TEORIA DEI NUMERI I

POL

Titolo nota 03/09/2007

$$\mathbb{Z} = \{ \dots -2, -1, 0, 1, 2 \dots \}$$

$$\mathbb{N} = \{ 0, 1, 2, 3 \dots \}$$

positivi > 0

$$n = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n} \cdot (-1)$$

$p \mid ab \Rightarrow p \mid a \quad p \mid b$

$p \mid a$

esiste n t.c. $pn = a$

$3 \mid 6 \qquad 6 \mid 18 \Rightarrow 3 \mid 18$

$a \mid b \qquad b \mid a \qquad a = \pm b$

Trovare n, p primo t.c.

$$5p + 4q = n^2$$

$$5p = n^2 - 4q = (n+7)(n-7)$$

$5p$	± 1
p	± 5
5	$\pm p$
1	$\pm 5p$

$$\begin{cases} n^2 - 7 = 5 \\ n^2 + 7 = p \end{cases}$$

$a + b = c$ $\qquad$ $p + p = p$

$d \mid a \qquad d \mid c$

$\Rightarrow d \mid b$

$\in$ $\qquad$ $3x^2 + 2y^2 = 1998$

$3 \mid 2y^2 \qquad 3 \mid y$

$y := 3y'$

$$3x^2 - 2y^2 = 1998$$

$$y = 3y'$$

$$3x^2 - 18y'^2 = 1998$$

$$x^2 - 6y'^2 = 666$$

$$(90, 21) = 3$$

$3^2 \cdot 2 \cdot 5 \quad 3 \cdot 7$

$$(a, b) = (a, b-a)$$

$$(a, b+a)$$

$$\boxed{(a, b+ka)}$$

$d \mid a$ $\qquad$ $d \mid a+kd$

$$(93, 27) =$$

$$= (93 - 27 \cdot 3, 27) = (12, 27)$$

$$= (27, 12) = (27 - 12 \cdot 2, 12) = (3, 12) =$$

$$= (12 - 3 \cdot 4, 3) = (0, 3) = 3$$

$93 - 27 \cdot 3 = 12$

$27 - 12 \cdot 2 = 3$

$27 - (93 - 27 \cdot 3) \cdot 2 = 3$

$$k_a \cdot 93 + k_b \cdot 27 = k_d$$

TEO. di BÉZOUT

$(a, b) = d$

esistono h, k

$$h \cdot a + k \cdot b = d$$

$$2^{27} \cdot 3^{15} = (x^3 - y^3) = (x - y)(x^2 + xy + y^2)$$

$$d = (x, y)$$

$$(x - y,\ x^2 + xy + y^2) =$$

$a(x)$ $b(x)$

$a(x) = b(x)\, q(x) + r(x)$

$\deg r \leq 0$

$$= (x^2 + xy + y^2 - (x-y)(x-y),\ x - y)$$

$$= (3xy,\ x - y)$$

$(3, x-y)$

$(x, x-y)$

$(y, x-y)$

$(x, y) = d$

$x = d \cdot x' \qquad y = d \cdot y'$

$(x', y') = 1$

$\geq \quad \geq$

$p \qquad x = p^m \cdot \ldots \qquad d = p^{\min(m,n)} \ldots$

$y = p^n \cdot \ldots$

$$x = d\,x'$$
$$y = d\,y''$$

$$\left(x - y,\ x^2 + xy + y^2\right) =$$

$$= \left(d(x' - y'),\ d^2(x'^2 + x'y' + y'^2)\right)$$

$$d\left(x' - y',\ d(x'^2 + x'y' + y'^2)\right)$$

$$\left(x' - y',\ x'^2 + x'y' + y'^2\right)$$

$$(x, y) = 1$$

$$\begin{bmatrix} x - y, & x^2 + xy + y^2 \end{bmatrix} \sim \begin{matrix} 1 \\ \\ 3 \end{matrix}$$

$$(x - y, \; 3xy)$$

$$= \left(x - y, \; \frac{3}{\frac{x}{y}}\right)$$

$$(x-y, x) = (-y, x) = (y, x) =$$

$$= 1$$

$$(x-y, y) = 1$$

$$(3, x-y) =$$

divisori

$$d \mid m = p_1^{a_1} p_2^{a_2} p_3^{a_3} \cdots p_k^{a_k}$$

$$\# d = 2 \cdot (a_1+1)(a_2+1)(a_3+1) \cdots (a_k+1)$$

per i negativi

$p_1^0, p_1^1, p_1^2, \ldots, p_1^{a_1}$ $\quad$ $p_2^0, p_2^1, p_2^2, \ldots, p_2^{a_2}$ $\quad$ $\cdots$ $\quad$ $1, m$

$d(m)$ divisori $\Leftrightarrow$ m quadrato perfetto

$\sigma(m) = d_1 + d_2 + \dots$

$\sigma(15) = 1 + 3 + 5 + 15 = 24$

$$(p_1^0 + p_1^1 + \dots + p_1^{a_1})(p_2^0 + p_2^1 + \dots + p_2^{a_2}) \dots (p_k^0 + \dots + p_k^{a_k})$$

$= \sigma(m)$

$$\sigma(n) = \frac{p_1^{a_1+1}-1}{p_1-1} \cdot \frac{p_2^{a_2+1}-1}{p_2-1} \cdot \ldots \frac{p_k^{a_{k+1}}-1}{p_k-1}$$

$$(\bmod m)\ a = b \iff \begin{cases} a, b \text{ hanno lo stesso resto nella divisione per } m \\ m \mid b-a \\ a = km+b \end{cases}$$

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

$$\Downarrow$$

$$a + c \equiv b + d \pmod{m}$$
$$a - c \equiv b - d \pmod{m}$$
$$ac \equiv bd \pmod{m}$$

$$a/c \equiv b/d \pmod{m}$$

$ka \equiv kb \pmod{m}$ $\Leftrightarrow$ $m \mid ka - kb$

$\Downarrow$? $\qquad\qquad$ $\Downarrow$

$a \equiv b$ $\qquad\qquad$ $k(a-b)$

$\Downarrow$

$m \mid a - b$

se $(k, m) = 1$

$3 \equiv 9 \pmod{6}$

$1 \equiv 3 \pmod{6}$

$2x^2 + 3y^2 = 37 \pmod m$ x, y interi

no congruenza $\Rightarrow$ no uguaglianza

$\Rightarrow$ $2x^2 \equiv 37 \equiv 1 \pmod 3$

$2 \cdot 2x^2 \equiv 2 \pmod 3$

$1 \cdot x^2 \equiv 2 \pmod 3$

3	
0	0
1	1
2	1

0	$0^2 \equiv 0$
1	$1^2 \equiv 1$
2	$2^2 \equiv 1$

$3 \equiv 0, 1$

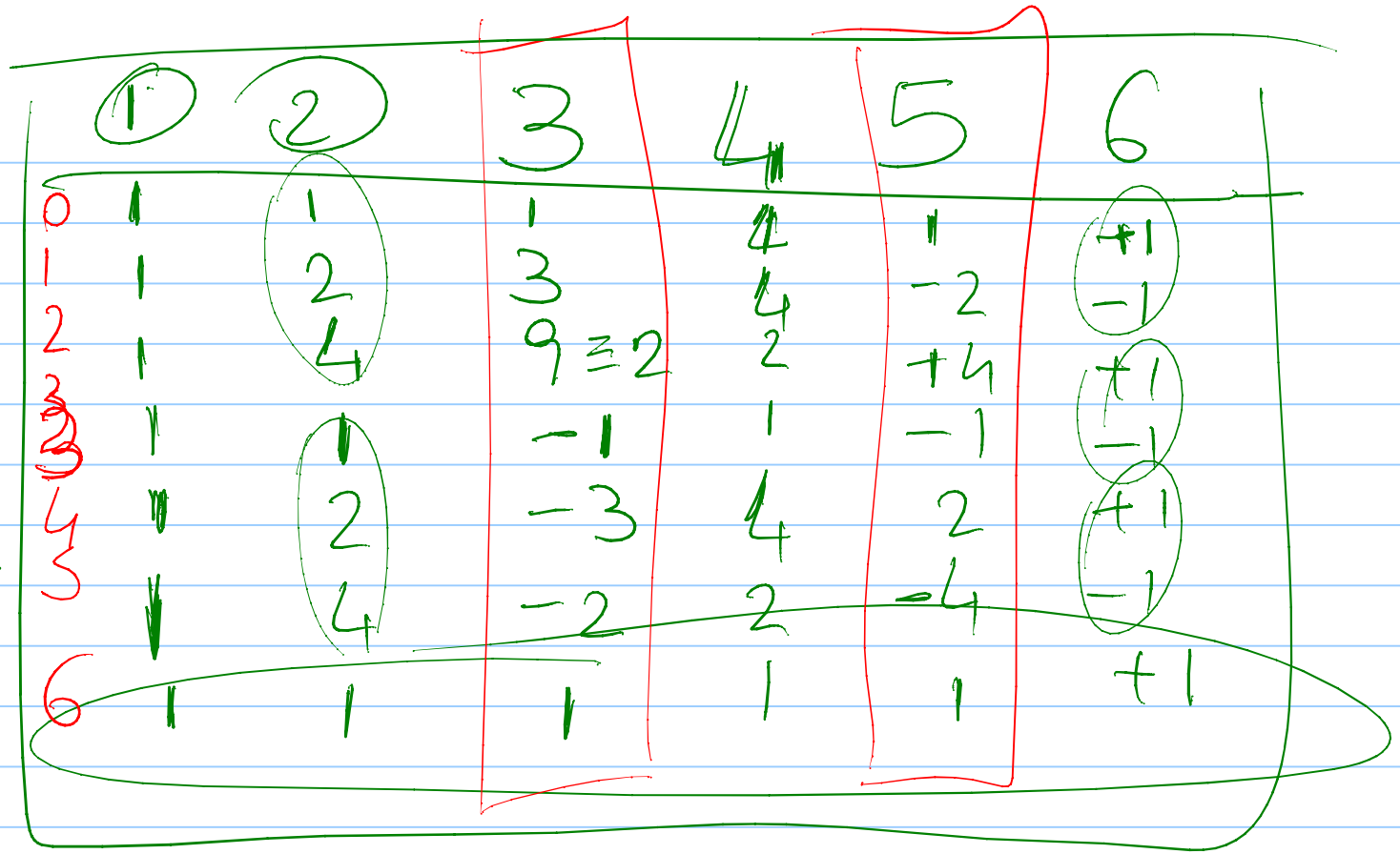
$4 \equiv 0, 1$

$5 \equiv 0, 1, -1$

$8 \equiv 0, 1, 4$

7

7



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

$\|\|\|$ $\|\|$

1 4

$p-1$ $\quad ord_p(n)$ $\quad p-1$

$2^3 \equiv 1 \quad ord_7(2) = 3 \quad ord_7(3) = 6$

Per ogni p, esiste un n tale che $\text{ord}_p(n) = p-1$

generatore

Piccolo teorema di Fermat

$a^{p-1} \equiv 1 \pmod{p}$ $\forall\, a$ non multiplo di p

oppure

$a^p \equiv a$ per ogni a

$0, 1, 2, 3, \dots \quad p-1$

$0, k, 2k \dots \quad (p-1)k \quad | \quad p \nmid k$

p

$k_i \equiv k_j \ (p) \qquad p \mid k_i - k_j$

$p \mid k(i-j)$

$i = j$

sistema completo di residui

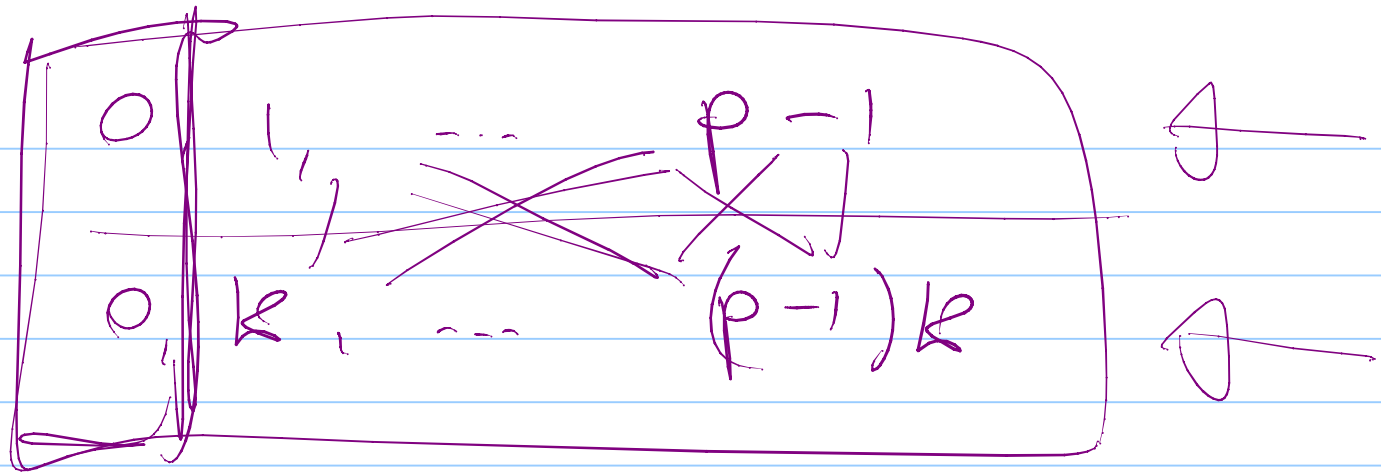
$h, h+1, \dots h+p-1$ sono un sistema completo

$0, g, g^2 \dots g^{p-1}$

4 mod 7

3 genera mod 7

$4 \equiv 3^{\square} \ (7)$



$$1 \cdot 2 \cdot 3 \cdots (p-1) \equiv k \cdot 2k \cdots (p-1)k$$

$$\equiv k^{p-1} \, 1 \cdot 2 \cdots (p-1)$$

$$1 \equiv k^{p-1}$$

PROBLEMA $m < p-1$ $(p+3)$ (-1)

$$S \equiv 0^m + 1^m + 2^m + 3^m + \dots + (p-1)^m \equiv ? \pmod p$$

$$\sum_{x \in \text{Sistema completo}} x^m$$

$0, k, 2k, \dots (p-1)k$ per una scelta di k tc $p \nmid k$

$$S \equiv 0^m + k^m + (2k)^m + \dots + (p-1)^m k^m$$

$$\equiv k^m \left(0^m + 1^m + 2^m + \dots + (p-1)^m\right) = S\,k^m$$

$m < p-1$

per tutti k t.c. $p \nmid k$

$$S = k^m S$$

$$(k^m - 1) S \equiv 0 \mod p$$

$$(g^m - 1) S \equiv 0$$

$$S \equiv 0$$

$p-1 \nmid m \Rightarrow S \equiv 0$

$p-1 \mid m \Rightarrow S \equiv p-1$

$0, 1, 2, \dots p-1$

Se p primo

$ab \equiv 0 \iff \begin{cases} a \equiv 0 \\ b \equiv 0 \end{cases}$

$p \mid ab \Rightarrow p \mid a$ oppure $p \mid b$

- somme
- sottrazioni
- moltiplicazioni
- divisioni per un numero $\neq 0$

$\frac{3}{5} \pmod 7$

$\frac{3}{5} \cdot 5 = 3$

"$\frac{18}{37}$"

$\frac{3}{5} \equiv 2 \pmod 7$

1999

$\cdot 37 = 18$

37

2·37

2·37

1999·37

18

1999

0

$$\frac{1}{5} \pmod 7$$

$$a \cdot 37 \equiv 1 \quad (ppp)$$

$$a \cdot 37 \equiv 1$$

$$37^{p-2} \cdot 37 \equiv 37^{p-1} \equiv 1$$

$$\frac{1}{a} \equiv a^{p-2} \quad (p)$$

$$\frac{b}{a} = b \cdot \frac{1}{a} = b \cdot a^{p-2}$$

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}$$

$bd \not\equiv 0 \mod p$

$$2^m + 3^m + 6^m \equiv$$

Trovare i p tali che

$$6 \cdot 2^{p-2} + 3^{p-2} + 6^{p-2} \equiv 1 \pmod{p}$$

$$\frac{1}{2} + \frac{1}{3} + \frac{1}{6} = 1 \pmod{p}$$

$p \neq 2, 3$

$2, 3$

$$\frac{1}{ab} = \frac{1}{a} \cdot \frac{1}{b} \qquad a^{p-2} \cdot b^{p-2} = (ab)^{p-2}$$

$(\mathrm{mod}\ 3)$ $2x^2 + 3y^2 = 37$ scegliamo $p = 3$

"0^0" $2^0 = 1$

$3^y - 2^x = 1$

$3 - 2 = 1$

$9 - 8 = 1$

$3x^2 + 2y^2 = 37$

$(-1)^y = 3^y \equiv 1 \pmod 4$

y pari

$$3^{2y'} - 2^x = 1$$

$$3^{2y'} - 1 = 2^x$$

$$(3^{y'} - 1)(3^{y'} + 1) = 2^x$$

$$2^a \quad 2^b$$

$$(2^a \cdot 2^b) = 2$$

$3^{y'} - 1 = 2$

oppure

$3^{y'} + 1 = 2$

$$(3^y - 1, 3^y + 1) = (3^y - 1, 2) = 2$$

g_1, g_2

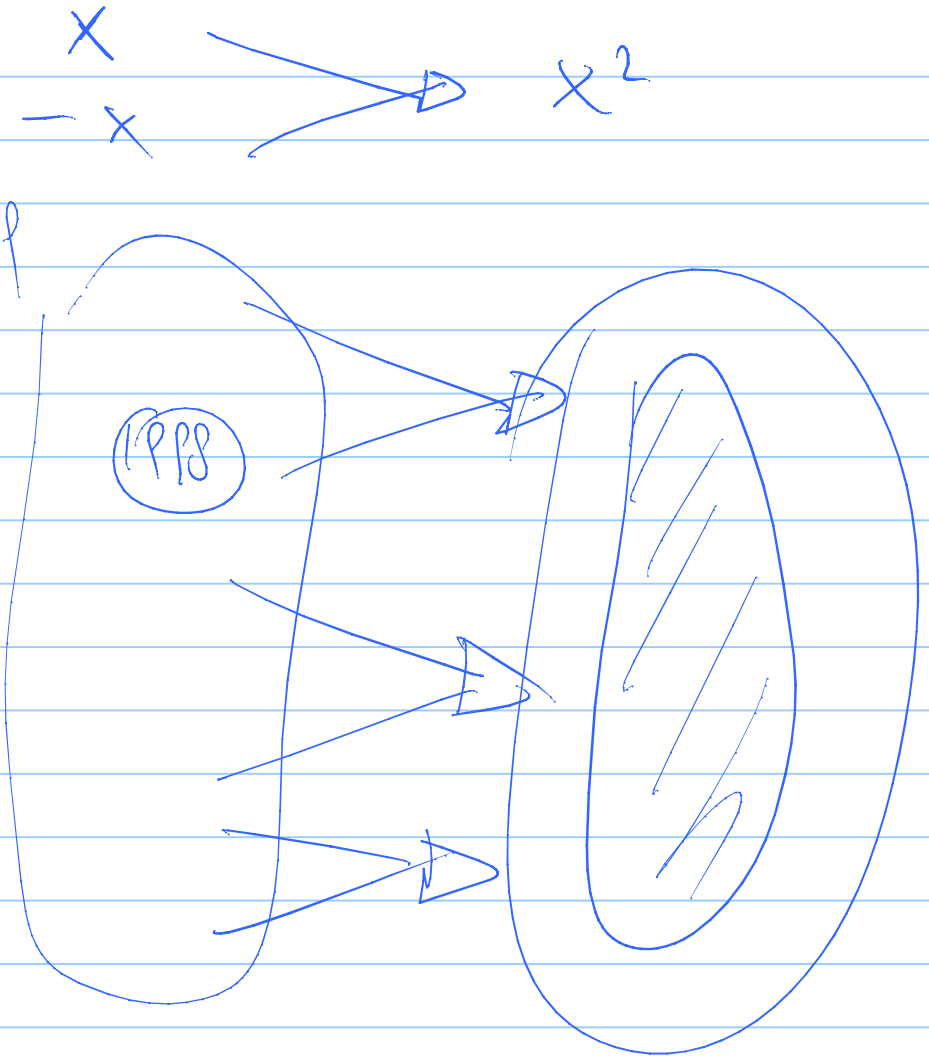
7

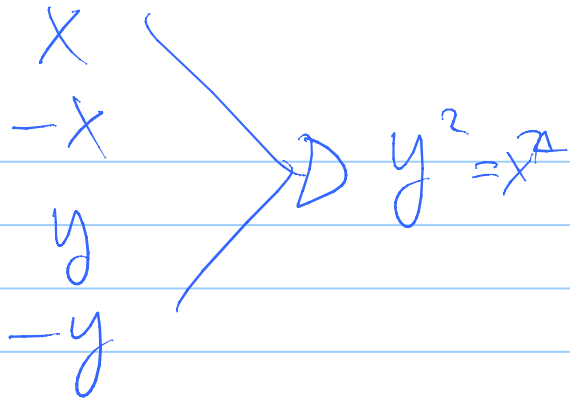
$3^1, 3^2, 3^3, 3^4, 3^5, 3^6$

$3^2, 3^4, 3^6, 3^8, 3^{10}, 3^{12}$

11

$3^2, 3^4, 3^6$





$y^2 = x^2$ (1PPP)

$\Downarrow$

$p \mid y^2 - x^2$

15

$p \mid (y+x)(y-x)$

3 5

7

g

$3^1, 3^2, 3^3, 3^4, 3^5, 3^6$

$3^5, 3^{10}, 3^{15} \ldots$

$3^4 \quad 3^3 \quad 3^2 \quad 3^1 \quad 3^0$

$1, 2, 3, \ldots p-2$

$k, 2k, 3k \ldots (p-2)k$

$(k, p-1)$

$ki \equiv kj \pmod{p-1}$

$p-1 \mid k(i-j)$

$(p-1, 2) = 2$

a^n

p

$\frac{1}{(p-1, a)}$ + (no zero)

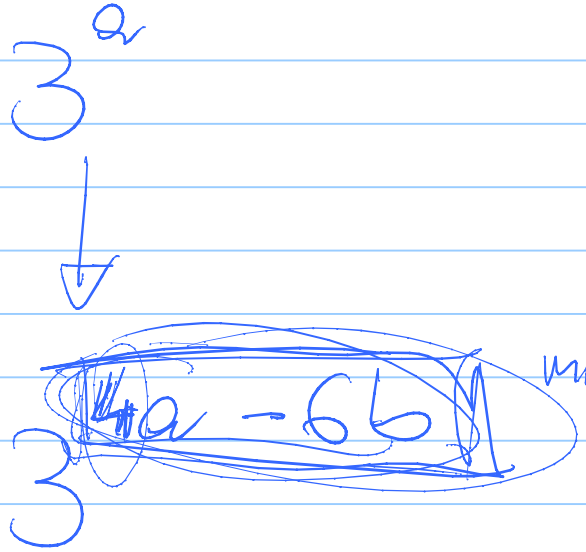
$1^4 \quad 2^4 \quad 3^4 \quad 4^4 \quad 5^4 \quad 6^4$

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

$(4, p-1)$

$3^0 \quad 3^4 \quad 3^8 \quad 3^{12} \quad 3^{16} \quad 3^{20}$

$3^2 \quad 3^0 \quad 3^4 \quad 3^2$



$4a - 6b = \dots$

7

$a^2 = 1$

$a^2 - 1 = 0 \rightarrow$ 2 sol

2·3

$a^3 - 1 = 0 \rightarrow$ 3 sol

13

$a^4 - 1 = 0$ < 4, 2

$x^3 - 1 = 0$

$x^3 - 8$ ✗ 3 0

$x^3 - 1 \mid x - 9$

grado 2

$x - 5$

grado 1