MCD}(a, m) = 1$$

Si trova con Euclide esteso: da $ax + my = 1$ segue $a^{-1} = x$.

ESEMPIO

$7^{-1} \equiv 15 \pmod{26}$ perché $7 \cdot 15 = 105 = 4 \cdot 26 + 1$.

3.6 Risolvere $ax \equiv b \pmod{m}$

Sia $d = \text{MCD}(a, m)$:

- $d \nmid b$: nessuna soluzione;
- $d = 1$: una classe, $x \equiv a^{-1}b$;
- $d \mid b$: si divide tutto per d (modulo compreso), e le soluzioni modulo m sono d.

ESEMPIO

$7x \equiv 3 \pmod{26} \Rightarrow x \equiv 15 \cdot 3 = 45 \equiv 19$.

4 I tre teoremi grossi

4.1 Piccolo teorema di Fermat

Se p è **primo** e $p \nmid a$:

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

Sempre valido, anche se $p \mid a$: $a^p \equiv a \pmod{p}$.

ESEMPIO

$2^{100} \bmod 13$: $2^{12} \equiv 1$, e $100 = 12 \cdot 8 + 4$, quindi $\equiv 2^4 = 16 \equiv 3$.

4.2 Teorema di Eulero

Se $\text{MCD}(a, m) = 1$:

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

È Fermat generalizzato ai moduli non primi.

ESEMPIO

$3^{40} \equiv 1 \pmod{100}$, perché $\varphi(100) = 40$: le ultime due cifre sono 01.

4.3 Teorema cinese del resto

Con moduli **a due a due coprimi**, il sistema $x \equiv r_i \pmod{m_i}$ ha una sola soluzione modulo $m_1 m_2 \cdots m_k$. Si risolve per **sostituzione**: da una congruenza si ricava $x = r_1 + m_1 t$ e si mette nella successiva.

ESEMPIO

$x \equiv 2(3), x \equiv 3(5), x \equiv 2(7) \Rightarrow x \equiv 23 \pmod{105}$.

Le potenze modulo m: come si riducono

Se	allora	esempio
m primo, $m \nmid a$	esponente modulo $m-1$	$2^{100} \equiv 2^4 \pmod{13}$
$\text{MCD}(a,m) = 1$	esponente modulo $\varphi(m)$	$3^{40} \equiv 1 \pmod{100}$
nessuna delle due	si cerca il ciclo a mano	$7^1, 7^2, 7^3, 7^4 \pmod{10}$

I sei errori che costano di più

- Leggere $a \mid b$ al contrario.
- Semplificare una congruenza per un numero non coprimo col modulo.
- Usare Fermat con modulo **non** primo, o senza $p \nmid a$.
- Dire che $ax + by = c$ ha soluzioni senza controllare $\text{MCD}(a,b) \mid c$.
- Dare *una* soluzione di una diofantea invece della famiglia.
- Confondere $d(n)$ (quanti divisori) con $\sigma(n)$ (quanto fanno sommati).