TDN
~~Combinatoria~~ 2

me_go

Titolo nota 04/09/2014

~~Esempio~~ Abbiamo perle di q colori distinti

Quante collane possiamo fare con p perle di questi q colori?

Supponiamo di voler risolvere la diofantea

$$ax + by = c \qquad (*)$$

$$1227x + 4721y = 3737$$

$(*)$ è risolubile se e solo se $MCD(a,b) \mid c$.

($\Rightarrow$) $d = MCD(a,b)$, $ax+by$ è div. per d.

($\Leftarrow$) Bézout.

Tutte le soluzioni sono della forma $\left(x_0 + \frac{b}{d}k,\ y_0 - \frac{a}{d}k\right)$

con $k \in \mathbb{Z}$, (x_0, y_0) ~~[k = 0 = 1]~~

Qual è la cifra delle unità di $N = 37^{2529}$ nella scrittura in base 13?

= il resto della divisione di N per 13.

Trovare il più piccolo $n \geq 0$ t.c. $N \equiv n \pmod{13}$

$37 \equiv (-2) \mod 13$

k	37^k
0	1
1	-2
2	4
3	-8
4	$16 \equiv 3$
5	-6
6	$12 \equiv -1$

7	2
8	-4
9	8
10	-3
11	6
12	1

$37^{12} \equiv 1 \pmod{13}$ $\qquad N = 37^{2529}$

$2529 \equiv 9 \pmod{12}$

l'ultima cifra ... è 9

Consideriamo $a \in \mathbb{Z}$ e p un primo.

$\underbrace{a^0 \equiv 1, \; a^1 \equiv a, \ldots, a^{p-1}}$

quante classi di resto? p classi di resto.

$(a,p) = 1 \qquad a^k \not\equiv 0 \mod p$

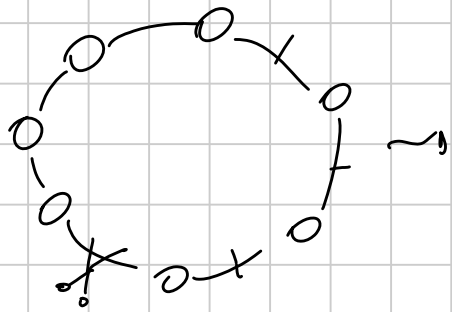
Per i coprimi, esistono $h,k \leq p-1$ t.c. $\boxed{a^h \equiv a^k}$

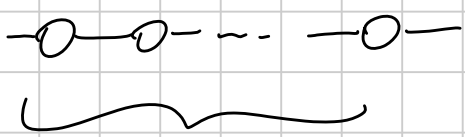
$\Rightarrow$ La succ. dei resti è def. periodica.

Se b è l'inv. di $a \mod p$, $a \cdot b \equiv 1 \Rightarrow a^h \cdot b^h \equiv 1$

$$1 \equiv a^h \cdot b^h \equiv a^k \cdot b^h = a^{k-h} \cdot (a^h \cdot b^h) \equiv a^{k-h}$$

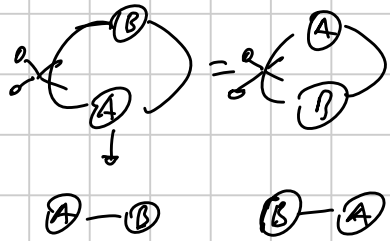
$\exists$ un int. $\ell \leq p-1$ t.c. $a^\ell \equiv 1 \pmod p$





q^p mod di fila una collana.

q collane monocromatiche



$q^p - q$ " non monocromatiche

↳ ciascuna contata p volte!

quante sono le collane non mono? $\frac{q^p - q}{p}$!

$$\frac{q^p - q}{p} \in \mathbb{Z} \Rightarrow q^p - q \equiv 0 \pmod p$$

Thm b inv. di $a \Rightarrow a^{p-1} \equiv 1 \pmod p$

(Piccolo teorema di Fermat)

es IMO 2005/4 | Determinare tutti gli interi coprimi con tutti i numeri della forma

$$X_n = \underbrace{6^n + 3^n + 2^n - 1}_{} \quad \text{per } n \geq 0$$

oss Basta lavorare con i primi.

Lavoriamo modulo p.

$$X_n = (3^n + 1)(2^n + 1) - 2$$

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

k $p \neq 2, 3$, $\quad 2, 3, 6$ sono invertibili

$\frac{1}{2}$ = inv. di 2, $\quad \frac{1}{3}$ = inv. di 3, $\quad \frac{1}{6}$ = inv di 6.

$$2^{p-1} \equiv 1 \pmod p$$
$$1$$

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

inv di $2 = 2^{p-2}$.

$$X_{p-2} = 2^{p-2} + 3^{p-2} + 6^{p-2} - 1$$

$$6X_{p-2} = 6 \cdot 2^{p-2} + 6 \cdot 3^{p-2} + 6^{p-1} - 6$$
$$1 \qquad\qquad\qquad 1$$
$$3 \cdot 2^{p-1} + 2 \cdot 3^{p-1} + 1 - 6 \equiv 0!$$

$\Rightarrow$ c'è 56 !

---

thm (Eulero-Fermat) $\quad a^{\varphi(m)} \equiv 1 \pmod m$

se $(a, m) = 1$

def $\varphi(m) = \#\{\text{interi } k,\ 1 \leq k \leq m,\ \text{coprimi con } m\}$

$\varphi(1) = 1$ $\qquad$ $(6) = 2$

$(2) = 1$ $\qquad$ $(37) = 36$

$(3) = 2$

$$\varphi\left(4721^{35} \cdot 65537^{12}\right) = 4721^{34}(4720) \cdot 65537^{11} \cdot 65536$$

$$65536 = 2^{16} = 2^{2^4}$$

$F_n := 2^{2^n} + 1$ è primo, si dice primo di Fermat.

es F_5 è div. per 641.

in generale $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1} = p^{\alpha-1}(p-1)$

$\varphi(m \cdot n) = \varphi(m) \cdot \varphi(n)$ se $MCD(m,n) = 1$.

fatto Prima abbiamo visto che -2 è tale che

$k>0$

12 è il più piccolo esponente t.c. $(-2)^k \equiv 1 \pmod{13}$

$(-2)^0, (-2)^1, \dots, (-2)^{11}$ sono classi distinte.

Per ogni p esiste g t.c. $g^0, g^1, \dots, g^{p-2}$ sono tutte distinte, e questo g si chiama generatore mod p.

Achtung! Esiste un generatore mod m se e solo se

m è in $\{2, 4, p^\alpha, 2p^\alpha\}$

no 2^{k+2} perché $a^2 \equiv 1 \pmod 8$ se $a \equiv 1 \pmod 2$.

no $p \cdot q$: perché?

Se g genera mod $p^\alpha \Rightarrow g$ o $g+p$ genera mod $p^{\alpha+1}$

es IMO 75/4 Dato n scrivo $S(n)$ = somma delle cifre.

$$S(S(S(4444^{4444}))) = ?$$

Facciamo mod 9! $\varphi(9)=6$

$$4444^{4444} \overset{?}{\equiv} 7^{4444} \equiv 7^4 \equiv (-2)^4 \equiv 16 \equiv 7$$

$A = S(4444^{4444}) \leq (4 \cdot 4444 - 1) \cdot 9 \leq 180000$

↳ ha meno di $4 \cdot 4444 - 1$ cifre

$B = S(A) \leq 4 \cdot 9 = 36$

$S(B) \leq 20$!! . quanti interi ≤ 11 sono $\equiv 7 \pmod 9$? Solo 7!

$$S(S(S(4444^{4444}))) = 7$$

---

es $1^{135} + 2^{135} + 3^{135} + \dots + 65536^{135}$

è divisibile per 65537?

sol 1 $k^{135} + (-k)^{135} \equiv 0 \pmod{65537}$ $\forall k$

sol $\exists g$ gen. tale che $\forall a \in \{1, \dots, p-1\}$ $\exists k$ t.c. $a = g^k$

$$= (g^{k_1})^{135} + (g^{k_2})^{135} + \dots + (g^{k_{p-1}})^{135} =$$

$$= (g^1)^{135} + (g^2)^{135} + \dots + (g^{p-1})^{135} =$$

$$= (g^{135})^0 + \dots + (g^{135})^{p-2} =$$

$$= \frac{(g^{135})^{p-1} - 1}{g^{135} - 1} \equiv \frac{1-1}{g^{135}-1} \equiv 0 \ (p).$$

$$1^2 + \dots + 65536^2$$

$$= \frac{(g^2)^{p-1} - 1}{g^2 - 1} \equiv \frac{1-1}{g^2-1} \pmod p$$

deve esistere l'inverso!

ovvero $g^2 \not\equiv 1 \pmod p$

$p=2$ $\quad 1 \not\equiv 1 \not\equiv 0 \pmod 2$

$p=3$ $\quad 1+4 = 5 \not\equiv 0 \pmod 3$

---

thm **Teorema cinese del resto**

Se m_1, m_2 sono coprimi, allora le congruenze

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \end{cases}$$

ha una ed una sola soluzione $\pmod{m_1 \cdot m_2}$.

$$x \equiv a_1 \pmod{m_1} \iff x = a_1 + k_1 m_1$$

$$\iff x = a_2 + k_2 m_2$$

stiamo cercando sol. (in k_1, k_2) dell'equazione

$$a_1 + k_1 m_1 = a_2 + k_2 m_2$$

$$m_1 k_1 - m_2 k_2 = (a_2 - a_1) \overset{\text{Bézout}}{\implies} \text{ha sol.}$$

se ho due sol., $k_1' - k_1$ multiplo di m_2

$$\left.\begin{aligned} x &= a_1 + k_1 \cdot m_1 \\ x' &= a_1 + k_1' \cdot m_1 \end{aligned}\right| \Rightarrow x - x' = m_1 \underbrace{(k_1 - k_1')}_{\text{div. per } m_2}$$

$$\Rightarrow x \equiv x' \pmod{m_1 \cdot m_2}$$

$$x + m_1 m_2 \equiv a_1 \pmod{m_1}$$

$$\equiv a_2 \pmod{m_2}$$

<u>es</u> Dimostrare che $\forall p \ \exists n \quad 2^n \equiv n \pmod{p}$

Se n è multiplo di $p-1 \Rightarrow 2^n \equiv (2^{p-1})^k \equiv 1$

Se $n \equiv 0 \ (p-1) \Rightarrow 2^n \equiv 1 \pmod{p}$

Concludo n come sopra, in più $n \equiv 1 \pmod{p}$

$p, p-1$ sono coprimi? $(p - (p-1) = 1!)$

$$\begin{cases} n \equiv 0 \pmod{p-1} \\ n \equiv 1 \pmod{p} \end{cases}$$

$\exists!$ cl. mod $p(p-1)$. $\Rightarrow$ ☺

$n = (p-1)^2$ $\qquad n \equiv 1 \pmod{p}$

$n \equiv 0 \pmod{p-1}$

(es 10, p 39) $D = \{ n \text{ t.c. } n \mid 2^n + 1 \}$

a) Quali sono i primi in D?

p. Allora $2^p + 1 \equiv 2 + 1 \equiv 3 \pmod p$

$\equiv 0 \mod p$ se e solo se $p = 3$!

$2^3 + 1 = 9 \equiv 0 \pmod p$.

$\Rightarrow$ L'unico primo in D è 3.

b) Quali sono le potenze di primi in D?

p^k. $\pmod p$ $2^{p^k} + 1 \equiv (2^{p^{k-1}})^p + 1 \equiv 2 + 1 \equiv 3$

(per induzione)

$\Rightarrow p = 3$.

$3 \mid 2^3 + 1$

$3^\alpha \parallel 2^{3^2} + 1 = (2^3)^3 + 1 = \underbrace{(2^3+1)}_{\text{è div. per } 3} \cdot \underbrace{((2^3)^2 - 2^3 + 1)}$

divide e basta.

$2^3 \equiv -1 \pmod 3$ $\qquad (2^3)^2 - 2^3 + 1$

$(-1)^2 - (-1) + 1 \equiv 0 \ (3)$

Se $3^\alpha \parallel 2^3 + 1 \Rightarrow 3^{\alpha+1} \nmid 2^{3^2} + 1$

$3^\alpha \parallel \underbrace{2^{3^k} + 1}_{N} \Rightarrow 2^{3^{k+1}} + 1 = N \cdot \left((N-1)^2 - (N-1) + 1\right)$

$N \equiv 0 \pmod 3 \Rightarrow (-1)^2 + 1 + 1$

$N - 1 \equiv -1 \pmod 3$

$3 \mid 2^3 + 1 \Rightarrow 3^k \mid 2^{3^k} + 1$

in realtà: $3^{k+1} \parallel 2^{3^k}+1$ (LTE)

(c) $p \cdot q$

Dimostrazione: se a è coprimo con p, allora $a^{p-1} \equiv 1 \ (p)$

$$ord_p(a) = \text{ordine moltiplicativo di } a \text{ mod } p =$$
$$= \min\{k>0 \mid a^k \equiv 1 \mod p\}$$

in realtà $ord_p(a) \mid p-1$ $\quad ord_a(p) = x$

$$a^{p-1} \equiv a^x \equiv 1 \Rightarrow a^{h(p-1)+kx} \equiv 1 \pmod p$$

$$\Rightarrow x = MCD(x, p-1) \Rightarrow x \mid p-1.$$

$$pq \mid 2^{pq}+1 \ ?$$

$$p \mid 2^{pq}+1 \Rightarrow 2^{pq}+1 \equiv 0 \ (p)$$
$$2^{pq}+1 \equiv 0 \ (q)$$

$$2^{pq}+1 \equiv (2^q)^p+1 \equiv 2^q+1 \equiv 0 \ (p)$$
$$2^p+1 \equiv 0 \ (q)$$

$$\Rightarrow 2^q \equiv -1 \ (p) \Rightarrow 2^{2q} \equiv (-1)^2 \equiv 1 \ (p)$$

$$2q = k \cdot ord_p(2)$$

(divisore di $p-1$)

$$\Rightarrow ord_p(2) \in \{1, 2, q, 2q\}$$

$\text{ord}_p(2) = 1 \Rightarrow 2^1 \equiv 1 \pmod p$ ho

$\text{ord}_p(2) = 2 \Rightarrow 2^2 \equiv 1 \pmod p \Rightarrow p = 3$

$\Rightarrow \underbrace{\text{ord}_p(2)}_{\text{div. di } p-1} \geq q \Rightarrow q \leq p-1$

$p \leq q-1 \quad (\text{se } q \neq 3)$

non può succedere a meno che $p = 3$

se $p = 3$: q t.c. $2^{3q} + 1 \equiv 0 \pmod q$

111

$q \pmod q$

$\Rightarrow q = 3$. $\Rightarrow$ non ci sono prodotti

$p \cdot q$ in D se p, q primi distinti.

TST 100 ? 01 02 !

m intero positivo, a intero positivo

$a, a^a, a^{a^a}, a^{a^{a^a}} \ldots$

Questa successione è definitivamente periodica mod m?

$x_1, x_2, \ldots, x_n, \ldots$

$\begin{cases} x_1 = a \\ x_{n+1} = \cancel{x_n^a} = a^{x_n} \end{cases}$

Dovrebbe essere vero che a^k è periodica (in k)

di periodo $\ell \mid \varphi(m)$ mod m da un certo punto in poi. (perché φ è moltiplicativa)

[vale teo. cinese + un po' di malizia].

È vero che x_{n+1} è def-periodica mod m
se x_n è " " mod $\varphi(m)$.

MA $\varphi(m) < m$ (se $m > 1$).

ind. esterna!
$\Longrightarrow$ x_n è periodica (da un certo punto in poi)

$x^2 \equiv 0, 1$ (3)

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

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

$x^2 \equiv 0, 1, -1$ (5)

dom Quanti sono i residui quadratici mod p?
cubici ?
k-esimi ?

$\rightarrow \frac{p+1}{2}$.

Sono al più $\frac{p+1}{2}$: facile: $|0|$ sta per conto suo
$|1, -1| \leftarrow$
$|2, -2| \leftarrow$
$\vdots$
$|\frac{p-1}{2}, -\frac{p-1}{2}| \leftarrow$

$a^2 \equiv b^2 \pmod p$, $0 \le a, b \le \frac{p-1}{2}$

$(a-b)(a+b) \equiv 0 \pmod p$ $\quad 0 \le a+b \le p-1$

o $a=b=0$,

oppure $p \mid a-b$

$\Rightarrow a=b$.

$\Rightarrow$ ci sono esattamente $\frac{p+1}{2}$ residui quad. mod p.

---

per $p=2$ ce ne sono 2.

Tutte le classi di resto $\neq 0$ sono potenze di un generatore.

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

$g^0, g^2, \dots, g^{2(p-1)}$ $\quad$ se $p>2$

$p-1$ è pari

$p-1 = \frac{p-1}{2} \cdot 2$

ci è g^{p-1}

$\longrightarrow + 1 \equiv 0$!!

$\frac{p-1}{2}$

$g^0, g^2, \dots, g^{p-3}, g^{p-1}$ poi si ripetono.

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

Quando $d = MCD(k, p-1) \neq 1$, ci sono ripetizioni!

La prima rip. è quando $k \cdot x$ è multiplo di $p-1$

Quando $x = \frac{p-1}{d}$

Ne abbiamo beccati $\frac{p-1}{d}$ distinti

e poi c'è lo 0 ☺

Come si fa a capire se n è un residuo quadratico mod p? es $n = -1$.

$\exists x$ t.c. $x^2 \equiv -1 \pmod p$

$x \not\equiv 0 \ (p) \Rightarrow x \equiv g^y$ per qualche y

$x^2 \equiv (g^y)^2 \equiv g^{2y}$.

$$(x^2)^{\frac{p-1}{2}} = x^{p-1} \equiv 1$$

e $q^{\frac{p-1}{2}} \equiv 1 \Rightarrow q$ è un res. quadratico.

$\| g^b$ per qualche b. Se b è pari $\Rightarrow$ ☺

$\Rightarrow q \equiv (g^{b/2})^2$.

e b è dispari? $b = 2c+1$

$g^{(2c+1)\frac{p-1}{2}} = \cancel{(g^{p-1})^c} \cdot g^{\frac{p-1}{2}} \not\equiv 1$ perché

g è un generatore ($\forall p > 2$)

$\Rightarrow$ a è un res. quad. mod $p \Leftrightarrow q^{\frac{p-1}{2}} \equiv 1 \ (p)$.

q è un res. k-esimo mod $p \Leftrightarrow q^{\frac{p-1}{d}} \equiv 1 \ (p)$

dove $d = MCD(k, p-1)$.

(-1) è res. quadratico $\iff (-1)^{\frac{p-1}{2}} \equiv 1 \pmod p$

- $\frac{p-1}{2}$ è pari, $(-1)^{\text{pari}} \equiv 1$ ✓
- $\frac{p-1}{2}$ è dispari, $(-1)^{\text{disp}} \equiv -1$ ✗

- (-1) è res. quad. mod. p se e solo se

$p = 2$ oppure $p \equiv 1 \pmod 4$

folklore se $p \equiv 1 \pmod 4$ allora $p = x^2 + y^2$

---

es ~~4~~, 56, 57, 58 pag. 11

es 4, 9 pag. 39 | es. 8, 10 p. 38

es Dimostrare che $\forall p \neq 2, 5$ $\exists$ $\underbrace{11\ldots11}_{n \text{ cifre}} \equiv 0 \pmod p$

es Sia $\mathcal{P}$ l'insieme dei primi che dividono almeno un numero della forma

$$2^{n^3+1} - 3^{n^2+1} + 5^{n+1}$$

Allora $\mathcal{P}$ è infinito.

---

es 57 | $A_n = 5^n + 3^n + 1$ è primo $\Rightarrow n$ è div per 12

sol $p \neq 3$ $p \neq 5$, poi si vede:

mod 3, $3^n \equiv 0 \pmod 3$ se $n \neq 0$.

$n = 0$, allora a posto $1+1+1$ primo ~~$\neq$~~, ma n è div. per 12.

↳ $5^n + 1^n \equiv (-1)^n + 1 \equiv 0$ se n è dispari.

se n disp., A_n è div. per 3, $A_n > 3$. ✓

- $5^n \equiv 0 \pmod 5$

$A_n \equiv 3^n + 1$ ← 1, 3, (-1), 2, 1 } $+1$. se $n \equiv 2 \pmod 4$

A_n è div per 5. $A_n > 5$ ⇝ non è primo.

$n = 1$ ⇝ $A_1 = 5 + 3 + 1 = 3^2$

$n = 2$ ⇝ $A_2 = 35 = 5 \cdot 7$

$A_n \equiv 5^n + 3^n + 1 \pmod 7$

5^n	3^n	
1	1	1 → 3
-2	3	1 → 3
4	2	1 → 0
-1	-1	1 → 1
2	-3	1 → 0
-4	-2	1 → 2
1	1	1 → 3

se $n \equiv 2, 4 \pmod 6$

⇓

$7 \mid 5^n + 3^n + 1$ ✓

⇒ $12 \mid n$. ☺.

es. 8) max d_n, $d_n = MCD(100 + n^2, 100 + (n+1)^2)$.

$MCD(a,b) \mid a - kb \quad \forall k \in \mathbb{Z}$.

$d_n \mid (100 + (n+1)^2) - (100 + n^2) = 2n+1$ → dispari

$d_n \mid MCD(200 + 2n^2, 2n+1) \mid 200 + 2n^2 - n(2n+1)$

$d_n \mid 200 - n \mid 400 - 2n$

$d_n \mid (400 - 2n) + (2n+1) = 401$

$n = 200$? $100 + 200^2 = 401 \cdot 100$

$100 + 201^2 = 100 + 200^2 + 401$ ☺

---

es 10| idea: non ci sono sol!

cerchiamo p tale che ci siano pochi residui quad. e 5-upli mod p.

$\rightsquigarrow$ $5 \mid p-1$ ma $p = 11$?

---

ex.

es 9| Dati d, m, n interi positivi, dimostrare che esiste una prog. aritm. lunga $m+1$ di ragione d tale che ogni elem. è divisibile per una pot. n-ma

sol Prendiamo $m+1$ primi $p_1, \dots, p_{m+1}$ che non dividono d.

$$x,\ x+d,\ x+2d,\ \dots,\ x+md$$

$$\begin{cases} x \equiv 0 \pmod{p_1^n} \\ x+d \equiv 0 \pmod{p_2^n} \\ \vdots \\ x+md \equiv 0 \pmod{p_{m+1}^n} \end{cases}$$

$$\begin{cases} x \equiv 0 \pmod{p_1^{n_1}} \\ x \equiv -d \pmod{p_2^{n_2}} \\ \vdots \\ x \equiv -m_d \pmod{p_{m_n}^{n_{m_n}}} \end{cases} \Rightarrow \exists \text{ sol. (teo. cinese).}$$

---

es ultimo $B_n = \underbrace{2^{n^3+1}}_{\gg} - \underbrace{3^{n^2+1} + 5^{n+1}}_{\text{se } n>>0,\ B_n - 2^{n^3+1} \ll 2^{n^3+1}}$

Supp. P finito: $p_1, \dots, p_N$ $\quad B_n - 2^{n^3+1} < 2^{n^3}$ ex

idea: trovo n t.c. B_n non sia div. per nessuno di questi prim.

se $(p_1-1) \mid n \Rightarrow B_n = 2^{(p_1-1)\cdot k+1} - 3^{(p_1-1)k'+1} + 5^{(p_1-1)\cdot k''+1}$

$\Rightarrow B_n \equiv (2^k)^{p_1-1} \cdot 2 - (--)^{p_1-1} \cdot 3 + (--)^{p_1-1} \cdot 5$

se $p \neq 2,3,5$ abbiamo visto

$B_n \equiv 4 \pmod{p_1} \Rightarrow B_n \neq 0 \pmod{p_1}$

$n := (p_1-1)(p_2-1) \cdots (p_N-1)$

ho quasi finito:

$5 \mid B_n$?

no, $2^{n^3+1} \equiv 2 \pmod 5$ $\quad (\text{se } N \geq 3)$

$3^{n^2+1} \equiv 3 \pmod 5$

idem per 3.

escludere che $B_n = 2^x$ per qualche x.