# TEORIA DEI NUMERI 2 (darkcrystal)

Titolo nota 06/09/2013

## Inverso moltiplicativo

$$ax \equiv b \pmod{n}$$

$ax \equiv 1 \pmod{n}$ ammette soluzione

$$\Updownarrow$$

$ax + ny = 1$ ammette soluz.

$$\Updownarrow$$

$$(a, n) = 1$$

Supponiamo di avere una soluzione, chiamia-mola $s$: $a \cdot s \equiv 1 \pmod{n}$

Come risolvo $a \cdot x \equiv b \pmod{n}$ ?

Moltiplico per "$a^{-1}$" (cioè $s$)

e trovo $(sa)x \equiv sb \ (n)$

$$x \equiv sb \pmod{n}$$

$s = a^{-1}$ = inverso moltiplicativo di $a$ mod $n$

Quindi, in generale?

$$ax \equiv b \pmod{n}$$

$$d = (a, n) \qquad n' = n/(a,n)$$

Condizione necessaria: $d \mid b$

$$(a,n)\underbrace{\frac{a}{(a,n)}}_{a'} x \equiv (a,n)\underbrace{\frac{b}{(a,n)}}_{b'} \pmod{n}$$

$\iff$

$$a' x \equiv b' \pmod{n'}$$

$\iff$ $$x \equiv (a')^{-1} b' \pmod{n'}$$

Oss importante

Supponiamo di sapere $ax \equiv ay \mod n$ con $(a,n) = 1$. Allora $x \equiv y \pmod{n}$

Dim: moltiplico per $a^{-1}$ entrambi i membri

$$3x \equiv 3 \pmod{10} \Rightarrow x \equiv 1 \ (10)$$

(Peraltro, $3^{-1} \doteq 7 \pmod{10}$)

Se invece ho $3x \equiv 13 \pmod{10}$, non posso "dividere per 3", ma posso "molt.

per $7 \equiv 3^{-1}$ ", quindi:

$$21x \equiv 91 \pmod{10}$$

$$x \equiv 1 \pmod{10}$$

# TEOREMA CINESE DEL RESTO

Cosa succede se ho 2 (o più) congruenze modulo cose diverse?

$$\begin{cases} x \equiv 13 \pmod{8} \\ x \equiv 1000 \pmod{96} \end{cases}$$

Un tale x non esiste! (parità)

$$\begin{cases} x \equiv 3 \mod 4 \\ x \equiv 7 \mod 5 \end{cases} \qquad x = 7$$

$$\iff \begin{cases} x \equiv 7 \mod 4 \\ x \equiv 7 \mod 5 \end{cases}$$

$$\iff 4 \mid x-7 \quad e \quad 5 \mid x-7$$

$$\iff 20 \mid x-7 \iff x \equiv 7 \pmod{20}$$

Con Bézout: $x = 3 + 4k$

$$x - 7 = (-4 + 4k) = 5h$$

$$\iff 4k + 5h' = 4$$

TEO: Un sistema di congruenze

$$\begin{cases} x \equiv a \pmod{m} \\ x \equiv b \pmod{n} \end{cases}$$

in cui $(m,n)=1$ ammette una ed una sola soluzione modulo $m \cdot n$

$$\begin{cases} x \equiv 13 \pmod{96} \\ x \equiv 27 \pmod{8} \end{cases}$$

Vogliamo moduli coprimi

$$x \equiv 13 \pmod{\underset{\substack{\| \\ 3\cdot 32}}{96}} \iff \begin{cases} x \equiv 13 \pmod{3} \\ x \equiv 13 \pmod{32} \end{cases}$$

$$\begin{cases} x \equiv 13 \pmod{3} \\ x \equiv 13 \pmod{32} \\ x \equiv 27 \pmod{8} \end{cases} \rightsquigarrow \begin{matrix} x \equiv 13 \pmod{8} \\ x \equiv 27 \pmod{8} \end{matrix}$$

Il sistema non ha soluzione. Invece

$$\begin{cases} x \equiv 13 \pmod{96} \\ x \equiv 5 \pmod{8} \end{cases}$$

$$\iff \begin{cases} x \equiv 13 & (3) \\ x \equiv 13 & (32) \\ x \equiv 5 & (8) \end{cases}$$ inutile

Esempio

$$\begin{cases} x \equiv 4 \pmod{5} \\ x \equiv 5 \pmod{6} \\ x \equiv 6 \pmod{7} \\ x \equiv 7 \pmod{8} \\ x \equiv 8 \pmod{9} \end{cases}$$

$$\iff \begin{cases} x \equiv 4 & (5) \\ \cancel{x \equiv 1} & (2) \\ \cancel{x \equiv 2} & (3) \\ x \equiv 6 & (7) \\ x \equiv 7 & (8) \\ x \equiv 8 & (9) \end{cases} \iff \begin{cases} x \equiv 4 & (5) \\ x \equiv 6 & (7) \\ x \equiv 7 & (8) \\ x \equiv 8 & (9) \end{cases}$$

Esiste un'unica soluz. della forma

$x \equiv \,?\quad (\text{mod } 5 \cdot 7 \cdot 8 \cdot 9)$

$$\iff \begin{cases} x \equiv -1 & (5) \\ \quad '' & (7) \\ & (8) \\ & (9) \end{cases}$$

LA soluzione è quindi $x \equiv -1 \; (5 \cdot 7 \cdot 8 \cdot 9)$

Altro esempio Trovare il resto della divisione di $10^{100}$ per $144$

$x \equiv 10^{100} \quad (\text{mod } 2^4 \cdot 3^2)$

$$\iff \begin{cases} x \equiv 10^{100} & (\text{mod } 2^4) \\ x \equiv 10^{100} & (\text{mod } 3^2) \end{cases}$$

$$\iff \begin{cases} x \equiv 0 & (\text{mod } 2^4) \\ x \equiv 1 & (\text{mod } 3^2) \end{cases}$$

$\iff x \equiv 64 \mod 144$

# Comportamento delle potenze

$1, a, a^2, a^3, \dots \mod n$

Per pigeonhole, esistono due esponenti $h$ e $k$ con $a^h \equiv a^k \mod n \quad (\star)$

Diciamo $k > h$

Supponiamo che $\boxed{(a, n) = 1.}$

Allora esiste un $b$ t.c. $ab \equiv 1 \pmod n$, e da $\star$ trovo $b^h a^h \equiv b^h a^h a^{k-h} \ (n)$

$$\iff (ba)^h \equiv (ba)^h \cdot a^{k-h} \pmod n$$

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

Se non ho $(a, n) = 1$?

Potenze di $2 \mod 16$: $\underbrace{1, 2, 4, 8,}\ 0, 0, 0, \dots$

Potenze di $2 \mod 48$:

$$\underbrace{1, 2, 4, 8,}\ 16, 32, 16, 32, \dots$$

$$2^k \mod 48 \longleftrightarrow \begin{cases} 2^k \mod 3 \\ 2^k \mod 16 \end{cases}$$

$$\begin{cases} 2^{0} \equiv 1 \pmod 3 \\ 2^{0} \equiv 1 \pmod{16} \end{cases}$$

$$\begin{cases} 2^1 \equiv 2 & (\mathrm{mod}\ 3) \\ 2^1 \equiv 2 & (\phantom{mod}\ 16) \end{cases}$$

$$\vdots$$

per $k \geq 4$ $\begin{cases} 2^k \equiv (-1)^k & (\mathrm{mod}\ 3) \\ 2^k \equiv 0 & (\mathrm{mod}\ 16) \end{cases}$

Potenze di 6 mod $2^5 \cdot 3^7$: prima o poi fanno zero...

**Ordine moltiplicativo** $(a, n) = 1$. Sappiamo che esiste $h > 0$ t.c. $a^h \equiv 1 \pmod{n}$

L' **ord. molt.** di $a$ mod $n$ – $\mathrm{ord}_n(a)$ – è il più piccolo $h$ con questa proprietà:

**Prop. fondamentale** $a^x \equiv 1 \pmod{n}$

$$\iff \mathrm{ord}_n(a) \mid x$$

$\Leftarrow$ ovvio: $a^x = \left(a^{\mathrm{ord}}\right)^{\text{qualcosa}} \equiv 1^q \equiv 1$

$\Rightarrow$ Scriviamo $x = \mathrm{ord}_n(a) \cdot h + r$,

dove $0 \leq r < \mathrm{ord}_n(a)$

$$1 \equiv a^x \equiv \left(a^{\mathrm{ord}_n(a)}\right)^h \cdot a^r \pmod{n}$$

$$\equiv 1^h \cdot a^r \pmod n$$

Quindi $a^r \equiv 1 \pmod n$, e siccome $r < \mathrm{ord}_n(a)$ $r$ deve essere $0$, cioè $\mathrm{ord} \mid x$.

Ordine moltiplicativo = periodo della successione

Cosa può essere $\mathrm{ord}_p(a)$ ?

Piccolo Teorema di Fermat: se $(a, p) = 1$,

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

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

Sempre $a^p \equiv a \pmod p$

Dimostrazione Considero $\{1, 2, 3, \dots, p-1\}$

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

Dico che modulo $p$ sono lo stesso insieme

$p = 5, \quad a = 3$ $\qquad \{1, 2, 3, 4\}$

$\{3, 6, 9, 12\}$

Basta verificare che $i \neq j \Rightarrow i \cdot a \not\equiv j \cdot a \ (p)$

Infatti

* $ia \not\equiv 0 \ (p)$, perché per ipotesi $p \nmid a$
  e $i = 1, \dots, p-1$, quindi $p \nmid i$

* se sono tutti diversi mod $p$, i loro rappr. privilegiati sono tutti diversi: ma questi sono $p-1$ numeri compresi tra $1$ e $p-1$, quindi sono (in un qualche ordine) $1, 2, \dots, p-1$

Verifichiamolo: $ia \equiv ja \pmod p$

$$\Rightarrow \quad i \equiv j \pmod p$$

$$\Rightarrow \quad i = j \quad (\text{perché entrambi } < p)$$

Allora

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

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

$$\Leftrightarrow \quad 1 \equiv a^{p-1} \mod p$$

Ex $(p-1)! \equiv -1 \pmod p$

E con $n$ generico? "Teorema di Eulero - Fermat"

Siano $a, n$ coprimi. Allora $a^{\varphi(n)} \equiv 1 \ (n)$.

Cos'è $\varphi(n)$?

$$\varphi(n) = \#\{1 \leq k \leq n \ \text{t.c.} \ (k, n) = 1\}$$

$\varphi(6)$? $\quad 1, \cancel{2}, \cancel{3}, \cancel{4}, 5, \cancel{6} \qquad \varphi(6) = 2$

$\varphi(p) = p - 1 \qquad (\Rightarrow$ piccolo t. Fermat$)$

$$\varphi(3^{100}) = \text{tutti} - \text{multipli di } 3$$
$$= \text{tutti} - 3^{99} = 3^{99} \cdot 2$$

$$\varphi(p^k) = p^k - \frac{1}{p} p^k = p^{k-1} \cdot (p-1)$$

Fatto Se $(m, n) = 1$, $\quad \varphi(m \cdot n) = \varphi(m)\varphi(n)$

$$\varphi(144) = \varphi(2^4 \cdot 3^2) = \varphi(2^4)\varphi(3^2)$$
$$= 2^3 \cdot 3 \cdot (3-1) = 3 \cdot 2^4$$

Es. $5^{48} \equiv 1 \pmod{144}$

Oss: se $(a, n) = 1$, $\quad \text{ord}_n(a) \mid \varphi(n)$

Ex $\quad x^{19} - y^{19} \equiv 0 \mod 31$

* 31 e' primo. Se $31 \mid x$, $31 \mid y$, quindi

$$x \equiv 0 \ (31) \iff y \equiv 0 \ (\text{mod } 31)$$

* Se $31 \nmid y$, esiste l'inverso di $y$ mod 31, chiamiamolo $z$. $\quad x^{19} z^{19} - y^{19} z^{19} \equiv 0 \ (31)$

$$\Rightarrow \quad (xz)^{19} - 1 \equiv 0 \quad (31)$$

$$\Rightarrow \quad \boxed{(xz)^{19} \equiv 1 \quad (\text{mod } 31)}$$

* $\text{ord}_{31}(xz) = \, ?$ $\quad \text{ord}_{31}(xz) \mid 19$

Eulero - Fermat $\Rightarrow$ $\text{ord}_{31}(xz) \mid \varphi(31) = 30$

$\text{ord}_{31}(xz) = 1$

* Quindi $(xz)^1 \equiv 1 \ (\text{mod } 31)$: moltiplico per $y$ e trovo $x \equiv y \ (\text{mod } 31)$

# Generatori

La stima del FLT è la migliore possibile?

Cioè: esiste un $a$ t.c. $\mathrm{ord}_p(a) = p-1$?

Risposta: <u>sì</u>, cioè per ogni $p$ esiste una classe di resto $g$ t.c. $\mathrm{ord}_p(g) = p-1$, e un tale elemento si chiama GENERATORE

$p = 7, \quad a = 3$

$$\underbrace{1,\ 3,\ 2,\ 6,\ 4,\ 5,}_{6 = p-1}\ 1, \dots$$

Tutte le classi di resto modulo $p$ si scrivono come una potenza di un generatore

Ex Esistono esattamente $\varphi(\varphi(p))$ generatori.

Un elemento $a = g^i$ che ordine ha?

$$a^x \equiv 1 \pmod p \iff g^{ix} \equiv 1 \pmod p$$

$$\iff (p-1) \mid ix$$

g generatore

$p = 7$, $g = 3$: se considero $3^2$, questo non ha speranze: $(3^2)^3 = 3^6 \equiv 1 \pmod 7$

Sia $d = (i, p-1)$

Allora $p-1 \mid ix \iff \frac{p-1}{d} \mid \frac{i}{d} \cdot x$

$\iff \frac{p-1}{d} \mid x$

Quindi $\mathrm{ord}_p(a) = \mathrm{ord}_p(g^i) = \frac{p-1}{(i, p-1)}$.

Se voglio che $a$ sia un generatore, e' nec. e suff. che $(i, p-1) = 1$. Quanti interi esistono coprimi con $p-1$ e minori di $p$? $\varphi(p-1) = \varphi(\varphi(p))$

## Esistenza di un generatore in generale

Esiste un generatore mod $n$, cioe' un $g$ con

$$\mathrm{ord}_n(g) = \varphi(n),$$

se e solo se $n = 2, 4, p^k$ o $2p^k$ con $p$ primo dispari

**Fatto** Se $g$ e' un generatore mod $p$, allora o $g$ o $g+p$ e' un generatore mod $p^k$ per ogni $k$

# Residui quadratici

Cioè: quand'è che $x^2 \equiv a \pmod p$ ha soluzioni?

* $a = 0$
* Se $y^2 \equiv z^2 \bmod p$, allora $(y-z)(y+z) \equiv 0 \ (p)$,

quindi $p \mid x-y$ oppure $p \mid x+y$

$$\begin{array}{ccc} p \mid x-y & & p \mid x+y \\ \Updownarrow & & \Updownarrow \\ x \equiv y \ (p) & & x \equiv -y \ (p) \end{array}$$

* In particolare,

$$1 \quad 2 \quad 3 \quad \cdots \quad \frac{p-1}{2} \quad \underbrace{\frac{p+1}{2} \quad \cdots \quad p-1}_{\frac{p-1}{2}}$$

quadrati

$$1^2 \quad 2^2 \quad 3^2 \cdots \left(\frac{p-1}{2}\right)^2 \quad \left(-\frac{p-1}{2}\right)^2 \quad \left(-\frac{p-3}{2}\right)^2 \cdots (-1)^2$$

$$1 \quad 2 \quad 3 \quad (-3) \quad (-2) \quad (-1)$$

$$1 \quad 4 \quad 9 \quad 9 \quad 4 \quad 1$$

**Morale:** ci sono

$$\underbrace{1}_{\text{lo zero}} + \underbrace{\frac{p-1}{2}}_{\text{residui non-zero}}$$

residui quadratici

## Quadrati vs generatore

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

quadrati

Residui quadratici = generatore elevato alla numero pari

Ma allora, cosa sono le potenze 19-esime mod 31? TUTTO!

Prendiamo una classe di resto mod 31,

$$a \equiv g^i \pmod{31}$$

Dico che posso scegliere $i \equiv 0 \pmod{19}$

Infatti posso sostituire $i$ con $i+30$,

ed in generale con qualunque esponente congruo ad $i$ mod 30.

Ma $\begin{cases} x \equiv i \pmod{30} \\ x \equiv 0 \pmod{19} \end{cases} \xRightarrow{\text{TCR}}$ ha soluzione

$\Rightarrow$ posso scegliere $i$ multiplo di 19.

Esercizi 32 p. 10, 33, 46, 48, 50

pag. 33 4, 7 e 10

Esistono 2013 interi consecutivi ognuno divisibile per una quinta potenza perfetta

$$\begin{cases} x \equiv 0 & (p_0^5) \\ x+1 \equiv 0 & (p_1^5) \\ x+2 \equiv 0 & \\ \vdots & \vdots \\ x+2012 \equiv 0 & (p_{2012}^5) \end{cases}$$

$p_0, p_1, \dots, p_{2012}$ primi tutti distinti

$\overset{TCR}{\Longrightarrow}$ esiste una soluzione (unica modulo $(p_0 \cdots p_{2012})^5$ )

Per ogni $p$ primo, esistono infiniti $n$ per cui $p \mid 2^n - n$

* Può succedere che $p \mid n$? Allora $p \mid 2^n$, e $p=2$ (posso prendere $n$ pari)

* $2^n \equiv n \pmod p$

"periodico di periodo $p$"

periodico, di un periodo che divide $p-1$

Se sostituisco $n$ con $n + Kp(p-1)$ che succede?

$$2^{n+Kp(p-1)} \equiv 2^n \cdot (\underbrace{2^{p-1}}_{1 \text{ FLT}})^{Kp} \equiv 2^n \pmod p$$

$$n + Kp(p-1) \equiv n \pmod p$$

* Basta trovare una soluzione

* Sappiamo che $2^n$ può fare 1.
Succede (perlomeno) se $n = h(p-1)$

Il membro destro è $\equiv 1$ se (sorpresa) $n \equiv 1 \ (p)$

Funzionano gli $n$ con $\begin{cases} n \equiv 0 & (p-1) \\ n \equiv 1 & (p) \end{cases}$

Uno esplicito è dato da $(1-p) + p(p-1)$

$= (p-1)^2$

Ultime 5 cifre di $5^{5^{5^{5^5}}} = x$

Voglio $x \mod 10^5$

$$\Leftrightarrow \begin{cases} x \equiv 0 \mod 5^5 \\ x \mod 2^5 \end{cases}$$

Cosa sappiamo? $5^{\varphi(32)} \equiv 1 \pmod{32}$

$$5^{\text{mostro}} \mod 32 \equiv 5^{(\text{mostro} \mod \varphi(32))} \ (32)$$

$\varphi(32) = 16$ : voglio $5^{5^{5^5}} \mod 16$

voglio $5^{5^5} \mod 8$

Siccome $5^5 \equiv 1 \pmod 4$, $5^{5^5} \equiv 5^1 \pmod 8$,

da cui $5^{5^{5^5}} \equiv 5^5 \pmod{16}$

$\equiv 5 \pmod{16}$

Oss: $x$ dispari $\Rightarrow x^2 \equiv 1 \pmod 8$

$\Rightarrow x^2 = 8k+1 \Rightarrow x^4 = 1 + 16k + 64k^2$

e $\equiv 1 \pmod{16}$

$$\begin{cases} x \equiv 5^5 \mod 32 \\ x \equiv 5^5 \mod (5^5) \end{cases} \Rightarrow x \equiv \overset{\overset{03125}{\shortparallel}}{5^5} \pmod{10^5}$$

$D = \{ n \text{ t.c. } n \mid 2^n + 1 \}$

PIÙ PICCOLO PRIMO (ppp)

Sia $p$ il ppp di $n$.

$$p \mid 2^n + 1 \iff 2^n \equiv -1 \pmod p$$

$$\Downarrow$$

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

$$\begin{cases} \text{ord}_p(2) \mid 2n \\ \text{ord}_p(2) \mid (p-1) \end{cases} \Rightarrow \text{ord}_p(2) \mid (p-1, 2n) = 2$$

Perché $(p-1, 2n) = 2$? Se $q \mid n$ e $q \mid p-1$, allora $q \leq p-1 < p = \text{ppp}(n)$ e quindi non esiste

$$\text{ord}_p(2) = \begin{cases} 1 \Rightarrow 2^1 \equiv 1 \pmod p \Rightarrow \text{assurdo} \\ 2 \Rightarrow 2^2 \equiv 1 \pmod p, \end{cases}$$

quindi $p = 3$.

b) $3^k \in D$? $\quad 3^k \mid 2^{3^k} + 1$

Per induzione su $k$. $k=1$ ok

Se è vero per $k$, $2^{3^k} + 1 = 3^k \cdot q$

Cosa fa $2^{3^{k+1}} + 1 = \left(2^{3^k}\right)^3 + 1$

$$= \left(3^k \cdot q - 1\right)^3 + 1 =$$

$$= 3^{3k} q^3 - 3 \cdot 3^{2k} \cdot q^2 + 3^{k+1} q$$

$$\equiv 0 \pmod{3^{k+1}}$$

$$3^{k+1} \parallel 2^{3^k} + 1$$

## Ancora residui d-esimi (mod p)

**Fatto:** ce ne sono esattamente

$$1 + \frac{p-1}{(p-1, d)}$$

Quali sono le classi di resto mod p?

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

Ci chiediamo se l'equazione $a \equiv x^d \ (p)$ (per a fissato) ha soluzione.

Scrivo $a = g^i$ e $x = g^y$: allora l'equazione diventa $g^i \equiv g^{yd} \mod p$

$\Longleftrightarrow (p-1) \mid yd - i \Longleftrightarrow yd \equiv i \ (p-1)$

$\Longleftrightarrow dy + (p-1)z = i$

Bézout

$\Longleftrightarrow$ ha soluzione se e solo se $(d, p-1) \mid i$

Quindi $a = x^i$ è residuo d-esimo $\Longleftrightarrow$ $(d, p-1) \mid i$. Quindi i residui d-esimi $\neq 0$ sono in corrispondenza con gli esponenti $i = 0, \dots, p-2$ divisibili per $(d, p-1)$, e quindi sono $\dfrac{p-1}{(d, p-1)}$

Esempio $y^2 = x^5 - 4$ non ha soluz mod 11.