Contiene la lezione di martedì 30 aprile

(Scaricatelo e portatelo in aula F8)

L'argomento della lezione è "Generazione di numeri pseudo-casuali con il metodo delle congruenze lineari"

(Lehmer, 1949)

①

6. IL METODO DELLE CONGRUENZE LINEARI PER GENERARE SEQUENZE DI NUMERI CASUALI (Lehmer, 1949)

I generatori di numeri casuali più frequentemente utilizzati non sono altro che delle varianti dello schema seguente, introdotto da D. H. Lehmer nel 1949.

Scegliamo quattro numeri magici:

- m, il modulo con $0 < m$
- a, il moltiplicatore con $0 \le a < m$
- c, l'incremento con $0 \le c < m$
- x_0, il valore iniziale con $0 \le x_0 < m$

Indichiamo poi con A il sistema completo di resti modulo m, cioè $A = \{[0],[1],[2],\ldots,[m-1]\}$ e definiamo l'applicazione

$f : A \to A$

$$x \mapsto f(x) \equiv ax + c(\operatorname{mod} m)$$

Consideriamo poi la successione di elementi di A definita iterativamente come segue, cioè

$$\begin{cases} x_0 = x_0 \\ x_{n+1} = f(x_n) \equiv ax_n + c(\operatorname{mod} m) \end{cases} \qquad x_0 \in A \qquad \textbf{0)}$$

Questa sequenza è detta "sequenza delle congruenze lineari". Per esempio, se prendiamo $m = 10, x_o = a = c = 7$ otteniamo la sequenza 7, 6, 9, 0, 7, 6, 9, 0, ... , che ha periodo 4.

Vedremo in seguito i principi che si devono seguire per scegliere appropriatamente i numeri. In particolare l'esempio sopra descritto mostra che la sequenza ha un loop, cioè c'è un ciclo di numeri che viene ripetuto all'infinito. Come risulta dal Lemma seguente, se $f : A \to A$ e A è un insieme finito, questa proprietà è comune a tutte le sequenze aventi la forma generale $x_{n+1} = f(x_n)$.

<u>**Lemma**</u>

Sia A un insieme finito e sia $f : A \to A$

2

La successione ricorsiva

$$\begin{cases} x_0 = x_0 \\ x_{n+1} = f(x_n) \end{cases} \qquad x_0 \in A \qquad\qquad 1)$$

è ciclica, con eventuale antiperiodo.

Dimostrazione

Per dimostrare questo fatto chiamiamo h il minimo intero ≥ 1 tale che esiste un j con $0 \leq j \leq h-1$ per cui

$$x_h = f(x_{h-1}) = x_j \qquad\qquad 2)$$

Tale h esiste certamente perché la catena

x_0

$x_1 \neq x_0$

$x_2 \neq x_0, x_1$

$x_3 \neq x_0, x_1, x_2$

...

$x_h \neq x_o, x_1, \ldots x_{h-1}$

termina dopo al più $|A|$ passi (con $|A|$ indico il numeri di elementi di A). Da questo punto in poi i valori si ripetono, cioè

$x_{h+1} = f(x_h) = f(x_j) = x_{j+1}$

$x_{h+2} = f(x_{h+1}) = f(x_{j+1}) = x_{j+2}$

...

$x_{h+r} = f(x_{h+r-1}) = f(x_{j+r-1}) = x_{j+r}$

...

Dunque il periodo è $T = h - j$ e $r \equiv s (\mathrm{mod}\, T) \Rightarrow x_r = x_s$.

(Se $h = 1$ si ha $j = 0$, cioè $x_1 = x_0$, $T = 1$ e la successione è costante). □

Chiaramente dato che si cerca un algoritmo per la generazione di numeri casuali, si desidera una sequenza con un periodo relativamente lungo.

Il caso speciale $c = 0$ merita una menzione specifica in quanto la generazione dei numeri è leggermente più rapida quando $c = 0$ rispetto a quando $c \neq 0$. Vedremo in seguito che la

(3)

restrizione $c=0$ riduce la lunghezza del periodo della sequenza, anche se è sempre possibile rendere questo periodo ragionevolmente lungo. Il lavoro originario di Lehmer prevedeva un metodo di generazione con $c=0$, anche se egli stesso menzionava $c \neq 0$ come una possibilità. L'idea di scegliere $c \neq 0$ per ottenere cicli di lunghezza più lunga è dovuta a Thomson e, indipendentemente, a Rotenberg.
I termini *metodo delle congruenze moltiplicativo* e *metodo delle congruenze misto* sono usati da molti autori per indicare il metodo delle congruenze lineari rispettivamente con $c=0$ e con $c \neq 0$.

Le lettere m, a, c e x_0 sono usate in questo capitolo nel senso descritto sopra.

Vogliamo ora dimostrare che per la sequenza x_n definita ricorsivamente dalla **0)** si può facilmente trovare un'espressione esplicita. Dimostriamo che

$$x_n \equiv a^n x_0 + c(a^0 + a^1 + a^2 + \ldots + a^{n-1}) (\operatorname{mod} m) \quad \forall n \geq 1. \qquad \textbf{3)}$$

Ragioniamo per induzione.

Per n=1 la **3)**è vera in quanto diviene $x_1 \equiv a x_0 + c (\operatorname{mod} m)$ che coincide con la **0)** per $n=0$, cioè $x_1 = f(x_0) \equiv a x_0 + c (\operatorname{mod} m)$, per la definizione **0)**.

Supponiamo ora vera la 3) per n=k e dimostriamo che allora vale anche per k+1. Si ha infatti

$$\begin{aligned} x_{k+1} &= f(x_k) \equiv \\ &\equiv a x_k + c \equiv \qquad \textbf{4)} \\ &\equiv a\left[a^k x_0 + c(1 + a + \ldots + a^{k-1})\right] + c \equiv \\ &\equiv a^{k+1} x_0 + c(1 + a + a^2 + \ldots + a^k) (\operatorname{mod} m) \end{aligned}$$

che è la **3)** con n=k+1. Ciò prova la **3)** $\forall n \geq 1$. □

Una generalizzazione di **3)** è

$$x_{n+k} \equiv a^k x_n + \frac{a^k - 1}{a - 1} c \ (\operatorname{mod} n) \quad \text{con } k \geq 0 \text{ e } n \geq 0$$

che esprime l'$n+k$-esimo termine direttamente in funzione dell'n-esimo termine (il caso speciale $n=0$ in questa equazione è quello dimostrato sopra).

(4)

Un **caso particolarmente importante** è il caso $x_0 = 0$ e $c = 1$. La **3)** diviene

$$x_n = a^0 + a^1 + a^2 + \ldots + a^{n-1} \pmod{m} \quad , \; n \geq 1 \qquad \mathbf{5)}$$

Successioni da scartare

Osserviamo che le scelte $a = 0$ e $a = 1$ sono, ovviamente, da scartare. Infatti la prima porta alla successione costante $x_n = c$, $\forall n \geq 1$, e la seconda a $x_n = x_0 + nc$, $\forall n \geq 1$, che non sono sequenze casuali. Per questi motivi supporremo $a \geq 2$.

5

6.1. Scelta del modulo m e del moltiplicatore a nel caso $x_0 = 0$ e $c = 1$.

Esaminiamo ora il problema della scelta del modulo m e del moltiplicatore a a esso collegato. Per semplificare la trattazione sceglieremo sempre $x_0 = 0$ e $c = 1$. In tal modo

$x_n \equiv 1 + a + a^2 + \ldots + a^{n-1} \pmod{m}$

6.1.1. I CASO: $m = p$ primo dispari, cioè $p > 2$.

Dato che, come abbiamo detto, $x_0 = 0$ e $c = 1$, la sequenza da considerare è la **5)**, cioè

$$x_n \equiv a^0 + a^1 + a^2 + \ldots + a^{n-1} = \sum_{k=1}^{n} a^{k-1} \pmod{p}, \quad n \geq 1 \qquad \textbf{6)}$$

Dalla **6)** segue moltiplicando membro a membro per a, che

$$a x_n \equiv a^1 + a^2 + \ldots + a^n \pmod{p} \qquad \textbf{7)}$$

E sottraendo **6)** da **7)** si ha

$$(a-1)x_n \equiv a^n - 1 \pmod{p} \qquad \textbf{8)}$$

Dato che $1 < a < p$ il coefficiente $(a-1)$ è invertibile $\bmod p$ e dalla **8)** segue

$$x_n \equiv (a^n - 1)(a-1)^{-1} \pmod{p}, \ \forall n \geq 1. \qquad \textbf{9)}$$

Osserviamo che

$$\begin{aligned} x_n \equiv x_m \pmod{p} \quad &\Leftrightarrow \quad (a^n - 1)(a-1)^{-1} \equiv (a^m - 1)(a-1)^{-1} \pmod{p} \quad \Leftrightarrow \\ &\Leftrightarrow \quad a^n \equiv a^m \pmod{p} \quad \Leftrightarrow \qquad \textbf{10)} \\ &\Leftrightarrow \quad n \equiv m \pmod{o_p(a)} \end{aligned}$$

dove con $o_p(a)$ abbiamo indicato l'ordine di $a \bmod p$.

Quindi la sequenza definita da **9)** per $n \geq 0$ è periodica $\bmod(o_p(a))$ e i cicli di lunghezza massima si otterranno con le radici primitive.

Siccome $o_p(a) \leq p-1 \ \forall a$, la **9)** non rappresenta per $n = 1,2,\ldots,o_p(a)$ l'intero sistema completo di resti $\bmod p$, cioè $0,1,2,\ldots,p-1$, neanche se a è una radice primitiva (in questo caso c'è sempre una sola eccezione). Infatti se $1 \leq b \leq p-1$ si ha

$$x_n \equiv (a^n - 1)(a-1)^{-1} \equiv b \pmod{p} \quad \Leftrightarrow \quad a^n \equiv b(a-1) + 1 \pmod{p} \qquad \textbf{11)}$$

e quest'ultima congruenza, se a è radice primitiva, ha sempre una sola soluzione, a meno che non sia $\quad b(a-1)+1 \equiv 0 (\bmod p) \quad \Leftrightarrow \quad b \equiv -(a-1)^{-1} (\bmod p)$ **12)**

Dunque l'elemento $-(a-1)^{-1}$ è l'unica eccezione, cioè è l'unico non rappresentabile nella sequenza x_n data dalla **9)**.

Osserviamo che se il primo p ha 2 come radice primitiva e si sceglie a=2, la **9)** diviene

$x_n \equiv 2^n - 1 (\bmod p)$ **13)**

e l'unico elemento del sistema completo di resti $\bmod p$ non rappresentato è $-1 \equiv p-1 (\bmod p)$.

6.1.1.1. Esempi numerici

Prendiamo il modulo $m = p$ primo con $p = 11$. Cerchiamo una radice primitiva modulo 11: proviamo con 2. Dato che gli ordini dividono $\varphi(11) = 10 = 2 \cdot 5$, e $2^5 \equiv -1 (\bmod 11)$, evidentemente 2 è radice primitiva modulo 11.

Se consideriamo ora la sequenza $\begin{cases} x_0 = 0 \\ x_{n+1} \equiv 2x_n + 1 \ (\bmod 11) \end{cases}$, in base a quanto visto in teoria, questa sequenza deve essere periodica di periodo 10 e deve rappresentare il sistema completo di resti modulo 11 con la sola eccezione di $x^* \equiv -(2-1)^{-1} \ (\bmod p)$ cioè $x^* \equiv -1 \ (\bmod 11)$.

Verifichiamolo:

$x_0 = 0$

$x_1 \equiv 2x_0 + 1 \equiv 2 \cdot 0 + 1 \equiv 1 \ (\bmod 11)$

$x_2 \equiv 2x_1 + 1 \equiv 2 \cdot 1 + 1 \equiv 3 \ (\bmod 11)$

$x_3 \equiv 2x_2 + 1 \equiv 2 \cdot 1 + 1 \equiv 7 \ (\bmod 11)$

$x_4 \equiv 2x_3 + 1 \equiv 2 \cdot 7 + 1 \equiv 4 \ (\bmod 11)$

$x_5 \equiv 2x_4 + 1 \equiv 2 \cdot 4 + 1 \equiv 9 \ (\bmod 11)$

$x_6 \equiv 2x_5 + 1 \equiv 2 \cdot 9 + 1 \equiv 8 \ (\bmod 11)$

$x_7 \equiv 2x_6 + 1 \equiv 2 \cdot 8 + 1 \equiv 6 \ (\bmod 11)$

$x_8 \equiv 2x_7 + 1 \equiv 2 \cdot 6 + 1 \equiv 2 \ (\bmod 11)$

7

$x_9 \equiv 2x_8 + 1 \equiv 2 \cdot 2 + 1 \equiv 5 \pmod{11}$

$x_{10} \equiv 2x_9 + 1 \equiv 2 \cdot 5 + 1 \equiv 11 \equiv 0 \pmod{11}$

Come si può notare la sequenza è periodica di periodo 10 e l'unico elemento del sistema completo di resto modulo 11, cioè, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10 non rappresentato è 10 (in accordo con la teoria). (0)

Presentiamo ora un altro esempio numerico.

Prendiamo sempre $m = p = 11$. Dato che $8 = 2^3$ e $(3, \varphi(11)) = (3,10) = 1$, anche 8 è radice primitiva modulo 11. Ora la sequenza è $\begin{cases} x_0 = 0 \\ x_{n+1} \equiv 8x_n + 1 \pmod{11} \end{cases}$

In base a quanto visto prima in teoria, la successione deve essere ancora periodica di periodo 10 e deve rappresentare il sistema completo di resti modulo 11, con la sola eccezione di $x^* \equiv -(8-1)^{-1} \equiv -7^{-1} \pmod{11}$. Dobbiamo allora calcolare l'inverso moltiplicativo di 7 modulo 11, cioè dobbiamo risolvere la congruenza $7x \equiv 1 \pmod{11}$.

Applicando l'algoritmo euclideo si ha:

$1 = MCD(11,7)$ e, in particolare, $-3 \cdot 7 + 2 \cdot 11 = 1$ per cui $-3 \cdot 7 \equiv -21 \equiv 1 \pmod{11}$ cioè -3 è l'inverso moltiplicativo di 7 modulo 11.

Quindi l'unico elemento del sistema completo di resti non rappresentato sarà $x^* \equiv -7^{-1} \equiv -(-3) = 3 \pmod{11}$.

Verifichiamolo:

$x_0 = 0$

$x_1 \equiv 8x_0 + 1 \equiv 1 \pmod{11}$

$x_2 \equiv 8x_1 + 1 \equiv 9 \pmod{11}$

$x_3 \equiv 8x_2 + 1 \equiv 7 \pmod{11}$

$x_4 \equiv 8x_3 + 1 \equiv 2 \pmod{11}$

$x_5 \equiv 8x_4 + 1 \equiv 6 \pmod{11}$

$x_6 \equiv 8x_5 + 1 \equiv 5 \pmod{11}$

$x_7 \equiv 8x_4 + 1 \equiv 8 \pmod{11}$

$x_8 \equiv 8x_7 + 1 \equiv 10 \pmod{11}$

$x_9 \equiv 8x_8 + 1 \equiv 4 \pmod{11}$

$x_{10} \equiv 8x_9 + 1 \equiv 0 \pmod{11}$

Come si può vedere, la sequenza è periodica di periodo 10 e l'unico elemento del sistema completo di resti modulo 11 che non è rappresentato è proprio il 3, in accordo con la teoria.

—

II° Caso, $m = p^k$

(con p primo dispari e $k \geq 2$)

In questo secondo caso ci sono tre possibili sottocasi, in funzione della scelta di a.

Sottocaso 1 : $1 < a < p^k$, $(a, p) = 1$, $a \not\equiv 1 \pmod{p}$

La sequenza ricorsiva definita dalla formula 0) di pag 1. (con $x_0 = 0$ e $c = 1$), ha un ciclo di lunghezza $\sigma_{p^k}(a)$ (con $\sigma_{p^k}(a)$ indichiamo l'ordine di a mod p^k). Dato che $\sigma_p(a) \mid \varphi(p^k) = p^{k-1}(p-1)$ i cicli di lunghezza massima si ottengono con a radice primitiva mod p^k.
Inoltre la sequenza $x_0 = 0, x_1, x_2, \ldots, x_{\varphi(p^k)-1}$

rappresenta il sistema completo di resti mod p^k, cioè $0, 1, 2, \ldots, p^k-1$, con p^{k-1} eccezioni. I numeri non rappresentati sono gli x^* con

$$14) \quad x^* \equiv -(a-1)^{-1} \pmod p$$

<u>Sottocaso 2</u> : $1 < a < p^k$, $(a, p^k) = p^\beta \geq p$.

Questa scelta è da evitare, infatti la sequenza definita da 0) di pag 1 (con $x_0 = 0$ e $c = 1$) è, in questo caso, definitivamente costante.

<u>Sottocaso 3</u> : $1 < a < p^k$, $a \equiv 1 \pmod p$.

Questo è effettivamente il caso più importante ed interessante, infatti la sequenza ricorsiva definita dalla solita formula 0) di pag 1 (con $x_0 = 0$ e $c = 1$), prima di diventare periodica descrive un <u>intero sistema completo di resti mod p^k</u>, <u>senza alcuna eccezione</u>.

Non dimostreremo nessuno di questi risultati (la dimostrazione è piuttosto lunga e complicata), ci limiteremo a presentare, nelle prossime pagine, qualche semplice esempio illustrativo.

Esempi illustrativi

Sottocaso 1:

Scegliamo $m = 3^2$ ed $a = 5$.
Consideriamo la sequenza

$$15) \begin{cases} x_0 = 0 \\ x_{n+1} \equiv 5x_n + 1 \pmod 9 \end{cases}$$

Otteniamo i numeri

$$16) \begin{aligned} x_0 &= 0 \\ x_1 &\equiv 5 \cdot 0 + 1 = 1 \\ x_2 &\equiv 5 \cdot 1 + 1 = 6 \\ x_3 &\equiv 5 \cdot 6 + 1 = 31 \equiv 4 \pmod 9 \\ x_4 &\equiv 5 \cdot 4 + 1 \equiv 21 \equiv 3 \pmod 9 \\ x_5 &= 5 \cdot 3 + 1 = 16 \equiv 7 \pmod 9 \\ x_6 &= 5 \cdot 7 + 1 = 36 \equiv 0 \pmod 9 \end{aligned}$$

Osserviamo che 5 è radice primitiva mod 9, infatti

$$17) \begin{cases} 5^1 \equiv 5 \ (9) \\ 5^2 \equiv 25 \equiv 7 \ (9) \\ 5^3 \equiv 35 \equiv -1 \equiv 8 \pmod 9 \\ 5^4 \equiv -5 \equiv 4 \pmod 9 \\ 5^5 \equiv 20 \equiv 2 \pmod 9 \\ 5^6 \equiv 10 \equiv 1 \pmod 9 \end{cases}$$

(le potenze $5^k \pmod 9$ rappresentano il sistema ridotto di resti mod 9 (con $k = 1, 2, \dots, 6 = \varphi(9)$))

Quindi, con $a=5$, la sequenza ricorsiva definita da 15), ha periodo massimo, pari a $\varphi(p^k)=\varphi(3^2)=6$ (Questo è confermato dalla 16)). La teoria ci dice inoltre che la 15) rappresenta il sistema completo di resti mod p^k (per noi mod $3^2=9$) con p^{k-1} (per noi $3^{2-1}=3$) eccezioni, rappresentate dai numeri $x^* \equiv -(a-1)^{-1} \pmod p$, per noi

$$18) \quad x^* \equiv -(5-1)^{-1} \equiv -4^{-1} \pmod 3$$

Dato che $4 \equiv 1 \pmod 3$ si ha $x^* \equiv -1 \equiv 2 \pmod 3$ e quindi gli elementi non rappresentati sono

$$19) \quad x^* = 2,\ 2+3,\ 2+2.3 = 2, 5, 8$$

La formula 16) è in perfetto accordo con la 19), come previsto dalla teoria.

<u>Sottocaso 2</u>

Scegliamo ancora $m=3^2$, mentre $a=3$.

La sequenza

$$20) \begin{cases} x_0 = 0 \\ x_{n+1} = 3x_n + 1 \pmod 9 \end{cases}$$

è la seguente:

$$21) \begin{cases} x_0 = 0 \\ x_1 = 1 \\ x_2 = 3.1+1 \equiv 4 \\ x_3 = 3.4+1 = 13 \equiv 4 \pmod 9 \end{cases}$$

(da questo punto in poi la sequenza è costante)

Ancora 20) e 21) sono in accordo con la teoria.

Sottocaso 3

Scegliamo ancora $m = 3^2$, ma $a = 4$ (osservate che $a \equiv 1 \pmod p$, per noi $4 \equiv 1 \pmod 3$).

La sequenza

$$22) \quad \begin{cases} x_0 = 0 \\ x_{n+1} \equiv 4 x_n + 1 \pmod 9 \end{cases}$$

è la seguente

$$23) \quad \begin{aligned} x_0 &= 0 \\ x_1 &= 1 \\ x_2 &= 4 \cdot 1 + 1 = 5 \\ x_3 &= 4 \cdot 5 + 1 = 21 \equiv 3 \pmod 9 \\ x_4 &= 4 \cdot 3 + 1 = 13 \equiv 4 \pmod 9 \\ x_5 &= 4 \cdot 4 + 1 = 17 \equiv 8 \pmod 9 \\ x_6 &= 4 \cdot 8 + 1 = 33 \equiv 6 \pmod 9 \\ x_7 &= 4 \cdot 6 + 1 = 25 \equiv 7 \pmod 9 \\ x_8 &= 4 \cdot 7 + 1 = 29 \equiv 2 \pmod 9 \\ x_9 &= 4 \cdot 2 + 1 \equiv 9 \equiv 0 \pmod 9 \end{aligned}$$

e, come previsto dalla teoria, rappresenta un sistema completo di resti mod 9, senza alcuna eccezione.

Il teorema generale

Si può dimostrare il seguente

Teorema 1 (Lehmer)

Il generatore di numeri pseudo-casuali definito da

$$24) \quad \begin{cases} x_0 = x_0 \\ x_{n+1} = (a x_n + b) \pmod m \end{cases}$$

ha periodo m se e solo se

i) $(b, m) = 1$

ii) $p \mid (a-1)$ per ogni primo $p \mid m$

iii) $4 \mid (a-1)$ se $4 \mid m$

—

Osservazione

Noi abbiamo sempre considerato $b=1$ (e quindi la condizione i) è automaticamente verificata). Inoltre la condizione ii) ci dice che, dato il modulo $m = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$, la scelta ottimale del moltiplicatore a si ottiene mediante il teorema cinese del resto, risolvendo il sistema

$$25) \quad \begin{cases} a \equiv 1 \pmod{p_1} \\ \text{———} \\ a \equiv 1 \pmod{p_k} \end{cases} \qquad \left(p_j \text{ primi}, \ p_j \mid m \right) \quad \text{se } 4 \mid m$$

Esempi illustrativi

Scegliamo $m = 3^2 \cdot 5^2 = 225$ e $a = 16 = 3 \cdot 5 + 1$. In questo caso si ha $a \equiv 1 \pmod 3$ e $a \equiv 1 \pmod 5$, come richiesto dalla ii): quindi il precedente teorema ci dice che la sequenza ricorsiva

$$26) \begin{cases} x_0 = 0 \\ x_{n+1} \equiv 16 x_n + 1 \pmod{225} \end{cases}$$

ha periodo 225 e la successione $x_0, x_1, x_2, \dots, x_{224}$ è una permutazione del sistema completo di resti mod 225, cioè di $0, 1, 2, 3, \dots, 224$.

Notate che il teorema ci garantisce la stessa cosa anche per la sequenza

$$27) \begin{cases} x_0 = 0 \\ x_{n+1} \equiv \left((16)^\alpha x_n + 1\right) \pmod{3^{100} \cdot 5^{360}} \end{cases}$$

con α esponente intero positivo. Si possono quindi ottenere periodi di lunghezza arbitraria.