SthcW

Teoria dei Numeri 1 (BASIC)

Titolo nota 03/09/2012

1ª parte
- divisibilità (mcd)
- fattorizzazione, (valutazioni p-adiche)
- scrittura in base b
- $ax+by=c$

(appl.)

---

a divide b vuol dire che b è multiplo di a o equivalentemente che esiste un intero k tale che $\boxed{k\cdot a = b}$

$$a \mid b \iff a\cdot k = b \quad \text{(per qualche intero } k\text{)}$$

$$k = \frac{b}{a}$$

$a \mid b$ $\quad$ $a \mid c$ $\quad\Rightarrow\quad$ $a \mid b+c$ $\quad$ $a \mid b-c$

$$a \mid kb + \ell c + ha$$

fatti notevoli:

- $a-b \mid a^n - b^n$

$$\frac{a^n-b^n}{a-b} = a^{n-1} + a^{n-2}b + a^{n-3}b^2 + \cdots + b^{n-1}$$

- $a+b \mid a^n + b^n$ (solo se n è dispari)

$a^3+b^3 \mid a^6+b^6$

$a^2+b^2 \mid (a^2)^3+(b^2)^3$

$a^2+b^2 \mid a^6+b^6$

$c=a^2 \quad d=b^2$

$c+d \mid c^3+d^3$

p si dice primo se $(p>1)$

- $p \mid ab \Rightarrow p \mid a$ o $p \mid b$

  se p divide un prodotto allora divide uno dei fattori

- $p = ab \Rightarrow a=\pm 1$ o $b=\pm 1$ (irriducibile)

  (primi di Mersenne)

Es. 2^n-1 è primo $\Rightarrow$ n è primo

[se n è primo $\Rightarrow$ $2^n-1 \equiv 1 \ (n)$]

Supponiamo $p \mid n$ $\quad 1<p<n$ $\quad (Hp1)$

$$(2^p)-(1^p) \mid a^{\frac{n}{p}} - b^{\frac{n}{p}} = 2^n - 1^n$$

$a-b$

$$2^p - 1 \mid 2^n - 1$$

Abbiamo trovato un fattore che divide 2^n-1

$$(2^p-1)\cdot k = 2^n - 1$$

ma $(Hp1) \Rightarrow 1 < 2^p - 1 < 2^n - 1$

(primi di fermat) ($2^{64}+1$ non è primo)

Es. 2 2^n+1 è primo $\Rightarrow$ n è una potenza di 2

Proviamo a dimostrarlo per assurdo, quindi prendo $n = 2^k \cdot d$ con d dispari, $d > 1$, ora vorrei far vedere che 2^n+1 non è primo

$$2^{2^k} + 1^{2^k} \mid 2^{2^k \cdot d} + 1^{2^k \cdot d} \quad (?)$$

$$2^{2^k} + 1^{2^k} \mid \left(2^{2^k}\right)^d + \left(1^{2^k}\right)^d$$

Massimo Comun Divisore (MCD)

$MCD(a, b)$ $\{(a,b)$ è il MCD tra a e $b\}$

Fattorizzazione: Ogni numero naturale è esprimibile in modo UNICO come prodotto di primi

$$n = p_1^{\alpha_1} p_2^{\alpha_2} p_3^{\alpha_3} \cdots p_k^{\alpha_k}$$

$12 = 2^2 \cdot 3$ $\quad$ $128 = 2^7$

$33 = 3 \cdot 11$ $\quad$ $2012 = 2^2 \cdot 503$

$2013 = 3 \cdot 11 \cdot 61$

$$2^2 \cdot 503 = 2012 = a^2 - b^2 = (a+b)(a-b)$$

$$\begin{cases} a+b = 503 \\ a-b = 2^2 \end{cases} \qquad \begin{cases} a+b = 503 \cdot 2 \\ a-b = 2 \end{cases} \qquad \begin{cases} a+b = 503 \cdot 2^2 \\ a-b = 1 \end{cases}$$

$$2a = 507$$

$a = 504$

$b = 502$

$S + D = pari$

$$2012 = 504^2 - 502^2$$

se $2 \mid n$ ma $4 \nmid n$ $\Rightarrow$ no sol. a $n = a^2 - b^2$

MCD fatto con la fattorizzazione

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} \qquad 2^2 \cdot 3 \qquad 3 \cdot 11 \cdot 13$$

$$b = p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k} \qquad 2 \cdot 3^2 \qquad 3^2 \cdot 67$$

$$(a,b) = p_1^{\min(\alpha_1,\beta_1)} p_2^{\min(\alpha_2,\beta_2)} \cdots p_k^{\min(\alpha_k,\beta_k)} \qquad 2 \cdot 3 \qquad 3$$

tra a e b

d è il massimo comun divisore se per ogni c t.c. $c \mid a$ e $c \mid b$, allora $c \mid d$ e $d \mid a$ e $d \mid b$

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$$
$$b = p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k}$$
$$c = p_1^{\gamma_1} p_2^{\gamma_2} \cdots p_k^{\gamma_k}$$

$$\begin{cases} c \mid a \iff \gamma_i \le \alpha_i \quad \forall i \\ c \mid b \iff \gamma_i \le \beta_i \quad \forall i \end{cases}$$

$$c \mid (a,b) \iff \gamma_i \le \min(\alpha_i, \beta_i)$$

$v_{p_i}(a) = \alpha_i$ valutazione p-adica di a =

"l'esponente di p nella fattorizzazione di a"

$$v_2(a \cdot b) = v_2(a) + v_2(b)$$

$$v_2(a+b) \geq \min(v_2(a), v_2(b))$$

$$\rightarrow \quad a+b = p^{\alpha} \cdot k + p^{\beta} \cdot J = \begin{cases} \alpha > \beta & p^{\beta}\left(p^{\alpha-\beta} \cdot k + J\right) \\ \alpha < \beta & p^{\alpha}\left(k + J \cdot p^{\beta-\alpha}\right) \end{cases}$$

$v_2(10) = 1$

$v_2(15) = 0$

$v_2(10+15) = 0 \geq \min(1,0)$

$\min\left(v_p(a), v_p(b)\right) = k$ $\qquad a = p^k \cdot a_1$, $\; b = p^k \cdot b_1$

$$v_p\left((a+b)\right) = v_p\left(p^k (a_1 + b_1)\right) \geq k .$$

Oss. Se $v_p(a) \neq v_p(b) \Rightarrow v_p(a+b) = \min\left(v_p(a), v_p(b)\right)$

Se $v_p(a) = v_p(b) \Rightarrow$ boh? $v_p(a+b)$ può essere qualunque numero $\geq$ di $\min\left(v_p(a), v_p(b)\right)$

$p = 2 \qquad v_2(a) = v_2(b) \Rightarrow v_2(a+b) \geq \min\left(v_2(a), v_2(b)\right) + 1$

$$2^{k_1} \cdot d_1 + 2^{k_1} \cdot d_2 = 2^{k_1}\left(d_1 + d_2\right)$$

$$\underset{(2)}{v_2(1+3)} = \underset{(0)}{v_2(1)} + 2$$

$v_p(a+b) \leq \; ?$ $\qquad a = p^k - 1$, $\; b = 1$ $\qquad v_p(a) = v_p(b) = 0$

$v_p(a+b) \geq k$

Es. Trovare il massimo valore di

$$\left(n^2 + 2012, (n+1)^2 + 2012\right)$$

$d_n = (n^2 + 2012, (n+1)^2 + 2012)$

$d_n \mid n^2 + 2012$

$d_n \mid (n+1)^2 + 2012$

$d_n \mid 2n+1$

bisogna "togliere" n

$d_n \mid 2 \cdot (n^2 + 2012)$

$d_n \mid n(2n+1)$

$d_n \mid 2n+1$

$d_n \mid 2 \cdot (4024 - n)$

$d_n \mid 2n+1$

$d_n \mid 8049$

$3 \cdot 2683$

Noi vorremo un n per cui $d_n = 8049$

$d_n \mid 2n+1$ $\quad$ $8049 \mid 2n+1$

$8049 = 2n+1$? $\quad$ 4024

$8049 \mid (4024)^2 + 2012$

$$(n^2+2012,\ (n+1)^2+2012) =$$

$$= (n^2+2012,\ 2n+1)$$

$$= (2n^2+4024,\ 2n+1) \qquad d_n = (8049,\ 2n+1)$$

$$= (4024-n,\ 2n+1)$$

$$= (8049,\ 2n+1)$$

$$d_n = (n^3+56,\ (n+1)^3+56)$$

quando è massimo?

$$d_n = (407+6n,\ 7n+2-68\cdot 407)$$

Teorema di Bezout

fissiamo a,b,c, vogliamo trovare x,y tali che

$$\boxed{ax+by=c}$$

$2x+3y=4$ (1)
- $(x,y)=(2,0)$
- $(x,y)=(-1,2)$
- $(x,y)=(5,-2)$
- $(x,y)=(-4,4)$

Cerco di risolvere $2x+3y=0$ "omogeneo" (2) $(x,y)=(3k,-2k)$

$$2x=-3y \xrightarrow{x=3k} -2k=y$$

se (x_0, y_0) è sol. di (1) e (x_1, y_1) è sol. di (2) allora

$$2x_0 + 3y_0 = 4$$
$$2x_1 + 3y_1 = 6$$

$$2(x_0+x_1) + 3(y_0+y_1) = 4$$

(x_0+x_1, y_0+y_1) è sol. di (1)

$(2+3k, -2k)$ sono sol. di (1)
(al variare di k)

$$2x + 4y = 3$$

NON CI SONO SOLUZIONI PERCHÉ IL PRIMO MEMBRO È PARI MENTRE IL SECONDO " È DISPARI ASSURDO!

$$ax + by = c$$

oss. se $d \mid a$ e $d \mid b \Rightarrow d \mid c$

$\rightsquigarrow$ $\boxed{(a,b) \mid c}$ ← CONDIZIONE NECESSARIA AFFINCHÉ CI SIANO SOLUZIONI

Th. (Bezout) (La condizione è anche sufficiente)

Dati $a, b \in \mathbb{Z}$, esistono dei interi x, y, tali che

$$ax + by = (a, b)$$

Se volessi risolvere

$$ax + by = c$$

con $(a,b) \mid c \Rightarrow c = k \cdot (a,b)$

$$(x, y) = (k \cdot x_B, k \cdot y_B)$$

$$\boxed{ax + by = c}$$

$$= a k x_B + b k y_B = k(a x_B + b y_B) =$$

$$= k(a, b) = c$$

$(401, 355)$	$401 = 1 \cdot 355 + 46$	$61 \cdot 355 - 54 \cdot 401 = 1$
$(355, 46)$	$355 = 7 \cdot 46 + 33$	$7 \cdot 355 - 54 \cdot 46 = 1$
$(46, 33)$	$46 = 1 \cdot 33 + 13$	$7 \cdot 33 - 5 \cdot 46 = 1$
$(33, 13)$	$33 = 2 \cdot 13 + 7$	$2 \cdot 33 - 5 \cdot 13 = 1$
$(13, 7)$	$13 = 1 \cdot 7 + 6$	$2 \cdot 7 - 1 \cdot 13 = 1$
$(7, 6)$	$7 = 1 \cdot 6 + 1$	$\leftarrow 7 - 1 \cdot 6 = 1$

$(6,1)$ "

$6 = 6 \cdot 1$

[Curiosità: Le coppie più "Lente" sono (F_n, F_{n+1})]

Scrittura in base

$$n = b_0 + b_1 \cdot b + b_2 \cdot b^2 + b_3 \cdot b^3 + \dots + b_k \cdot b^k =$$

$$= \underline{b_k b_{k-1} b_{k-2} \dots b_0}_b$$

$$\underline{10}_2 = 2 = \underline{2}_3 = \underline{2}_4 = \underline{2}_{2012}$$

$$\underline{1001}_3 = 28 = \underline{11100}_2$$

$$7 \cdot 4 = \underline{111}_2 \cdot \underline{100}_2 = \underline{11100}_2$$

Es. 15 test iniziale $(a>b,\ c>d,\ b>d)$

$$\frac{2^a - 2^b}{2^c - 2^d} = \frac{2^b\left(2^{a-b} - 1\right)}{2^d\left(2^{c-d} - 1\right)} =$$

$$= 2^{b-d} \cdot \frac{2^\alpha - 1}{2^\beta - 1}$$

Quando $2^\beta - 1 \mid 2^\alpha - 1$? CLAIM: $\beta \mid \alpha$

1ª parte se $\beta \mid \alpha \Rightarrow 2^\beta - 1 \mid 2^\alpha - 1$

$$2^\beta - 1 \mid (2^\beta)^{\frac{\alpha}{\beta}} - (1)^{\frac{\alpha}{\beta}} = 2^\alpha - 1$$

2ª parte $2^\beta - 1 \mid 2^\alpha - 1 \iff$

$$2^\beta - 1 \mid 2^\beta (2^{\alpha-\beta} - 1) \iff$$

$$2^\beta - 1 \mid 2^{\alpha-\beta} - 1$$

$a \mid bc$, $(a,b) = 1 \iff a \mid c$

1° caso $\alpha - \beta < \beta$

Fatto se $a \mid b$ (e $b \neq 0$)

allora $|a| \leq |b|$

$a \cdot k = b$

$|a| \leq |a|\,|k| = |b|$

Se $0 < |b| < |a| \Rightarrow a \nmid b$

$|2^{\alpha-\beta} - 1| < |2^\beta - 1|$ non contraddice la tesi

solo quando $\alpha = \beta$

ma $\alpha = \beta \Rightarrow \beta \mid \alpha$ che contraddice l'ipotesi

---

se itero il procedimento di prima arrivo a

$$2^{\beta} - 1 \mid 2^{r} - 1 \qquad 0 \le r < \beta$$

$r = 0 \Rightarrow \beta \mid \alpha$

$r \neq 0 \Rightarrow$ assurdo

$$2^{\beta} - 1 \mid 2^{\alpha} - 1 \iff \beta \mid \alpha$$

Es. $\left(3^{\alpha} - 1, 3^{\beta} - 1\right) = 3^{(\alpha,\beta)} - 1$

$[(a,b) = (a, b-a)]$ ← basta questo

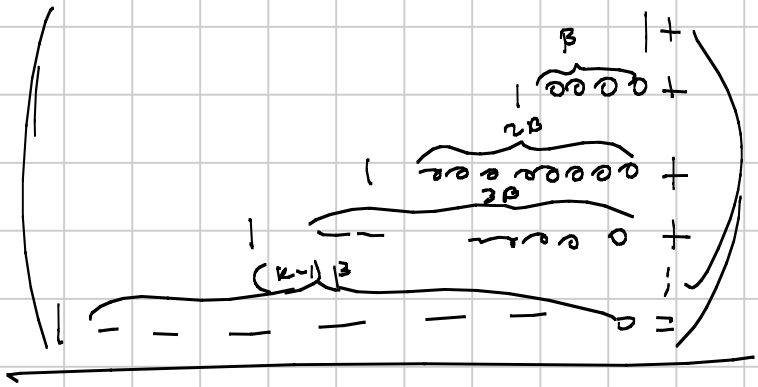
$= (b, b-a)$

Numeri della forma $2^{r} \cdot \dfrac{2^{\alpha} - 1}{2^{\beta} - 1}$. Dal

Fatto precedente $\alpha = k\beta$

$$2^{\gamma} \frac{2^{k\beta} - 1}{2^{\beta} - 1} = 2^{\gamma}\left(2^{(k-1)\beta} + 2^{(k-2)\beta} + \cdots + 2^{\beta} + 1\right) =$$

z



$$\underbrace{1000}_{B-1}\,|\,\underbrace{000}_{B-1}\,|\,\underbrace{000}_{B-1}\,|\,\underbrace{000}_{B-1}\,|\,00000$$

n° uni b

$$\underbrace{1\,0000}_{a}\;\underbrace{1\,000}_{a}\;\underbrace{1\,000}_{a}\;1\;\cdots\;|\,0000_{c}\,|_2 =$$

$$= 2^{c}\cdot\frac{2^{b(a+1)}-1}{2^{(a+1)}-1}$$

$$g = \underline{101}_2$$

$$B = \underline{1101}_2$$

$$\underline{11010000}_2$$

$$\boxed{1101}\,\underline{0000000000}_2$$

$\boxed{c=2 \quad d=1 \quad b=1}$

$$\frac{2^{a}-2^{b}}{2^{c}-2^{d}} = 2^{a-1}-1 \qquad a=p.$$

ARITMETICA MODULARE (o DELL'OROLOGIO)

Sono le 8. Tra 5 ore che ore sarà?

l'una

"$8 + 5 = 1$"

"$8 + 24 = 8$"

"$8 + 77 = 1$"

"$5 + 12 \cdot 8 = 5$"

"$5 + 11 \cdot 8 = 9$"

Le ore sono uguali a meno di multipli di 12. Considero gli interi "a meno" di multipli di 12.

$$(a + 12k)(b + 12j) =$$

$$= ab + 12kb + 12ja + 144jk$$

$$= ab + 12h$$

$$(3k \pm 1)^2 = 1 \pm 6k + 9k^2 = 1 + 3j$$

"un numero non multiplo di 3, elevato al quadrato, dà resto 1 diviso per 3"

"è congruo a 1 modulo 3"

$$(2k+1)^2 = 1 + 4k + 4k^2 = 1 + 4(k(k+1))$$

$$= 1 + 8j$$

generico $2h$ va in $4+n$

$4k+2$

$2d = 2(2k+1) = 4k+2$

"un q. di un n° disp. è $\equiv 1 \mod 8$"

$a \equiv b \quad (n)$ $\qquad a = b + kn$

$c \equiv d \quad (n)$ $\qquad c = d + jn$

$a + c \equiv b + d \quad (n)$ $\qquad a + c = b + d + nh_1$

$a \cdot c \equiv b \cdot d \quad (n)$ $\qquad ac = bd + n \cdot h_2$

Come funziona la divisione?

Cosa vuol dire dividere per 2?

Vuol dire moltiplicare per $\frac{1}{2}$. Chi è $\frac{1}{2}$?

$\frac{1}{2}$ è l'inverso moltiplicativo (detto reciproco) di 2, cioè quel numero che, moltiplicato per 2, dà come prodotto 1.

Se siamo in $\mathbb{N}$, esiste l'inverso di 1? sì

" " " 2? No

Se siamo in $\mathbb{Z}/n\mathbb{Z}$, esiste l'in- di 1? sì

esiste " " 2? non sisa

$\mathbb{Z}/4\mathbb{Z} = \{0, 1, 2, 3\}$

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

·	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

$\mathbb{Z}/3\mathbb{Z}$

·	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

2 ha un inverso e questo è 2 stesso

$$2^{-1} \equiv 2 \quad (3)$$

Quando esiste l'inverso di a modulo n?
Voglio trovare x tale che

$$ax \equiv 1 \quad (n)$$

$$ax = 1 + k \cdot n$$

$$ax - k \cdot n = 1 \qquad (*)$$

Ho riformulato in questo modo: devo trovare x, k tali che $(*)$ sia verificata. Ossia esistono sse $(a,n) \mid 1 \iff (a,n) = 1$,

Per trovare nei fatti x, mi basta applicare l'algoritmo di Bezout.

$$a \equiv b \quad (n)$$
$$c \equiv d \quad (n) \qquad (n, c) = 1$$

$$[(n, c) = (n, c + kn)]$$

$$a \cdot c^{-1} \equiv b \cdot d^{-1} \quad (n)$$

$$a \equiv b \quad (n)$$

(i) $2 \mid a \quad 2 \mid b \quad 2 \nmid n$

$$a \cdot 2^{-1} \equiv b \cdot 2^{-1} \quad (n)$$

$(a/2) \quad (b/2)$

$$2 \equiv 16 \quad (7)$$

$$1 \equiv 8 \quad (7) \qquad 8 \equiv 64 \quad (7)$$

$$2 \cdot 1 \equiv 2 \cdot 8$$

$$2^{-1} \cdot 2 \cdot 1 \equiv 2^{-1} \cdot 2 \cdot 8 \quad (7)$$

$$1 \cdot 1 \equiv 1 \cdot 8$$

(ii) $2 \mid a \quad 2 \mid b \quad 2 \mid n$

$$a \equiv b \quad (n)$$

$$a = b + kn$$

$$2a' = 2b' + k2n'$$

$$a' = b' + kn'$$

$$a' \equiv b' \quad (n')$$

$$(a/2) \equiv (b/2) \quad (n/2)$$

$a_1, a_2, a_3, \dots, a_k$ sono numeri naturali distinti $\leq n$

$$\text{Hp:} \begin{cases} n \mid a_1(a_2-1) \\ n \mid a_2(a_3-1) \\ \vdots \\ n \mid a_{k-1}(a_k-1) \end{cases} \qquad \text{Th: } n \nmid a_k(a_1-1)$$

$$n \mid a_1(a_2-1) \Rightarrow n \cdot k = a_1(a_2-1)$$

$$\Rightarrow a_1(a_2-1) \equiv 0 \pmod{n}$$

$$a_1 a_2 - a_1 \equiv 0 \pmod{n}$$

$$a_1 \equiv a_1 a_2 \pmod{n}$$

Attenzione, non possiamo dividere per a_1, o meglio non è detto.

$$\begin{aligned} a_1 &\equiv a_1 a_2 \pmod{n} \\ a_2 &\equiv a_2 a_3 \pmod{n} \\ a_3 &\equiv a_3 a_4 \pmod{n} \\ &\vdots \\ a_{k-1} &\equiv a_k a_{k-1} \pmod{n} \end{aligned}$$

$a_1 \equiv a_1 a_2 a_3 a_4 a_5 \dots a_k \pmod{n}$

$a_2 \equiv a_1 a_2 a_3 \dots a_k$.

Se avessimo $a_k \equiv a_k a_1$ otterrei $a_1 \equiv a_2 \equiv a_3 \dots \equiv a_k \equiv a_1 \dots a_k$

quindi tutti i numeri sono congrui tra di loro

ho contraddetto l'ipotesi? sì, usando il fatto che sono tutti $0 \le \ < n$

$a, b \quad a \neq b \quad e \quad a \equiv b \pmod{n}$

$n \mid a-b \Rightarrow n \le |a-b|$ no!!.

IMO - 2009 / 1.

Struttura moltiplicativa

$(2, 31) = 1$

	(31)	(11)	(5)	(3)
	5	10	4	2
$2^0 \equiv$	1	1	1	1
$2^1 \equiv$	2	2	2	2
$2^2 \equiv$	4	4	-1	1
$2^3 \equiv$	8	-3	-2	2
$2^4 \equiv$	16	5	1	1
$2^5 \equiv$	1	-1	2	2
		-2		1
		-4		2
		3		1
		5		2
t^{10}		1		

$(a,n)=1$ è vero che esiste $j>0$ t.c.

$$a^j \equiv 1 \quad (n) \; ?$$

Posso dire (principio dei cassetti) che esistono due esp. k_1, k_2 t.c. $(k_2 > k_1)$

$$a^{k_1} \equiv a^{k_2} \quad (n)$$

$$a^{k_1} \equiv a^{k_1} \cdot a^{k_2-k_1} \quad (n)$$

Ora divido per a k_1 volte e ottengo

$$1 \equiv a^{k_2-k_1} \quad (n)$$

il periodo di a^k modulo n si indica con $\text{ord}_n(a)$. È il minimo $j>0$ per cui $a^j \equiv 1 \; (n)$.

- Se $a^k \equiv 1 \; (n)$ allora $\text{ord}_n(a) \mid k$.

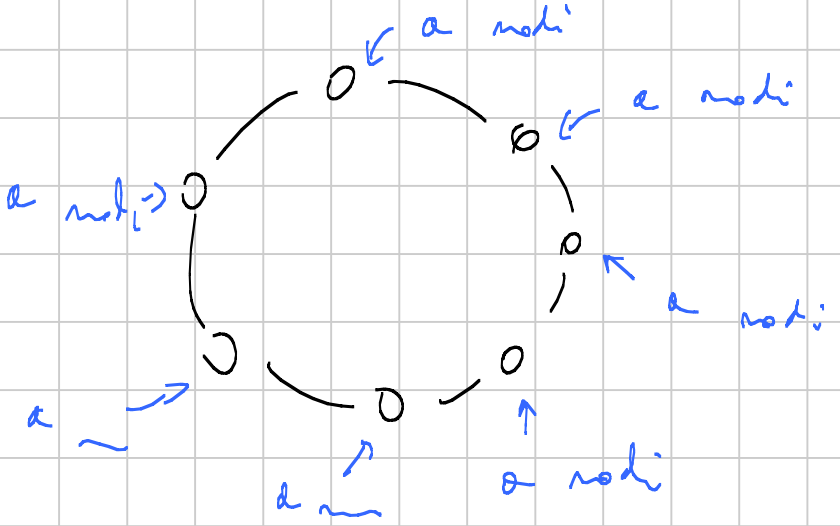
Piccolo Teorema di Fermat (LFT)

Sia p un numero primo e a un qualunque intero; allora vale

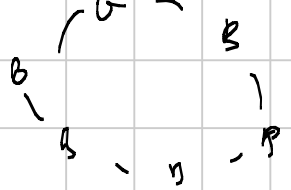
$$a^p \equiv a \quad (p)$$

Modo combinatorio (calato dal nulla)

Voglio costruire delle collane di perline, con p perline e ho a disposizione perline di a colori diversi. Quante sono le collane NON monocromatiche?



Scelgo in a^p modi le perline, tolgo le monocromatiche: $a^p - a$. Poiché se prendo una collana non monocromatica e la giro p volte ottengo p conf. diverse, allora



il numero di collane non monoc. è $\frac{a^p - a}{p}$

$\rightsquigarrow$ $p \mid a^p - a$ cioè $a^p \equiv a \ (p)$

□

II modo

$$\{1, 2, 3, 4, \dots, p-1\}$$

poi prendo $(a,p)=1$ $\quad p \nmid a$

$$\{a, 2a, 3a, 4a, \dots, (p-1)a\}$$

nessuno di essi è zero. Può essere che ci siano 2 numeri uguali modulo p?

$$ia \equiv 3a \quad (p)$$

$$i \equiv 3 \quad (p)$$

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

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

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

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

modo III, per induzione

$$\binom{p}{i} \equiv 0 \quad (p) \quad \text{se } i \neq 0, p$$

$$(a+1)^p \equiv a^p + \binom{p}{1} a^{p-1} + \binom{p}{2} a^{p-2} + \cdots + \binom{p}{p-1} a + 1$$

$$\equiv a^p + 1$$

Dim. per induz. (su a) $\forall$ che $a^p \equiv a \pmod p$

<u>base induttiva</u>: $a = 0$ $\quad 0^p \equiv 0 \pmod p$

<u>passo induttivo</u>: Supp. che $a^p \equiv a \pmod p$

ma allora $(a+1)^p \equiv a^p + 1 \equiv a + 1 \pmod p$.

□.

$(a, p) = 1 \Rightarrow a^{p-1} \equiv 1 \pmod p$

$\mathrm{ord}_p(a) \mid p-1$

$x^3 + y^5 = z^k$

lavorate modulo primi t.c. $3 \mid p-1$ o $5 \mid p-1$ o $15 \mid p-1$