Criteri di divisibilità

Dato $a \in \mathbb{N}$ quando $b \mid a$ dove $b \in \mathbb{N}$ fissato

Sviluppo decimale di a o in base 10

$$a = \sum_{i=0}^{d} a_i 10^i = a_0 + 10a_1 + \quad + 10^d a_d = a_d \; a_0$$

dove a_i CIFRE $\quad 0 \le a_i \le 9 \quad a_d \neq 0$

$b = 2 \quad 2 \mid a \iff 2 \mid a_0 \quad a = \sum_{i=0}^{d} a_i 10^i = \sum_{i=1}^{d} a_i 10^i + a_0 \equiv_2 0 + a_0$

$10 \equiv_2 0 \Rightarrow 10^i \equiv_2 0 \; \forall i \ge 1$

$b = 3 \quad 3 \mid a \iff 3 \mid \sum_{i=0}^{d} a_i \quad a = \sum_{i=0}^{d} a_i 10^i \equiv_3 \sum_{i=0}^{d} a_i$

$10 \equiv_3 1$

In particolare $a \equiv_3 0 \iff \sum_{0}^{d} a_i \equiv_3 0$

$a \approx 10^d \quad S(a) = \sum_{i=0}^{d} a_i \approx 9(d+1) = 9(\log_{10} a + 1)$

$b = 5 \quad 5 \mid a \iff 5 \mid a_0$ stesso trucco per $b = 2 \quad 10 \equiv_5 0$

$b = 9 \quad a \equiv_9 \sum_{i=0}^{d} a_i \quad$ " " " $b = 3 \quad 10 \equiv_9 1$

$b = 11 \quad 10 \equiv_{11} -1 \quad a = \sum_{0}^{d} a_i 10^i \equiv_{11} \sum_{0}^{d} a_i (-1)^i = a_0 - a_1 + a_2 - a_3 \quad \pm a_d$

Esempio: $a = 341 = 31 \cdot 11 \equiv_{11} 0 \quad A(a) = 3 - 4 + 1 = 0$

somma a segni alterni cifre di a

$b = 7 \quad 10 \equiv_7 3 \quad \sum a_i 10^i$

i	0	1	2	3	4	5	6
10^i	1	3	2	6	4	5	1
				-1			

$a \equiv_7 a_0 + 3a_1 + 2a_2 + 6a_3 + \dots$

$1000 \equiv_7 -1 \quad a = \sum_{i=0}^{t} b_i \cdot 10^{3i} \quad 0 \le b_i \le 999$

$a \equiv_7 \sum_{0}^{t} b_i (-1)^i$

$10 \equiv_7 3 \quad 3^{-1} \equiv_7 -2 \quad 7 \mid a \iff a \equiv_7 0 \Rightarrow -2a \equiv_7 0$

$\Leftarrow 0 \equiv 3(-2a) \equiv -6a \equiv a$

$bx = c \quad x = b^{-1}c$

$$-2a = -2 \cdot 10 \cdot \sum_{i=1}^{d} a_i \cdot 10^{i-1} - 2a_0 \equiv_7 \sum_{i=1}^{d} a_i 10^{i-1} - 2a_0$$

$a = a_d a_{d-1} \; a_0 \quad H(a) = a_d \dots a_1$

$L(a) = H(a) - 2a_0$

Esempio: $a = 5437$ $H(a) = 543$ $L(a) = 543 - 14 = 529 \xrightarrow[L]{} 52 - 18 = 34$

$\longrightarrow 3 - 8 = -5 \not\equiv_7 0$ $7 \nmid a$

Questo algoritmo sembra polinomiale come enunciare un criterio di arresto $0 \xrightarrow[L]{} 0$ $\exists\, a \in \mathbb{Z}$ $L(a) = a$

Primi Esempi di Codici Rilevatori e Correttori di Errori

Prova del nove $a, b \in \mathbb{Z}$ $m = a \cdot b$ $\tilde{m}$

Problema: Controllare che abbia il valore corretto per m

$S(a) = \sum_i a_i$ $S(b) = \sum b_i$ $S(\tilde{m}) = \sum \tilde{m}_i$

$$S(a) \cdot S(b) \equiv_9 S(\tilde{m})$$

è condizione necessaria affinché $\tilde{m} = a \cdot b$

$\tilde{m} = a \cdot b \longrightarrow \tilde{m} \equiv_9 a \cdot b$ $[\tilde{m}]_9 = [a]_9 \cdot [b]_9 =$

$= [S(a)]_9 \cdot [S(b)]_9 \equiv_9 S(a) \cdot S(b)$

Notato che se $S(\tilde{m}) \not\equiv_9 S(a)S(b)$ $\tilde{m}$ è sbagliato

Ma potrebbe $S(\tilde{m}) \equiv_9 S(a)S(b)$ e $\tilde{m}$ essere sbagliato

Ex: a, b fissati determinare tutti gli $\tilde{m}$ tali che

$$S(\tilde{m}) \equiv_9 S(a)S(b)$$

Luhn $a = a_n \dots a_0$ $n = 11$ a numero 12 cifre

$C = \{0, \dots, 9\}$ $L(c) = \begin{cases} c & c = 0, 9 \\ 2c \bmod 9 & \text{altrimenti} \end{cases}$

$2c \bmod 9$ ← rappresentante canonico

c	0	1	2	3	4	5	6	7	8	9
$L(c)$	0	2	4	6	8	1	3	5	7	9

$v = a_0 + L(a_1) + a_2 + \dots + L(a_{11})$ v è valida SOLO SE $v \equiv_{10} 0$

Congruenze in $A = K[x]$

$n = n(x) \in A$ dico che $n \mid d \iff \exists c \in A \quad nc = d$

n divide d

E_n: $a E_n b \iff n \mid b - a$

Ex: E_n è congruenza rispetto a $+$, $*$ prodotto tra polinomi

Esempi: $n = 0_A$ E_0 $0_A \mid b-a \iff a E_0 b$ $b - a = 0_A \cdot c = 0_A \iff b = a$

: $0_K \neq n \in K \leq K[x]$ $k \longmapsto k \cdot 1_A + 0 \cdot x + 0 \cdot x^2 + \dots$

$b E_n a$ $b - a = nc = nn^{-1}(b-a)$ $[0]_{E_n} = A$

Sia $n \notin K$ $d = \deg n > 0$ $A/n = \{[a]_{E_n} : a \in A\}$ A/n ?

anello quoziente di A rispetto a E_n

$[a]_{E_n} = \{b \in A : b - a = nc\} = \{b \in A : b = a + nc\} = a + nA$ classe laterale di a rispetto ad n

$[0_A]_{E_n} = \{nc : c \in A\} = nA$ ideale generato da n

Esistono rappresentanti CANONICI per $[a]_{E_n}$

Teorema: Dato $n \in A$, $d = \deg n > 0$ dato $a \in A$ $\exists!\, r \in A$ esiste ed è unico

i) $r \in [a]_{E_n} \iff [r]_{E_n} = [a]_{E_n} \iff a E_n r$

ii) $\deg r < d$ (eventualmente $-\infty$ $r = 0_A$)

Dim: $a = nq + r$ $a - r = nq$ $a E_n r$ $\deg r < d$ r è unico $\square$

Esempio: $K = \mathbb{R}$ campo $A = \mathbb{R}[x]$ $n = x^2 + 1$ $N = nA$ ideale generato da n

$A/n = A/N = \{r + N : r \in A \ \deg r < 2\} = \{a + bx + N : a, b \in \mathbb{R}\}$

$\updownarrow$

$(a, b) \in \mathbb{R}^2$

$(a + N) + (b + N) = (a + b) + N$ $\lambda \cdot (a + N) := \lambda a + N$

λ: scalare, a: vettore

A/N diventa spazio vettoriale su $\mathbb{R}$

$(a_1 + b_1 x + N) + (a_2 + b_2 x + N) = (a_1 + a_2) + (b_1 + b_2)x + N$

$(a_1, b_1) + (a_2, b_2) = (a_1 + a_2, b_1 + b_2)$

$$\lambda(a+bx+N) = \lambda a + \lambda bx + N$$

$$\lambda(a,b) = (\lambda a, \lambda b)$$

$$(a+bx+N)(c+dx+N) = (a+bx)(c+dx) + N$$

$$(ac+bdx^2)+(ad+bc)x+N$$

$$(ac-bd+bd(1+x^2))+(ad+bc)x+N \qquad x \longleftrightarrow i$$

$$0+N$$