# ARITMETICA 26 OTT 2017

Note Title 10/26/2017

## Prove di divisibilità.

$$x = a_n 10^n + a_{n-1} 10^{n-1} + \dots + a_1 \cdot 10 + a_0$$

$$0 \leq a_i \leq 9$$

Divisibilità per 2: $\iff a_0 \equiv 0 \pmod 2$

$(10^k \equiv 0 \pmod 2 \quad \forall k \geq 1)$.

Divisibilità per 5: $\iff a_0 \equiv 0 \pmod 5$

(come sopra)

Divisibilità per 4 $\iff a_1 10 + a_0 \equiv 0 \pmod 4$

(il numero formato dalle ultime due cifre è divisibile per 4)

$\to$ Divisibilità per 25 (ultime due cifre).

**Prova del 9** Un numero è divisibile per 9 se e solo se lo è la somma delle sue cifre.

$$x = a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + \dots + a_1 \cdot 10 + a_0$$

$$10 \equiv 1 \pmod 9 \Rightarrow 10^k \equiv 1 \pmod 9 \quad \forall k \geq 0.$$

$$x \equiv a_n + a_{n-1} + \dots + a_1 + a_0$$

(Vale anche per la divisibilità per 3)

Divisibilità per 11.

$10 \equiv -1 \pmod{11}$ $\quad 10^2 \equiv 1 \pmod{11}$ $\quad \dots \quad 10^k \equiv (-1)^k \pmod{11}$

$$x \equiv (-1)^n a_n + (-1)^{n-1} a_{n-1} + \dots + -a_1 + a_0 \pmod{11}$$

Somma delle cifre con segni alterni

Divisibilità $\iff$ somma delle cifre di posto pari $\equiv$ somma delle cifre di posto dispari $\pmod{11}$.

## Divisibilità per 7

$10^1 \equiv 3 \pmod 7$ $\quad 10^2 \equiv 2$ $\quad \boxed{10^3 \equiv -1}$

$10^4 \equiv -3$ $\quad 10^5 \equiv -2$ $\quad \boxed{10^6 \equiv 1}$

$$12345678 = 12 \cdot \underset{+1}{10^6} + 345 \cdot \underset{-1}{10^3} + 678$$

$$x = b_n \cdot 10^{3n} + b_{n-1} 10^{3(n-1)} + \dots + b_1 \cdot 10^3 + b_0$$

$$x \equiv (-1)^n b_n + (-1)^{n-1} b_{n-1} + \dots - b_1 + b_0 .$$

---

SCRITTURA DECIMALE DEI RAZIONALI.

$$\frac{t}{2^a 5^b m}$$ scritto in forma ridotta $(t, 2^a 5^b m) = 1$.

$$(m, 10) = 1$$

$$\frac{t}{2^a 5^b m} = \frac{A}{2^a 5^b} + \frac{B}{m}$$

(È equivalente a $t = Am + B\,2^a 5^b$)

Nota: Ogni soluzione avrà $(A, 2^a 5^b) = 1$
$(B, m) = 1$.

$M = \max\{a, b\}$

$2^M \cdot 5^M \frac{A}{2^a 5^b} = 10^M \cdot \frac{A}{2^a 5^b} \in \mathbb{Z}$.

$\Rightarrow$ ci sono al più $M$ cifre decimali.

D'altra parte, $10^{M-1} \frac{A}{2^a 5^b} \notin \mathbb{Z}$

$M = a$ oppure $M = b$

Rimane o 2 o 5 al denominatore.

Scrittura di $\frac{B}{m}$ in base 10,

Cifre prima della virgola:

$B = qm + r$ (divisione euclidea)

$$\frac{B}{m} = q, \dots\dots \qquad = \frac{r}{m}.$$

(1) $10r = q_1 m + r_1$

$10 r_1 = q_2 m + r_2$

(2) $100r = 10 q_1 m + 10 r_1 = 100 q_1 m + q_2 m + r_2$

$$r_1 \equiv 10r \pmod m$$
$$r_2 \equiv 100r \pmod m$$
$$r_k \equiv 10^k r \pmod m$$

→ Questo implica in modo ovvio che la successione degli $r_i$ è periodica

→ se $10^s \equiv 1 \pmod m$ sono tornato da capo

Quindi le cifre si ripetono periodicamente con periodo uguale all' "ordine di 10 mod m" cioè il minimo $d$ tale che $10^d \equiv 1 \pmod m$

$$\frac{t}{2^a 5^b m} = \frac{A}{2^a 5^b} + \frac{B}{m}$$

n° finito di cifre — puramente periodic.

ANTIPERIODO — PERIODO

$$\frac{5}{7} = 0,\overline{714285}$$

$$5 \cdot 10^6 \equiv 5 \cdot 1 \equiv 5 \pmod 7$$

$$50 = 7 \cdot 7 + 1$$
$$10 = 7 \cdot 1 + 3$$
$$30 = 7 \cdot 4 + 2$$
$$20 = 7 \cdot 2 + 6$$
$$60 = 7 \cdot 8 + 4$$
$$40 = 7 \cdot 5 + 5$$
$$50 = 7 \cdot 7 + 1$$

$$\frac{1}{7} = 0,\overline{142857}$$

$$142 + 857 = 999$$

$\frac{1}{p}$ $p$ primo, $\neq 2, 5$

Supponiamo che $\frac{1}{p} = 0,\overline{a_1 \dots a_n b_1 \dots b_n}$

abbia una scrittura periodica di periodo PARI ($2n$ cifre)

Allora $a_1 \dots a_n + b_1 \dots b_n = \underbrace{99 \dots 9}_{n \text{ volte}}$

---

## Teorema di Wilson

$p$ primo. Allora $(p-1)! \equiv -1 \pmod{p}$.

$(p-1)! = 1 \cdot 2 \cdot 3 \cdot \dots \cdot (p-1)$

$\forall x$ con $1 \leq x \leq p-1$
$\exists y$ con $1 \leq y \leq p-1$
tale che $xy \equiv 1 \pmod{p}$.

Metto vicine, a coppie*, i termini $x, y$ con $xy \equiv 1 \pmod{p}$.

Può succedere $x \equiv y \pmod p$

quando $x \cdot x \equiv x^2 \equiv 1 \pmod p$

$x \equiv \pm 1 \pmod p$

coppia + coppia + ... + coppia + $\{1\}$ + $\{-1\}$

Prod = 1 $\quad$ Prod = 1 $\quad$ Prod = 1

$\rightarrow$ Prodotto totale $\equiv -1 \pmod p$.

---

$p$ primo $> 2$. Considero il numero razionale

$$1 + \frac{1}{2} + \frac{1}{3} + \dots + \frac{1}{p-1} = \frac{a}{b} \qquad (a,b) = 1$$

Tesi: $p \mid a$. $\qquad$ ($p-1$ pari).

Raggruppamento a coppie.

$$\frac{1}{k} + \frac{1}{p-k} \qquad 1 \leq k \leq \frac{p-1}{2}.$$

$$= \frac{p}{k(p-k)}$$

$p \mid$ numeratore

$p \nmid$ denominatore

$$\frac{pa}{b} + \frac{pc}{d} \qquad p \nmid b \quad p \nmid d$$

$$= \frac{pad + pbc}{bd}$$

$p \mid$ NUM

$p \nmid$ DEN.

$p$ NON SI CANCELLA.

$(p-1)! \equiv -1 \pmod{p}$ se $p$ è primo

$(n-1)! \equiv 0 \pmod{n}$ se $n$ non è primo e $n > 4$.

---

Funzioni moltiplicative.

<u>Def</u>: $f : \mathbb{N} \to \mathbb{N}$ si dice moltiplicativa se $(a,b)=1 \Rightarrow f(ab) = f(a)f(b)$

<u>Oss.</u> Ci sono dei casi in cui l'ipotesi $(a,b)=1$ è inessenziale.

<u>Es.</u> $f(n) = n$. $f(n) = n^k$.

$f(n) = n°$ dei divisori di $n$. $= \boxed{d(n)}$

$$n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$$

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

$$m = q_1^{b_1} q_2^{b_2} \cdots q_h^{b_h}$$

$(n,m)=1$ $\quad p_i \neq q_j \quad \forall i \ \forall j$.

$$d(nm) = (a_1+1)\cdots(a_k+1)(b_1+1)\cdots(b_h+1)$$
$$= d(n)\,d(m).$$

---

<u>Oss.</u> Se $(a,b)=1$ ogni divisore $d$ di $ab$

si scrive in maniera unica come prodotto di un divisore $d_1$ di $a$ per un divisore $d_2$ di $b$.

$$a = p_1^{\alpha_1} \cdots p_k^{\alpha_k} \qquad b = q_1^{\beta_1} \cdots q_h^{\beta_h}$$

$$d = p_1^{\delta_1} \cdots p_k^{\delta_k} q_1^{\delta'_1} \cdots q_h^{\delta'_h}$$

$$0 \le \delta_i \le \alpha_k \qquad 0 \le \delta'_j \le \beta_j .$$

Questo mi dice che la funzione

$$\sigma(n) = \sum_{d|n} d \quad \text{è moltiplicativa.}$$

Caso $n = p^a q^b$ $\qquad d = p^i q^j$

$$\sigma(p^a) = 1 + p + p^2 + \dots + p^a$$
$$\sigma(q^b) = 1 + q + q^2 + \dots + q^b$$
$$\sigma(n) = \sum_{i=0}^{a} \sum_{j=0}^{b} p^i q^j = \sigma(p^a)\sigma(p^b)$$

---

Numeri perfetti pari.

<u>Def</u>. $n \in \mathbb{N}$ si dice PERFETTO se
$$\sigma(n) = 2n.$$

<u>Esempio</u> $n = 6$ $\qquad \sigma(6) = 1+2+3+6 = 12 = 2 \cdot 6$

$$n = 2^{q-1}(2^q - 1) \quad \text{dove } 2^q - 1 = p$$

è un primo di Mersenne

$$\sigma(n) = \sigma(2^{q-1})\,\sigma(2^q - 1)$$

$$= (1 + 2 + 2^2 + \dots + 2^{q-1})(1 + 2^q - 1)$$

$$= (2^q - 1) \cdot 2^q \qquad = 2n$$

<u>Esempio 2</u> $\quad n = 28 = 4 \cdot 7 = 2^2(2^3 - 1)$.

$$\boxed{\text{Non ci sono altri esempi con numeri PARI}}$$

Supponiamo infatti che $\sigma(n) = 2n$.

Scriviamo $n$ nella forma $n = 2^a k$
con $(2, k) = 1$

$$\sigma(n) = \sigma(2^a)\,\sigma(k) = (2^{a+1} - 1)\,\sigma(k)$$

$$= 2^{a+1} \cdot k \qquad (= 2n).$$

$$2^{a+1} - 1 \mid 2^{a+1} \cdot k \implies 2^{a+1} - 1 \mid k$$

$$k = (2^{a+1} - 1)\,h.$$

$$\cancel{(2^{a+1} - 1)}\,\sigma(k) = 2^{a+1}\,\cancel{(2^{a+1} - 1)}\,h$$

$$\sigma(k) = 2^{a+1} \cdot h$$

k ha due divisori ovvi:

$$h \qquad (2^{a+1}-1)h$$

che sommano $2^{a+1} \cdot h$

(totale della somma dei divisori)

Non ce ne sono altri.

$\Rightarrow \quad k = (2^{a+1}-1)h \quad$ = primo

$h=1 \quad 2^{a+1}-1$ è un primo di Mersenne.