TEORIA dei NUMERI

Titolo nota 11/09/2006

- notazione posizionale
- MCD mcm Euclide Bézout ...
- divisione intera
- congruenze, aritmetica modulare.

$$57'314$$

$$= 5 \cdot 10^4 + 7 \cdot 10^3 + 3 \cdot 10^2$$

$$+ 1 \cdot 10^1 + 4 \cdot 10^0$$

$\mathbb{N}$, fissata la base [10]

restano individuate in modo unico coefficienti (cifre)

$$X = \overbrace{A\,B\,C\,D\,E}^{K}\,F$$

(6 cifre)

$$Y = F\,\underbrace{A\,B\,C\,D\,E}_{K}$$

$$7 \mid X \iff 7 \mid Y$$

$$X = \underbrace{A \cdot 10^5 + \dots + E \cdot 10}_{10K} + F$$

$$Y = K + F \cdot 10^5$$

$$10^5 = 7w + 5$$

$$Y = 5F + K + \langle \text{multiplo di } 7 \rangle$$

$$\begin{array}{r|l} 100\,000 & 7 \\ \hline 30 & \cancel{14285} \quad w \\ 20 & \\ 60 & \\ 40 & \\ 5 & \end{array}$$

$X \equiv 54$ (7)

(mod 7)

$5F + K$

$5 \cdot 3K + F5 =$

$3^{-1} = 5$

$5^{-1} = 3$

$10k + F$ $\qquad$ $5F + k + 7 \ldots$

primi fattorizzazioni

$$7 \mid z \iff 7 \mid 5z$$

$$5x = 50k + 5F = 5F + k + \langle \text{m. d. } 7 \rangle$$

$$7 \mid x \iff 7 \mid 5F + k \iff 7 \mid y$$

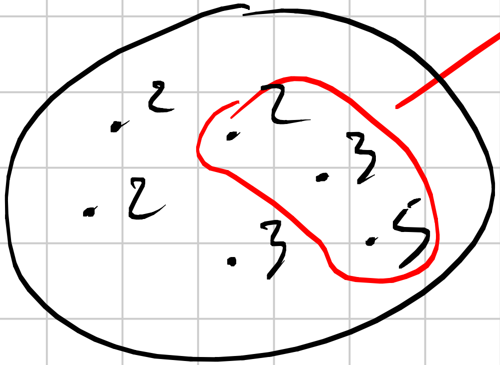
$$N = p_1 \cdot p_2 \cdot p_3 \ldots p_k \qquad p_i \text{ primi}$$

$$\stackrel{\ldots}{=} p_1^{\alpha_1} \; p_2^{\alpha_2} \; p_3^{\alpha_3}$$

$$360 = 36 \cdot 10 = 2^2 \cdot 3^2 \cdot 2 \cdot 5$$
$$= 2^3 \cdot 3^2 \cdot 5$$

360

I



$2 \cdot 3 \cdot 5 = 30 \mid 360$

$$2^{\alpha}\, 3^{\beta}\, 5^{\gamma}$$

$0 \le \alpha \le 3$	4	24 divisori
$0 \le \beta \le 2$	3	
$0 \le \gamma \le 1$	2	

——— o ———

Quadrato $\Longleftrightarrow$ tutti gli esponenti sono pari

$\Longleftarrow$

$\Longrightarrow$

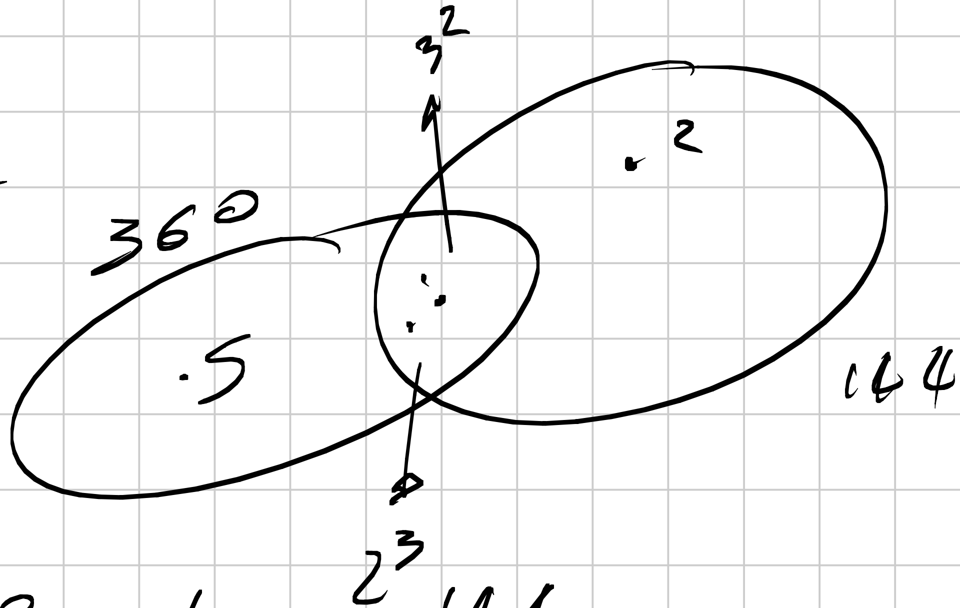
$p^{\alpha} \,\|\, N$ $\qquad p^{\alpha} \mid N \qquad p^{\alpha+1} \nmid N$

$N^2 = N \cdot N$ $\qquad p^{2\alpha} \,\|\, N^2$

$p \neq \pm 1 \qquad p \mid ab \Rightarrow p \mid a$ o $p \mid b$

$360 = 2^3 \cdot 3^2 \cdot 5$

$144 = 12^2 = 2^4 \cdot 3^2$



"intersezione"

$2^3 \cdot 3^2$

divide sia 360 che 144

è il massimo tra i divisori comuni

MCD (gcd greatest common divisor)

$$\text{mcm}(a,b) = \frac{ab}{\text{MCD}(a,b)}$$

Identità di Bézout

$$(a, b) = d$$

Il minimo possibile [positivo] tra i numeri della forma

$$S, T \in \mathbb{Z}$$

$$Sa + Tb$$

$$\underbrace{360}_{d?}\, S + \underbrace{144}_{d?}\, T = 72$$

$d \mid 72$

Dati due interi non nulli a, b, esistono S e T interi t.c.

$$MCD(a, b) = Sa + Tb$$

Algoritmo di Euclide

$a, b, q, r \in \mathbb{Z}$

Dati a e b $(b \neq 0)$

la divisione di $a : b$

quoziente q resto r t.c.

$$a = q \cdot b + r \qquad 0 \leq r < b$$

$$a \,,\quad b \longrightarrow \cancel{q_1} \quad r_1$$

dividendo divisore quoziente resto

$$b \quad r_1 \longrightarrow \cancel{q_2} \quad r_2$$

$$\underbrace{360}_{} = \underbrace{144 \cdot \cancel{2}}_{} + 72 \qquad \begin{array}{r} 360 \\ 288 \\ \hline 72 \end{array}$$

$$144 = \boxed{72} \cdot 2 + 0$$

prossimo divisore

Ultimo resto diverso da 0

è il MCD (360, 144)

$$74 = 19 \cdot 3 + 17 \qquad (74, 19) = 1$$

$$19 = 17 \cdot 1 + 2$$

$$17 = 2 \cdot 8 + \boxed{1}$$

$$2 = \boxed{1} \cdot 2 + 0$$

$$74\,S + 19\,T = 1$$

$\downarrow \quad \downarrow^{74} \quad \downarrow^{19}$

1) $(74, 1, 0)$

2) $(19, 0, 1)$

$74 = 1 \cdot 74 + 0 \cdot 19$
$19 = 0 \cdot 74 + 1 \cdot 19$

1 $-$ 3 2

3) $(17, 1, -3)$

2 $-$ 3

4) $(2, -1, 4)$

1ª cof sono i divisori successivi di A. E.

Coeff.

5 = 3 $-$ 8 4

$(1, 9, -35)$

$17 = 1 \cdot 74 - 3 \cdot 19$

$2 = -1 \cdot 74 + 4 \cdot 19$

$$\boxed{1 = 9 \cdot 74 - 35 \cdot 19}$$

ARITMETICA MODULARE

100.000 : 7

Resto

lunedì 11 settembre 2006

? 11 " 2007

martedì

52 < multiplo di 7 >

365 = ~~52~~ settimane +

1 giorno

— 10 set 06 → 11 set → . . . . → . → . → 11 set 07

Lun → Mar → Mer → Gio → Ven → Sab → Dom → Lun

Resto di una divisione per 7.

−2 → −1 → 0 → 1 → 2

0 → 1 → 2 → 3 → 4 → 5 → 6 → 0

10 → 3

11 → 4

5

6

possibili resti

Si possono fare + − ×

$n = 7\cancel{q} + \underbrace{r}$

$n = 10 \quad r = 3$

$n = 7q + r \qquad 5 \qquad 5$

$m = 7q' + r' \qquad 6 \qquad 6$

$n+m = 7\cancel{(q+q')} + \underbrace{r + r'} \qquad 11 \quad 7 \quad 4$

$n \equiv r \pmod{7}$

congruo

modulo

mod 7

$$720 = 700 + 20$$

$$(\text{mod } 7) \equiv 20 \quad (\text{mod } 7)$$

$$\equiv 6$$

$$20 = 14 + 6$$

$+$ $\times$

$$720 = 72 \cdot 10 = 2 \cdot 36 \cdot 10 \equiv 6$$

$$\begin{matrix} 2 & 1 & 3 \end{matrix}$$

(7)

$$36 = 35 + 1 \equiv 1$$

$$10 = 7 + 3 \equiv 3$$

$$2 \equiv 2$$

$m = 7q + r$

$n = 7q' + r'$

$mn = 7\langle \quad \rangle + r \cdot r' \equiv r \cdot r' \quad (7)$

Un numero è multiplo di 5

se la sua ultima cifra è

0, 5

$X = \boxed{\ldots F D C B} A = A + 10B + 10^2 C + \ldots$

modulo 5

$10 \equiv 0 \qquad 10^3 \equiv 0^3$

$10^2 \equiv 0^2 \equiv 0$

$X \equiv A \pmod 5$ 0

5

2 10 25 -00 -25 -50 -75 16 -1234

9 $9 \mid X \iff 9 \mid$ somma delle cifre

$A + 10B + 10^2 C + \dots \quad (9)$

$\equiv A + 1 \cdot B + 1^2 C + 1^3 D$

$A + B + C + D \dots$ somma delle cifre

$N = aabb$ quadrato

$\ \ \ \ \ \ \ \ -\ +\ -\ +$

- b ha solo alcune possibilità:

$b = 0\ 1\ 4\ 5\ 6\ 9$

	10
0	0
1	1
2	4
3	9
4	6
5	5
6	6

- Divisibilità per 11

$11 \mid N$

- $121 \mid N$ $\qquad \dfrac{N}{121}$ è q.p.

- $100a + b$ mult. di 11

$$N = \overline{aabb} = a\,10^3 + a\,10^2 + b\cdot 10 + b$$

$$\frac{N}{11} = \overline{a0b}$$

$$= 100a\,(11) + b\cdot(11)$$

$$100a+b$$

$$= 11\cdot(100a+b)$$

$$11 \mid 100a+b$$

$$100a+b \equiv 0 \pmod{11}$$

$$\Downarrow$$

$$a+b = 11$$

$$N = 0000$$

a	11	10	7	6	5	2
b	0	1	4	5	6	9

$$7744 = 88^2$$

$$100a+b = 9\cdot 11a + \overbrace{a+b}^{=11} = 11(9a+1)$$

$$\square$$

- Divisioni mod n

$x = a : b$ $\qquad bx \equiv a \pmod{m}$

$x = \frac{1}{b}$

$\boxed{a = 1}$

Dato b, trovare x t.c. $bx = 1$

x è l'inverso di $b \pmod{m}$

$1 \equiv bx \pmod{m}$

$1 = \boxed{b}x + k\boxed{m}$ $\qquad$ Bézout

$(b, m) \mid 1 \Longrightarrow (b, m) = 1$ $\qquad$ [coprimi / rel. primi / primi tra loro

$$1 = s \cdot b + \underbrace{\cancel{T m}}$$

$(b, m) = 1$

$(\text{mod } m)$

$1 \equiv s \cdot b$ $\qquad$ s è <u>l'inverso</u> di b

$13 \quad \text{mod} \quad 74$

$3x \equiv 5 \quad (11)$

$3 \cdot 4x \equiv 20 \equiv -2$

$x \equiv -2 \equiv 9 \quad (11)$

$3x = 5$ in $\mathbb{Q}$

$x = \frac{5}{3}$ $\qquad$ $3^{-1} \equiv 4 \quad (11)$

$$a x \equiv b \quad (m)$$

$$(a, m) = d \qquad a = dA, \quad m = dM$$

$$\underbrace{dA\,x}_{\substack{m \\ 0}} \equiv b \quad (dM) \qquad b \equiv 0 \quad (d)$$

$$(d) \qquad b = dB$$

$$x \equiv y \quad (m)$$

$$m' \mid m$$

$$\Longleftrightarrow m \mid x - y \Longrightarrow m' \mid m \mid x - y \Longrightarrow x \equiv y \quad (m')$$

$$dAx \equiv dB \quad (dM)$$

$dM \mid dAx - dB \implies M \mid Ax - B \iff Ax \equiv B \pmod{M}$

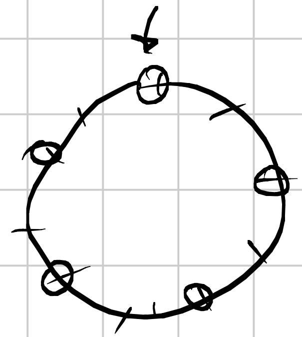
$12x \equiv 4 \ (10)$ $\qquad (12, 10) = 2$

$6x \equiv 2 \ (5)$

$x \equiv 2 \qquad x = 2 + k5$

$12x + 10y = 4$

$12s + 10t = 2$



$T = 5 = \frac{10}{(10, 12)}$

Potenze

(modulo, base) = 1

$10 \equiv 3 \quad 7$

le potenze sono periodiche

a	3^a (7)		
0	1	4	-3
1	3	5	-2
2	2	6	1
3	-1		

$3^3 = 3^2 \cdot 3 = 2 \cdot 3 = -1$

$3^4 = 3^3 \cdot 3 = -3$

$3^6 = 1$

$3^{6k+h} = (3^6)^k \cdot 3^h = 3^h$

~~base~~ modulo è un numero primo p

l'ordine moltiplicativo (i.e. il periodo con cui le potenze si ripetono le ~~pot.~~)

è un divisore di $p-1$

$2^{2^{2^{2^{2}}}}$ (11)

2222^{2222} (7) $\equiv 3$

2222^{2222}

$$\begin{array}{c|l} 2222 & 7 \\ 101 & \end{array}$$

2121

31

$2222 \equiv 3 \implies \underline{2222}^{2222} \equiv 3^{2222}$ ordine 6 $\equiv 2 \pmod{7}$

$2222 = 6k+h$ $\equiv 2$

$\equiv 2 \quad (6)$ $h=2$ $3^{6k+2} \equiv 3^2$ (7)

$1^t \equiv 1 \quad (73)$

$1^{72} \equiv 1$ [piccolo] Teorema di Fermat

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

p primo

$(a,p)=1$

$72 \mid t$ è soluzione

$1^t \equiv 1$ sempre $\forall t$

$t \equiv 0 \pmod 1$ [tutti]

$$2222^{2222} \pmod{7}$$

$$\left(\begin{array}{l} \cdot \quad 2222 \equiv 3 \pmod{7} \\ \\ 3^{2222} \quad \text{ordine è } 6 \end{array} \right.$$

$$2222 = 6 \cdot \ldots$$

t	3^t
0	1
1	3
2	2
3	-1
4	-3
5	-2
6	1