ARITMETICA (II PARTE)

Prop: Dati $a, b, q, r \in \mathbb{Z}$ t.c. $a = b \cdot q + r$ allora i divisori comuni ad a e b coincidono con i divisori comuni a b ed r.
In particolare: $MCD(a,b) = MCD(b,r)$.

Dim: Sia $d \in \mathbb{Z}$ t.c. $d | a$ e $d | b$. Allora $\exists \alpha, \beta \in \mathbb{Z}$ t.c. $a = d\alpha$ e $b = d \cdot \beta$
Ma allora la relazione $a = bq + r$ si riscrive $d\alpha = d\beta q + r$, quindi

$$r = d\alpha - d\beta q = d(\alpha - \beta q) \Rightarrow d | r.$$

Viceversa, sia $d \in \mathbb{Z}$ t.c. $d | b$ e $d | r$. Allora $\exists \beta, \rho \in \mathbb{Z}$ t.c. $b = d \cdot \beta$ e $r = d \cdot \rho$.
Ma allora $a = bq + r$ diventa $a = d\beta q + d\rho = d(\beta q + \rho) \Rightarrow d | a$. $\boxtimes$

Algoritmo euclideo

Partiamo da $a, b \in \mathbb{Z}$ con $b \neq 0$ e procediamo con la divisione euclidea:

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

Sappiamo che $MCD(a,b) = MCD(b,r)$

procediamo dividendo b per r:

$$b = r \cdot q_1 + r_1 \qquad 0 \leq r_1 < r$$

inoltre $MCD(b,r) = MCD(r, r_1)$ è più facile da calcolare

Costruiamo così una successione di quozienti $q_1, q_2, \dots$ e resti $r_1, r_2 \dots$ con le proprietà:

(i) $MCD(a,b) = MCD(b,r) = MCD(r,r_1) = \dots = MCD(r_n, r_{n+1}) = \dots$

(ii) $|b| > r > r_1 > r_2 > \dots > r_n > \dots \geq 0$

La seconda successione ha termine. Cioè $\exists\, n \in \mathbb{N}$ t.c. $r_{n+1} = 0$.

Ma allora $r_{n-1} = r_n \cdot q_{n+1} + 0 \implies MCD(r_{n-1}, r_n) = MCD(r_n, 0) = r_n$

Perciò $r_n = MCD(r_{n-1}, r_n) = MCD(r_{n-2}, r_{n-1}) = \dots = MCD(b,r) = MCD(a,b)$.

Esempio: $MCD(2702, 324) = ?$ $\quad a = 2702 \quad b = 324$

$$\begin{array}{r} 2702 : 324 = 8 \quad q \\ 2592 \\ \hline 110 \quad r \end{array}$$

$$2702 = 324 \cdot \underbrace{8}_{q} + \underbrace{110}_{r}$$

$$324 = 110 \cdot \underbrace{2}_{q_1} + \underbrace{104}_{r_1}$$

$$110 = 104 \cdot \underbrace{1}_{q_2} + \underbrace{6}_{r_2}$$

$$104 = 6 \cdot \underbrace{17}_{q_3} + \underbrace{2}_{r_3} \implies MCD(2702, 324) = 2$$

$$6 = 2 \cdot 3 + \underbrace{0}_{r_4}$$

Teorema (Identità di Bézout): Siano $a, b \in \mathbb{Z}$ e $d = MCD(a,b)$. Allora esistono $x, y \in \mathbb{Z}$ tali che
$$d = ax + by.$$

Vediamo l'applicazione all'esempio precedente ($a=2702$, $b=324$, $d=2$). "Invertiamo" i risultati delle divisioni:

$$2 = 104 - 6 \cdot 17 \longrightarrow 2 = 104 - (110 - 104) \cdot 17$$
$$6 = 110 - 104 \qquad = 104(1+17) - 110 \cdot 17 = 104 \cdot 18 - 110 \cdot 17$$
$$104 = 324 - 2 \cdot 110 \qquad = (324 - 2 \cdot 110) \cdot 18 - 110 \cdot 17 = 324 \cdot 18 - 110 \cdot (2 \cdot 18 + 17)$$
$$110 = 2702 - 8 \cdot 324 \qquad = 324 \cdot 18 - 110 \cdot 53$$
$$= 324 \cdot 18 - (2702 - 8 \cdot 324) \cdot 53$$
$$= 324 \cdot (18 + 8 \cdot 53) - 2702 \cdot 53$$

Conclusione: $\boxed{2 = 2702 \cdot (-53) + 324 \cdot 442}$ $\quad (x = -53,\ y = 442)$

Nel teorema precedente, x e y <u>non sono unici</u>!

<u>Es</u>: $a = 6$, $b = 9$ $\quad MCD(6,9) = 3$

$$3 = -6 + 9 = 6 \cdot (-1) + 9 \cdot 1 \qquad (x,y) = (-1,1)$$
$$3 = 12 - 9 = 6 \cdot 2 + 9 \cdot (-1) \qquad (x,y) = (2,-1)$$
$$3 = 6 \cdot (-4) + 9 \cdot 3 \qquad (x,y) = (-4,3)$$
$$\dots \qquad \dots$$

sono tutte le soluzioni dell'equazione diofantea $6x + 9y = 3$ $\longleftarrow$

Corollario: Dati $a, b, c \in \mathbb{Z}$, l'equazione
$$ax + by = c$$
ha soluzioni $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ se e solo se $MCD(a, b) \mid c$.

Es: $2702x + 324y = 4$ ha soluzioni? Sì perché $MCD(2702, 324) = 2 \mid 4$

Per trovare x e y basta moltiplicare per 2 l'identità di Bézout

Es: $2702x + 324y = 3$ non ha soluzioni.

Notazione posizionale

Che cosa significa la scrittura 1238?

$$1238 = 8 + 3 \cdot 10 + 2 \cdot 100 + 1 \cdot 1000 = 8 \cdot 10^0 + 3 \cdot 10^1 + 2 \cdot 10^2 + 1 \cdot 10^3$$

$$\begin{aligned} 1238 &= 123 \cdot 10 + \boxed{8} \\ 123 &= 12 \cdot 10 + \boxed{3} \\ 12 &= 1 \cdot 10 + \boxed{2} \\ 1 &= 0 \cdot 10 + \boxed{1} \end{aligned}$$

Def: Sia $b \geq 2$ un intero, detto base e $\mathcal{C}$ un insieme di cifre o simboli rappresentanti gli interi da 0 a $b-1$. La notazione posizionale di $n \in \mathbb{N}$ in base b è la stringa di cifre $n = c_s c_{s-1} \dots c_1 c_{0\,[b]}$ $(c_i \in \mathcal{C})$ univocamente determinata dalla proprietà: $n = c_0 \cdot b^0 + c_1 \cdot b^1 + \dots + c_{s-1} \cdot b^{s-1} + c_s \cdot b^s$.

Es: $1238 = ?_2$

$$
\begin{aligned}
1238 &= 619 \cdot 2 + 0 \\
619 &= 309 \cdot 2 + 1 \\
309 &= 154 \cdot 2 + 1 \\
154 &= 77 \cdot 2 + 0 \\
77 &= 38 \cdot 2 + 1 \\
38 &= 19 \cdot 2 + 0 \\
19 &= 9 \cdot 2 + 1 \\
9 &= 4 \cdot 2 + 1 \\
4 &= 2 \cdot 2 + 0 \\
2 &= 1 \cdot 2 + 0 \\
1 &= 0 \cdot 2 + 1
\end{aligned}
$$

$1238_{10} = 10011010110_2$

$10011010110_2 = 1 \cdot 2^1 + 1 \cdot 2^2 + 2^4 + 2^6 + 2^7 + 2^{10} =$
$= 2 + 4 + 16 + 64 + 128 + 1024 = 1238$

$1238 = ?_{16}$

$$
\begin{aligned}
1238 &= 77 \cdot 16 + 6 \\
77 &= 4 \cdot 16 + 13 = D \\
4 &= 0 \cdot 16 + 4
\end{aligned}
$$

$1238_{10} = 4D6_{16}$

Def: Un numero $n \in \mathbb{Z}$, $n \notin \{0,+1,-1\}$ si dice:

- irriducibile se $n = a \cdot b \quad (a,b \in \mathbb{Z}) \Rightarrow a = \pm 1 \vee b = \pm 1$
- primo se $n \mid ab \quad (a,b \in \mathbb{Z}) \Rightarrow n \mid a \vee n \mid b$

Teorema: $n \in \mathbb{Z}$ $n \notin \{0,+1,-1\}$ è primo se e solo se è irriducibile.

Dim: "se". Sia n irriducibile. Supponiamo $n \mid ab$ e scriviamo $ab = nk$ $(k \in \mathbb{Z})$. Se $n \mid a$ abbiamo finito.
Se $n \nmid a$, allora poiché n è irriducibile $\Rightarrow MCD(a,n) = 1$
Per l'identità di Bézout, $\exists x,y \in \mathbb{Z}$ t.c. $1 = ax + ny$
Moltiplichiamo per b: $\quad b = bax + bny = nkx + bny = n(kx + by) \Rightarrow n \mid b \Rightarrow n$ primo.

"solo se". Sia n primo e valga $n = a \cdot b \Rightarrow n \mid a \cdot b \Rightarrow$ poiché n primo $n \mid a \vee n \mid b$.
Supponiamo $n \mid a \Rightarrow a = n \cdot k \quad (k \in \mathbb{Z}) \Rightarrow \cancel{n} = a \cdot b = \cancel{n} k b \Rightarrow 1 = k \cdot b \Rightarrow k = b = \pm 1$
$\Rightarrow n$ irriducibile.

Teorema (fondamentale dell'Aritmetica): $n \in \mathbb{Z}$, $n \notin \{0,+1,-1\}$ si fattorizza in modo essenzialmente unico come prodotto di primi.

$$n = \pm p_1 \cdot p_2 \cdot \ldots \cdot p_s \qquad (p_i \text{ primi } > 0).$$

Dim: Esistenza: Dimostriamo per $n>0$ $(n\geq 2)$ (per i negativi basta cambiare segno).

Passo base: $n=2$ $\quad 2=2 \quad s=1 \quad p_1=2$.

Passo induttivo: supponiamo l'enunciato valido $\forall x \in \mathbb{Z}$ $\quad 2\leq x\leq n-1$.

Se n primo $\Rightarrow$ n irriducibile $\Rightarrow$ $p_1=n$ fine.

Se n non è primo $\Rightarrow$ n riducibile $\quad n=a\cdot b \quad a,b\neq \pm 1$.

Allora applico l'ipotesi induttiva su a e b. (che sono $< n$)

$$a=p_1\cdot p_2\cdot\ldots\cdot p_j \quad ; \quad b=q_1q_2\cdots q_k$$

$$n=ab=p_1 p_2\cdots p_j\cdot q_1 q_2\cdot\ldots\cdot q_k .$$

Unicità: Sia $n=p_1\cdot p_2\cdot\ldots\cdot p_s=q_1q_2\cdots q_t$. Possiamo sempre supporre $s\leq t$

$p_1 \mid n=q_1q_2\cdots q_t \Rightarrow$ poiché p_1 è primo $\exists q_i$ t.c. $p_1 \mid q_i$

Ma q_i è irriducibile $\Rightarrow$ $p_1=q_i$ e riordinando possiamo supporre $p_1=q_1$

quindi $\quad \cancel{p_1}p_2\cdots p_s=\cancel{p_1}\cdot q_2\cdots q_t$

Ripetiamo il procedimento e otteniamo $p_2=q_2 \ldots p_s=q_s \ldots$ fino ad avere

$$1=q_{s+1}\cdots q_t \quad \text{è possibile solo se } s=t \quad \ldots \quad 1=1$$

Perciò le due fattorizzazioni coincidono.

$\boxtimes$