N 1

AM

Titolo nota 08/09/2008

$$1024 = 1 \cdot 10^3 + 0 \cdot 10^2 + 2 \cdot 10^1 + 4 \cdot 10^0$$

$$10110 = 1 \cdot 2^4 + 0 \cdot 2^3 + 1 \cdot 2^2 + 1 \cdot 2^1 + 0 \cdot 2^0$$

$$11_{10} = 1 \cdot 2^3 + 0 \cdot 2^2 + 1 \cdot 2^1 + 1 \cdot 2^0 =$$

$$3 \quad 1 \qquad = 1011_2$$

$38_{10} = ?_5 = 1 \cdot 5^2 + 2 \cdot 5^1 + 3 \cdot 5^0$

$13 : 5^1 = 2$

3

$38_{10} = 123_5$

$$549 : 7 = 78$$

$$\underline{56}$$

$$\underline{7}$$

$$549 = 7 \cdot 78 + 1$$

$a \qquad b \qquad\qquad b \neq 0$

$\exists \; q, r :$

$$a = bq + r$$

$$0 \leq r < |b|$$

b divide a

$b \mid a$

$c \mid ab$

$p \mid \not{q} b \Rightarrow p \mid a$ oppure $p \mid b$

$MCD(a, b) =$

d :

$1 \rightarrow \quad d \mid a \quad , \quad d \mid b$

$2 \rightarrow \quad d_1 \mid a \quad , \quad d_1 \mid b \Rightarrow d_1 \mid d$

$mcm(a, b)$

m :

$1 \rightarrow \quad a \mid m \quad , \quad b \mid m$

$2 \rightarrow \quad a \mid m_1 \quad , \quad b \mid m_1 \Rightarrow m \mid m_1$

$$a = p_1^{\alpha_1} \; p_2^{\alpha_2} \; p \cdots p_n^{\alpha_n}$$

$$b = q_1^{\beta_1} \; q_2^{\beta_2} \cdots q_m^{\beta_m}$$

MCD = tutti i primi presenti

SIA in a che in b con

l'esponente MINIMO

$12 = 2^2 \cdot 3$ $\quad 45 = 3^2 \cdot 5$ $\quad MCD = 3^1$

5 F　　8 F

61

$(5, 8) = 1$ ↙

$\underbrace{1}_{6} = \overbrace{2 \cdot 8 - 3 \cdot 5}^{15}$

61 F

$(6, 15) = 3$ ↙

$k \cdot 6 + h \cdot 15 = 3 \cdot m$

TEOREMA DI BEZOUT

$a, b \in \mathbb{Z}$ $\quad \exists\ m, n \in \mathbb{Z}$

$d = (a, b)$

$$ma + nb = d$$

trovare d dati a e b

$$(a, b) = d$$

$$d \mid a \quad , \quad d \mid b$$

$$\boxed{d = (a, a-b)}$$

$51 \quad 15$

$51 : 15 = 3$

6

$15 : 6 = 2$

3

$6 : 3 = 2$

0

$d|51 \quad d|15 \quad d|6$

$51 = 3 \cdot 15 + 6$

$15 = 2 \cdot 6 + 3$

$6 = 3 \cdot 2$

$3 = 15 - 2 \cdot 6$

$$51 = 3 \cdot 15 + 6 \longrightarrow 6 = 51 - 3 \cdot 15$$

$$3 = 15 - 2 \cdot 6$$

$$3 = 15 - 2\left[51 - 3 \cdot 15\right] = 15 - 2 \cdot 51 + 6 \cdot 15 =$$

$$= 7 \cdot 15 - 2 \cdot 51$$

$$3 = 7 \cdot 15 + (-2)\,51$$

$3 = 3 \cdot 6 - 15$

$1 = 2 \cdot 8 - 3 \cdot 5$

$a_1, a_2, a_3 \cdots a_n \qquad d = (a_1, a_2 \cdots a_n)$

$\exists\ m_1, m_2 \cdots \cdots \quad m_n$

$d = m_1 e_1 + m_2 e_2 + \cdots \cdots$

$$m\alpha + m\beta = d$$

Congruenze

$8 - 6 = 2 \quad (\text{o.m})$

$\rightarrow 8 + 6 = 2 \quad (\text{p.m}) \quad 1$

$7 + 6 \overset{?}{=} 1 \quad (\text{pm})$

a b congrui modulo m

$$a \equiv b \pmod{m}$$

$$a \equiv b \pmod{m}$$

$$m \mid a - b$$

a (24)

$9 \cdot 10 \qquad (4)$

$90 : 4 \mid = 2$

$1 \cdot 2 = 2$

$a_1 \equiv a_2 \quad (m)$

$b_1 \equiv b_2 \quad (m)$

$a_1 + b_1 \equiv a_2 + b_2 \quad (m)$

$a_1 b_1 \equiv a_2 b_2 \quad (m)$

8 : 4 (3)

8 / 4 = 2 (3)

8 : 3 = 2 (w)

4 : 2 = 1 (w)

2 : 1 = 2

12 = 4 (8)

6 = 2 (8)

8 ( ) 12 - 4

k · 8 = 12 - 4 / : 2

k · 4 = 6 - 2

$$18 \equiv 4 \quad (3)$$

$$4 \equiv 1 \quad (3)$$

$$16 \equiv 7 \quad (3)$$

$$\left[\frac{16}{7}\right] \equiv 1 \quad (3)$$

$$16 \cdot \left[\frac{1}{7}\right] \equiv \frac{16}{7} \quad (3)$$

27

$\exists \; 7 \cdot 7 \equiv 1 \pmod 3$

$(a, m) = 1 \quad \exists \; h, k :$

$ha + km = 1$

$km = 1 - ha$

$1 \equiv ha \pmod m$

→ $\frac{1}{2} - \frac{1}{3} = \frac{1}{6} \quad (p)$

CONGRUENCE MOD p

$ab \equiv 0 \ (p) \leftarrow \quad p \mid ab$

$a \equiv 0 \ (p) \ \vee \ b \equiv 0 \ (p)$

$p \mid a \qquad p \mid b$

$$ab \equiv 0 \pmod{m}$$

$$a \equiv 0 \pmod{m}$$

$$b \equiv 0 \pmod{m}$$

a

$a \quad 2a \quad 3a \quad \cdots\cdots \quad ka \quad \cdots\cdots \pmod{m}$

$$a \equiv ka \pmod{m}$$

$$2a \equiv (k+1)a \pmod{m}$$

$$3a \equiv (k+2)a \pmod{m}$$

$\vdots$

2 0 4

$(a, m) = 1$

$a, 2a, \ldots (m-1)a, ma$

$0, 1, 2, \ldots, m-1$

$ka \equiv ha \pmod{m}$ $\quad k, h < m$

$(k-h)a \equiv 0 \pmod{m}$

$k = h$

$\boxed{k \equiv h}$ $\quad \left(\frac{m}{d}\right)$

p primo

$a \quad 2a \quad \dots \quad pa$

$(\not\exists)$

$2 \quad 4 \quad 6 \quad 1 \quad 3 \quad 5 \quad 0 \quad 2 \quad 4$

$a \quad a^2 \quad a^3 \quad \dots \quad a^k \quad \dots$

$a^k \equiv a^h \ (p)$

$a^{k+1} \equiv a^{h+1} \ (p)$

$$a^k \equiv a^h \pmod p$$

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

$p \mid a$

$$(p-1)^2$$

$$(-1)^2 \equiv 1 \pmod p$$

$\forall a \quad \exists k \qquad a^k \equiv 1 \pmod p$

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

PICCOLO TEOREMA DI FERMAT

1ª dimostrazione (INDUZIONE)

LEMMA $(x+y)^p \equiv x^p + y^p \ (p)$

$$(x+y)^p = \sum_{i=0}^{p} \binom{p}{i} x^i y^{p-i} = y^p + p\,x\,y^{p-1} + \binom{p}{2} x^2 y^{p-2} \cdots + x^p$$

$$\binom{p}{i} = \frac{p!}{i!\,(p-i)!}$$

$\rightarrow a^p \equiv a \quad (p)$

$\rightarrow a^{p-1} \equiv 1 \quad (p)$

P. B $\quad 1^p \equiv 1 \quad (p)$

P. I $\quad x^p \equiv x \quad (p)$

$(x+1)^p \equiv x^p + 1^p \equiv x + 1 \quad (p)$ $\square$

2ª dimostrazione

-> a 2a 3a .... (p-1)a (p)

-) 1 2 3 .... p-1

$a \cdot (2a) \cdot (3a) \cdots (p-1)a \quad (p)$

$1 \cdot 2 \cdot \cdots \cdots (p-1) \quad (p)$

$a^{p-1} \cdot (p-1)!$

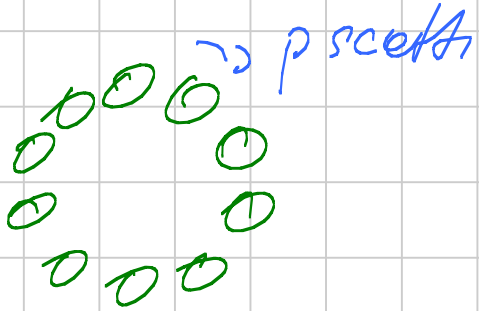
$(p-1)!$

$a^{p-1} \cancel{(p-1)!} \equiv \cancel{(p-1)!} \quad (p)$

$a^{p-1} \equiv 1 \quad (p)$

3ª dimostrazione

$a^p \equiv a \pmod p$



p perline

a colori

$\#\text{collane} = \dfrac{a^p - a}{p}$

k | p

k = p

$\Rightarrow a^p \equiv a \pmod p$

$1 \quad a \quad a^2 \quad \dots \quad a^k \dots$

$a^{p-1} \equiv 1 \quad (p)$

$a^k \equiv 1 \quad (p)$ [1] k il minimo per cui vale [1]

$a^{p-1} \equiv 1 \quad (p)$ ← il + grande multiplo ← $p-1$

$a^k \equiv 1 \quad a^{2k} \equiv 1 \dots$

$a^{mk} \equiv 1 \rightarrow a^{p-1} \equiv 1 \ (p)$

$a^{(m+1)k} \equiv 1$

$k \mid p-1$

k ordine moltiplicativo di a mod p

$$ord_p(a) \mid p-1$$

a : $ord_p(a) = p-1$ si dice generatore

$$(p-1)! \equiv -1 \quad (p)$$

$\hookrightarrow$ g □

$$g^0 \cdot g^1 \cdot \ldots \cdot g^{p-1} \equiv g^{p\frac{(p-1)}{2}} \left(g^{k(p-1)}\right)^{\frac{(p-1)}{2}}$$

$g^{k(p-1)} \to 1$

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

$$g^{\frac{p-1}{2}} \equiv \pm 1 \pmod{p} \qquad x^2 - 1 \equiv 0 \pmod{p}$$

$\Rightarrow$

$p^4 - q^4$ usare mod 5

52 carte

1 → 2 24 → 3

2 → 4

⋮ ⋮

26 → 52 52 → 51

27 → 1

$1 \to 2$

$2 \to 4$

$\vdots$

$26 \to 52$

$27 \to 1 \to 54 \pmod{53}$

$x \to 2x \pmod{53}$

1

2

2^2

$\vdots$

2^5

→ 26
13
4
2

2^2

2^4

2^{13}

$2^6 \equiv 64 \equiv 11$

$2^6 \cdot 2^6 \cdot 2 \equiv 11 \cdot 11 \cdot 2 = 242 \ (59)$

x^2 (p)

x^2 $(p-x)^2$

$x \equiv$ (12)

$x \equiv$ (2)

$x \equiv$ (3)

$x \equiv 1$ (7)

$x^2 \equiv 2$ (3)

x^6 (7)

$x^2 \equiv 0, 1$ (4) (8)

x^3 (9)

(7)

$(x^3)^2 \equiv 1$ (7)

$x^3 \equiv \pm 1$ (7)