Pillole di Teoria dei Numeri

G.a.u.s.S. – Gruppo Allenatori Universitari Studenti della Sapienza
a cura di
Danilo Ciaffi

In questa scheda daremo per scontato che tutti i numeri siano interi (positivi o negativi).

Divisibilità

1. Un numero n si dice *primo* se i suoi unici divisori sono ± 1 e $\pm n$, *composto* altrimenti.
   Attenzione: se d è un divisore di n allora lo è anche $-d$, quindi attenzione quando si fa la conta dei divisori di un numero.

2. Ogni numero n può essere scritto in modo unico come prodotto di potenze di primi, cioè

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

3. Un numero è divisibile per:

   - 2^n se le sue ultime n cifre sono divisibili per 2^n;
   - 3 se la somma delle sue cifre è divisibile per 3;
   - 5^n se le sue ultime n cifre sono divisibili per 5^n;
   - 7 se la differenza tra il numero ottenuto escludendo la cifra delle unità e il doppio dell'ultima cifra è divisibile per 7 (ad esempio $217 \to 21 - 2 \cdot 7 = 7$ che è divisibile per 7);
   - 9 se la somma delle sue cifre è divisibile per 9;
   - 11 se la somma delle sue cifre a segno alterno è divisibile per 11 (ad esempio $9141 \to 9-1+4-1 = 11$);

4. Dati m e n, si dice:

   - *minimo comune multiplo* $mcm(m, n)$ il più piccolo intero che è multiplo sia di m che di n, ed esso è divisore di ogni altro numero che sia multiplo di entrambi;
   - *massimo comun divisore* $MCD(m, n)$ il più grande intero che è divisore sia di m che di n, ed esso è multiplo di ogni altro numero che sia divisore di entrambi;
   - m ed n sono coprimi se $MCD(m, n) = 1$.

   Si osservi che $mn = MCD(m, n) \cdot mcm(m, n)$.

5. **Identità di Bézout**: Presi comunque m, n e posto $d = MCD(m, n)$, esistono sempre due interi (con segno!) h e k tali che $mh + nk = d$.

   Osservazioni: Poiché il massimo comun divisore tra due numeri divide anche la loro differenza, d è il più piccolo dei numeri della forma $mh + nk$, ma tutti gli altri saranno suoi multipli. Questo vuol dire che un'equazione negli interi x e y del tipo $mx + ny = c$ (queste equazioni si chiamano *diofantee lineari*) ammette soluzione se e solo se c è divisibile per d.

Congruenze

1. Si di ce che a è *congruo* a b modulo m se a e b danno lo stesso resto nella divisione per m, e si scrive $a \equiv b \pmod{m}$.

2. Se $a_1 \equiv a_2$ e $b_1 \equiv b_2 \pmod{m}$, allora:

   - $a_1 + b_1 \equiv a_2 + b_2 \pmod{m}$
   - $a_1 - b_1 \equiv a_2 - b_2 \pmod{m}$
   - $a_1 \cdot b_1 \equiv a_2 \cdot b_2 \pmod{m}$

   Attenzione: La divisione non funziona bene come le altre operazioni a meno che m non sia un numero primo.

3. I *residui quadratici* modulo m sono le classi di congruenza dei quadrati perfetti. Alcuni tra i più importanti sono:

   - Modulo 3: 0,1;
   - Modulo 4: 0 (i pari), 1 (i dispari);
   - Modulo 5: 0, 1,−1;
   - Modulo 10: 0, 1, 4, 6, 9;

4. Si dicono *equazioni lineari* tutte le equazioni della forma $ax \equiv b \pmod{m}$. Esse ammettono soluzione soltanto se $MCD(a, m)$ divide b (c'entra qualcosa l'identità di Bézout?), ma per il resto si risolvono come immaginate.

5. **Piccolo Teorema di Fermat**: Se p è un numero primo e a non è divisibile per p, allora

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

6. **Teorema Cinese del Resto**: Siano $m_1, m_2, ...m_n$ numeri naturali maggiori di 1 due a due coprimi e $a_1, a_2, ..., a_n$ interi relativi. Allora il sistema di congruenze

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \vdots \\ x \equiv a_n \pmod{m_n} \end{cases}$$

   Ammette sempre un'unica soluzione modulo $m_1 \cdot m_2 \cdot ... \cdot m_n$.

   Per *trovare* questa soluzione si parte dalla prima equazione: essa ci dice che

$$x = k_1 \cdot m_1 + a_1$$

   per qualche intero k_1. Usiamo questo risultato nella seconda equazione:

$$x = k_1 \cdot m_1 + a_1 \equiv a_2 \pmod{m_2}.$$

   Allora, indicando con m_1' l'inverso di m_1, si ha

$$k_1 \cdot m_1 + a_2 \equiv a_2$$

   cioè

$$k_1 \equiv m_1' \cdot a_2 - a_1$$

   ossia, per un qualche k_2,

$$k_1 = m_2 \cdot k_2 + m_1'(a_2 - a_1)$$

   Sostituendo questo valore di k_1 nell'espressione ottenuta dalla prima equazione e iterando il procedimento, si troverà la classe di resto modulo $m_1 \cdot m_2 \cdot ... \cdot m_n$ della soluzione.