Equazioni modulari

$$ax \equiv b \mod n$$

Sia $\langle a \rangle = \{ a^{(x)} : x > 0 \} = \{ ax \bmod n : x > 0 \}$

↓

sottogruppo di $\mathbb{Z}_n$ generato da a

L'equazione ha soluzione x se e solo se $b \in \langle a \rangle$ (multiplo di a)

Teorema $\forall\, a, n$ interi positivi, se $d = MCD(a, n)$, allora

$$\langle a \rangle = \langle d \rangle = \{ 0, d, 2d, \dots, (n/d - 1) \cdot d \}$$

e, quindi, $|\langle a \rangle| = n/d$

Conseguenze

Corollario Sia $d = MCD(a, n)$. $ax \equiv b \bmod n$ è risolubile se e solo se $d \mid b$

$\langle a \rangle = \langle d \rangle \Rightarrow$ risolubile $\iff b \in \langle d \rangle \iff d \mid b$

(b multiplo di d)

Corollario Sia $d = MCD(a, n)$. $ax \equiv b \bmod n$ ha d distinte soluzioni mod n oppure non ha soluzioni

Teorema Sia $d = MCD(a, n)$, $d = ax' + by'$, x', y' interi.
Se $d \mid b$, una delle sol. a $ax \equiv b \bmod n$ è

$$x_0 = x' \cdot \left(b/d\right) \bmod n$$

Teorema Sia x_0 soluzione per $ax \equiv b \bmod n$.

Allora l'equazione ha d soluzioni distinte

$$x_i = x_0 + i\,(n/d) \bmod n$$

per $i = 1, \dots, d-1$

Nota $ax \equiv b \bmod n$ $\iff$ $MCD(a,n) = 1$, una soluzione

$ax \equiv 1 \bmod n$ $\iff$ $MCD(a,n) = 1$, una soluzione

(Re-prova unicità inverso moltiplicativo in $\mathbb{Z}_n^*$)

Lemma Siano p, n tali che $p \mid n$. Allora, $\forall a \in \mathbb{Z}$,

$$(a \bmod n) \bmod p = a \bmod p$$

Lemma Siano $n_1, \dots, n_r$ interi positivi rel. primi e $N = n_1 \cdots n_r$. Per ogni x ed a interi

$x \equiv a \bmod n_i$ per $i = 1, \dots, r$

se e solo se

$x \equiv a \bmod N$

Stessa equazione, modulo diversi. E per sistemi di eqn. generici?

Teorema cinese del resto

Teorema. TCR Siano $n_1, \dots, n_2$ interi positivi rel. primi, $N = n_1 \cdots n_2$, $a_1, a_2, \dots a_2$ interi. Il sistema di 2 equazioni

$$x \equiv a_i \pmod{n_i}, \quad \text{per } i = 1, \dots, 2$$

ha un'unica soluzione modulo N.

Precisamente, per $i = 1, \dots, 2$, indicando con $N_i = N/n_i$ e $y_i = N_i^{-1} \bmod n_i$, risulta

$$x = \sum_{i=1}^{2} a_i \cdot N_i \cdot y_i \bmod N$$

Enunciati alternativi

Teorema. Siano $n_1, \dots n_2$ interi rel. primi, $N = n_1 \cdot \dots \cdot n_2$.

La corrispondenza

$$a \in \mathbb{Z}_N \longleftrightarrow (a_1, \dots, a_2) \in \mathbb{Z}_{n_1} \times \dots \times \mathbb{Z}_{n_2}$$

è biunivoca.

Implicazione. Le operazioni sugli elementi di $\mathbb{Z}_n$ possono essere eseguite equivalentemente sulle 2-ple

e.g. $(a+b) \bmod N \longleftrightarrow \left((a_1+b_1) \bmod n_1, \dots, (a_2+b_2) \bmod n_2\right)$

Enunciati alternativi

Una corrispondenza tra due gruppi $(A, \oplus_1)$ e $(B, \oplus_2)$ che preserva le operazioni si dice isomorfismo

(I gruppi hanno la "stessa forma")

I gruppi $(\mathbb{Z}_N, +_N)$ e $(\mathbb{Z}_{n_1} \times \dots \times \mathbb{Z}_{n_2}, +_{n_1 \dots n_2})$ sono isomorfi

coordinata per coordinata

$$a_i = a \bmod n_i \qquad a = \sum_{i=1}^{n} a_i N_i y_i \bmod N$$

$i = 1, \dots, n$

Identico discorso per $(\mathbb{Z}_N^*, *_N)$ e $(\mathbb{Z}_{n_1}^* \times \dots \times \mathbb{Z}_{n_2}^*, *_{n_1 \dots n_2})$

Uso del TCR

Calcolare $14 \cdot 13 \bmod 15$ in $\mathbb{Z}_{15}^*$

$n = 5 \cdot 3 \Rightarrow \mathbb{Z}_{15}^*$ isomorfo a $\mathbb{Z}_5^* \times \mathbb{Z}_3^*$

$14 \longleftrightarrow (4, 2)$ $\quad$ $13 \longleftrightarrow (3, 1)$

$(4, 2) \cdot (3, 1) = ([4 \cdot 3 \bmod 5], [2 \cdot 1 \bmod 3]) = (2, 2)$

$(2, 2) \longleftrightarrow 2 \Rightarrow 14 \cdot 13 \bmod 15 = 2 \bmod 15$

Uso del TCR

Calcolare $18^{25} \bmod 35$ in $\mathbb{Z}_{35}^*$

$n = 5 \cdot 7$ $\quad \mathbb{Z}_{35}^* \longleftrightarrow \mathbb{Z}_5^* \times \mathbb{Z}_7^*$

$18 \longleftrightarrow (3, 4) \Rightarrow 18^{25} \bmod 35 \leftrightarrow (3^{25} \bmod 5, 4^{25} \bmod 7)$

$\mathbb{Z}_5^*$ è un gruppo di ordine $\varphi(5) = 4$

$\mathbb{Z}_7^*$ è un gruppo di ordine $\varphi(7) = 6$

$3^{25} \bmod 5 = 3^{25 \bmod 4} \bmod 5 = 3^1 \bmod 5 = 3$

$4^{25} \bmod 7 = 4^{25 \bmod 6} \bmod 7 = 4^1 \bmod 7 = 4$

$(3, 4)$ ↕ 18

$18^{25} \bmod 35 = 18$ ←

Note

Useremo in futuro la corrispondenza per $n = p \cdot q$

(primi distinti dispari)

In generale $(G_1, \oplus_1)$ e $(G_2, \oplus_2)$ isomorfi

f isomorfismo, f^{-1} isomorfismo inverso

$g_1, g_2 \in G_1$

$h_1 = f(g_1)$, $h_2 = f(g_2)$

$h = h_1 \oplus_2 h_2$

$g = f^{-1}(h)$

(calcolo diretto)

$g = g_1 \oplus_1 g_2$

f, f^{-1} calcolo indiretto

calc. efficientemente

Proprietà generali di gruppi

Teorema G gruppo finito di ordine $n > 1$. Sia $e > 0$ intero

$$f_e : G \to G \quad \text{definita da} \quad f_e(g) = g^e$$

se $MCD(e, n) = 1$, f_e permutazione su G

Inoltre se $d = e^{-1} \bmod n$ allora

$$f_d : G \to G \quad , \quad f_d(g) = g^d$$

è la permutazione inversa.

Teorema Sia $(G, \oplus)$ un gruppo ciclico di ordine n e sia g un generatore di G. Allora

$$f : \mathbb{Z}_n \to G, \quad f(a) = g^a$$

è un isomorfismo tra $(\mathbb{Z}_n, +_n)$ e $(G, \oplus)$

Segue: tutti i gruppi ciclici dello stesso ordine sono isomorfi!

Nota: non è vero che sono la "stessa cosa" da un punto di vista computazionale! f potrebbe essere calcolabile in modo efficiente, mentre $f^{-1} : G \to \mathbb{Z}_n$ no

Proprietà del gruppo $\mathbb{Z}_n^*$

Teorema (di Eulero) $\forall\ n > 1$ e $\forall\ a \in \mathbb{Z}_n^*$

$$a^{\varphi(n)} \equiv 1 \bmod n$$

Teorema (di Fermat) $\forall$ primo p e $\forall\ a \in \mathbb{Z}_p^*$

$$a^{p-1} \equiv 1 \bmod p$$

Teorema (di Nisen e Zuckermann) $\mathbb{Z}_n^*$ è ciclico per i valori di n uguali a: 2, 4, p^e e $2p^e$ per tutti i primi dispari p ed interi positivi e

Teorema (del logaritmo discreto) Se g è un generatore di $\mathbb{Z}_n^*$

$$g^x \equiv g^y \bmod n \quad \text{se e solo se} \quad x \equiv y \bmod \varphi(n)$$

Teorema (radici quadrate dell'unità) Se p è un primo dispari ed $e \geq 1$ intero positivo, allora

$$x^2 \equiv 1 \bmod p^e$$

ha solo due soluzioni, $x = 1$ e $x = -1$

Corollario Se $\exists$ una radice quadrata non banale di $1 \bmod n$ allora n è composto

Generazione di numeri primi

$\pi(x)$ funzione di distribuzione dei primi — $\pi(10) = 4$

primi $\leq x$, per ogni valore reale di x — $\{2, 3, 5, 7\}$

Teorema dei numeri primi.

$$\lim_{x \to \infty} \frac{\pi(x)}{x / \ln x} = 1$$

... al crescere di x, $x / \ln x$ è una stima ragionevole per $\pi(x)$

(conosciamo approssimazioni migliori)

$\Rightarrow$ $1 / \ln n$ stima della prob. che n scelto a caso sia primo

" Dovremmo esaminare tutti interi vicini ad n per trovare un primo della lunghezza di n "

Sapendo distinguere primi da composti, possiamo generare numeri primi efficientemente

Prova di divisione: divido n per ogni intero più piccolo, i.e., 2, 3 --- fino a $\sqrt{n}$

($\sqrt{n} \cdot \sqrt{n} = n$ --- è sufficiente)

Quanto costa? Caso peggiore (n primo) $\sqrt{n}$ divisioni

Se B lunghezza di n in bit, $2^{B/2}$ divisioni

(costo $poly(B) \cdot 2^{B/2}$)

Idea: usare il teorema di Fermat

Se n è primo, $a^{n-1} \equiv 1 \bmod n$ $\forall a \in \mathbb{Z}_n^*$

Se trovo un a: $a^{n-1} \not\equiv 1 \bmod n$, n è composto (certamente)

↳ altrimenti, scommetto che sia primo (potrebbe --)

Test funziona abbastanza bene, errori di un tipo (composti scambiati per primi)

Problema: numeri di Carmichael. Superano il test $\forall a \in \mathbb{Z}_n^*$ ma sono composti

Usiamo anche un secondo risultato

Se n è primo $x^2 \equiv 1 \bmod n$ ha solo radici banali

$\Rightarrow$ una radice non banale, n composto

Test di Miller e Rabin

Scegli più valori di a uniformi a caso e verifica che

$$a^{n-1} \equiv 1 \bmod n$$

Mentre calcola a^{n-1} controlla che non abbia generato radici non banali dell'unità.

Calcolo dell'esponenziazione modulare

$a^b \bmod n$

$a \cdot a \cdot a \cdots a \bmod n$ inefficiente

(b volte)

(# moltiplicazioni esp. nella lunghezza di b)

```
Modular_exp (a, b, n)
    c ← 0                          (al termine c contiene il valore di b)
    d ← 1                          (  "    "  contiene il valore a^b mod n)
    sia <b_k ... b_0> la rappr. binaria di b
    for i = k to 0
        c ← 2c
        d ← d·d mod n              ← quadrato
        if b_i = 1
            then c ← c+1
                 d ← d·a mod n     ← molt. per a
    return d
```

costo

moltiplicazioni proporzionale alla lunghezza di b

Test di Miller e Rabin

Random $(1, n-1)$ restituisce $1 < a < n-1$ uniforme

Witness (a, n) restituisce TRUE se a è "un testimone della compostezza di n"

```
Miller_Rabin (n, s)
    for j = 1 to s
        a ← Random (1, n-1)
        if Witness (a, n) = TRUE
            then return "composto"
    return "primo"
```

Witness (a, n) semplice modifica di Modular-exp (a, b, n)

Modular-exp (a, b, n)

$c \leftarrow 0$

$d \leftarrow 1$

sia $\langle b_k \dots b_0 \rangle$ la rappr. di b

for $i = k$ to 0

$c \leftarrow 2c$ → quadrato

$d \leftarrow d \cdot d \bmod n$

if $b_i = 1$

then $c \leftarrow c + 1$

$d \leftarrow d \cdot a \bmod n$ → molt. per a

return d

Witness (a, n)

$d \leftarrow 1$

sia $\langle b_k \dots b_0 \rangle$ la rappr. di $n - 1$

for $i = k$ to 0

$x \leftarrow d$

$d \leftarrow d \cdot d \bmod n$

Radice Quadrata:

if $d = 1$ e $x \neq 1$ e $x \neq n - 1$

then return TRUE

if $b_i = 1$

then $d \leftarrow d \cdot a \bmod n$

Fermat:

if $d \neq 1$

then return TRUE

return FALSE

La procedura di Miller e Rabin è una ricerca probabilistica parametrizzata di una prova di compostezza di n

Sceglie s valori casuali a

- se una di queste scelte produce un testimone, allora restituisce "composto"
- se nessun testimone viene trovato, assume che non ve esistano e restituisce "primo"

Come scegliere s?

Teorema. (Testimoni) Se n è un intero dispari composto, allora il numero di testimoni della sua compostezza è almeno $(n-1)/2$

(più della metà sono testimoni)

Teorema. Per ogni intero dispari $n > 2$ ed ogni intero positivo s, la probabilità che il test di Miller e Rabin sbagli è al più 2^{-s}

Dim. Teorema testimoni, sbaglia con prob $\leq 1/2$ ogni it.
In s iterazioni indipendenti, $\leq \left(\frac{1}{2}\right)^s = \frac{1}{2^s} = 2^{-s}$.

Idea della prova.

Si dimostra che i NON testimoni sono al più $(n-1)/2$

Qualsiasi NON testimone a deve appartenere a $\mathbb{Z}_n^*$

perché $a^{n-1} \equiv 1 \bmod n$

Pertanto, tutti gli $a \in \mathbb{Z}_n - \mathbb{Z}_n^*$ sono testimoni della compostezza.

Possiamo far vedere che i NON testimoni sono contenuti in un sottogruppo proprio $B \subset \mathbb{Z}_n^*$

Poiché $|\mathbb{Z}_n^*| \leq n-1$, risulta $|B| \leq \frac{(n-1)}{2}$

→ Richiede analisi di due casi. Il secondo è più complesso.

Gruppi ciclici di ordine primo

Sia p primo. $\mathbb{Z}_p^*$ è un gruppo ciclico ed ha ordine $\varphi(p) = p-1$

Sia α un generatore di $\mathbb{Z}_p^*$. Ogni β può essere scritto come $\beta = \alpha^i$ per qualche $0 \le i \le p-2$

Lemma. L'ordine di $\beta = \alpha^i$ è $\text{ord}(\beta) = \dfrac{(p-1)}{MCD(p-1, i)}$.

Osservazioni: se $MCD(p-1, i) = 1$, β è un generatore esso stesso.

Il numero di generatori di $\mathbb{Z}_p^*$ è $\varphi(p-1)$

Se il gruppo G ha ordine q primo, tutti gli elementi (eccetto l'unità) sono generatori

Come scegliere un generatore di $\mathbb{Z}_p^*$?

Teorema. Sia p primo e sia $a \in \mathbb{Z}_p^*$. Allora a è un generatore se e solo se

$$a^{(p-1)/q} \neq 1 \bmod p$$

per tutti i primi q tali che $q \mid (p-1)$

Osservazione: occorre conoscere la fattorizzazione di $(p-1)$.

e poi cercare un a opportuno

(Ma potremmo procedere all'inverso, scegliendo i fattori e costruendo p ...)

Come posso costruire un gruppo di ordine primo?

Teorema Sia $p = 2q + 1$, con p e q primi. Allora

$$G \stackrel{def}{=} \{ h^2 \bmod p \mid h \in \mathbb{Z}_p^* \}$$

è un sottogruppo di $\mathbb{Z}_p^*$ di ordine q.

Nota Se $2 = 2$ (i.e., $p = 2q + 1$) G contiene i quadrati di tutti gli elementi di $\mathbb{Z}_p^*$, che chiameremo residui quadratici

$q \longrightarrow$ primi di Sophie-Germain

$p \longrightarrow$ primi sicuri (safe primes)

Esempio

$(\mathbb{Z}_{11}^*, \cdot_{11})$ 11 è un primo. $\varphi(11) = 10$

potenze di 2

2^0	2^1	2^2	2^3	2^4	2^5	2^6	2^7	2^8	2^9
1	2	4	8	5	10	9	7	3	6

Pertanto 2 è un generatore

potenze di 3

3^0	3^1	3^2	3^3	3^4	3^5	3^6	3^7	3^8	3^9
1	3	9	5	4	1	3	9	5	4

Quindi 3 non genera $\mathbb{Z}_{11}^*$. Genera $H = \{1, 3, 9, 5, 4\}$ (ordine 5)

potenze di 10

10^0	10^1	10^2	10^3	10^4	10^5	10^6	10^7	10^8	10^9
1	10	1	10	1	10	1	10	1	10

Genera $H = \{1, 10\}$ (ordine 2)

Ora, notate che $11 = 2 \cdot 5 + 1$

$p = 2q + 1$

1^2	2^2	3^2	4^2	5^2	6^2	7^2	8^2	9^2	10^2
1	4	9	5	3	1	4	9	5	3

I quadrati di tutti gli elementi danno un sottogruppo di ordine 5.

Ma $11 = 5 \cdot 2 + 1$

1^5	2^5	3^5	4^5	5^5	6^5	7^5	8^5	9^5	10^5
1	10	1	10	1	10	1	10	1	10

Le potenze quinte di tutti gli elementi danno un sottogruppo di ordine 2

Il teorema precedente offre

- un metodo per scegliere unif. a caso un elemento di G
- un metodo per verificare se $a \in \mathbb{Z}_p^*$ appartiene anche a G

1. Generazione. Si sceglie unif. a caso $h \in \mathbb{Z}_p^*$ e si calcola $h^2 \bmod p$. (Ogni elemento di G è un generatore)

2. Verifica. Si controlla che $h^q \equiv 1 \bmod p$

Perché? Sia g gen di $\mathbb{Z}_p^*$, $h = g^i$

$$h^q \equiv 1 \bmod p \iff (g^i)^q \equiv 1 \bmod p \iff$$

$$iq \equiv 0 \bmod (p-1) \iff iq \equiv 0 \bmod 2q$$

$$\iff iq = K \cdot 2q \iff 2q \mid iq \iff 2 \mid i$$

$$h = g^i = g^{c2} = (g^c)^2$$