Ratio Math. 3
(1992), 57 - 79

SU ALCUNE CARATTERIZZAZIONI DELLE SUCCESSIONI DI NUMERI PSEUDOCASUALI OTTENUTE A PARTIRE DA ALGEBRE DI SUPPORTO

Antonio Maturo(*)

1. INTRODUZIONE

Siano $(Z_m,+,\bullet)$ l'anello degli interi modulo m, $(S,\oplus,\otimes)$ un anello commutativo unitario e * una operazione esterna in S avente Z_m come dominio degli operatori.

Definizione 1.1 Diciamo che S è *un'algebra di supporto di dimensione* n su Z_m se sono soddisfatte le seguenti proprietà

(P1) S è, rispetto all'operazione esterna *, un'algebra su Z_m;
(P2) esiste, in S, una base $\mathscr{B}$ formata da n elementi a cui appartiene l'unità u di S;
(P3) esiste, in S, un elemento x tale che gli elementi di $\mathscr{B}$ coincidono, tranne al più l'ordine, con le potenze $x^0=u,x,x^2,\ldots,x^{n-1}$;
(P4) l'elemento x è invertibile rispetto a $\otimes$.

In [9] sono state studiate alcune proprietà delle algebre di supporto e delle successioni di numeri pseudocasuali ottenute da esse.

In questo lavoro si esaminano alcune caratterizzazioni di tali successioni e si presentano alcuni esempi.

(*) Dipartimento di Scienze, Storia dell'Architettura e Restauro - Università "G. D'Annunzio" - Viale Pindaro 42 - Pescara.

2. COSTRUZIONE DI ALGEBRE DI SUPPORTO PER MEZZO DI POLINOMI SU Z_m

Sia P(y) l'insieme dei polinomi a coefficienti in Z_m. Esso, rispetto all'addizione e moltiplicazione in P(y) e al prodotto di un elemento di Z_m per un polinomio costituisce un'algebra commutativa su Z_m avente come unità il polinomio che si riduce all'unità di Z_m.

Sia f(y) un polinomio di grado $n\geq 1$ e sia (f(y)) l'ideale da esso generato, formato dai prodotti $f(y)\cdot g(y)$, al variare di g(y) in P(y).

Sia S=P(y)/(f(y)) l'insieme quoziente di P(y) rispetto all'ideale (f(y)). Indichiamo con [p(y)] la classe di equivalenza a cui appartiene il generico polinomio p(y).

Poniamo, per ogni p(y), q(y) in P(y) e per ogni $\alpha\in Z_m$

$$\begin{cases}[p(y)]+[q(y)]=[p(y)+q(y)]\\ [p(y)]\cdot[q(y)]=[p(y)\cdot q(y)]\\ \alpha[p(y)]=[\alpha p(y)]\end{cases} \qquad (2.1)$$

Rispetto alle operazioni appena definite S è, com'è noto, una algebra commutativa unitaria, detta *algebra quoziente* di P(y) rispetto a (f(y)). In particolare (f(y))=[f(y)]=[0].

Teorema 2.1 Se f(y) è un polinomio di grado n monico o comunque avente il coefficiente di y^n invertibile, allora ad ogni elemento di S appartiene uno e un solo polinomio di grado minore di n.

Dimostrazione Per un noto teorema, nelle condizioni ammesse per f(y), per ogni g(y) esistono e sono univocamente determinati due polinomi q(y) ed r(y), detti quoziente e resto della divisione di g(y) per f(y) tali che

$$\begin{cases} g(y)=f(y)\cdot q(y)+r(y)\\ \text{grado di } r(y)<\text{grado di } f(y)\end{cases} \qquad (2.2)$$

Le (2.2) implicano che, per ogni g(y), esiste un r(y), di grado minore di n, tale che $r(y)\in[g(y)]$. Se vi fosse anche un $r_1(y)\neq r(y)$ di grado minore di n tale che $r_1(y)\in[g(y)]$ dovrebbe esistere un $q_1(y)$ tale che $g(y)=f(y)q_1(y)+r_1(y)$ il che è contro l'unicità della coppia (q(y),r(y)) soddisfacente le (2.2). ◊◊◊

Osserviamo che se $f(y)=\alpha_0+\alpha_1 y+\ldots+\alpha_n y^n$ è tale che α_n è un divisore dello zero il teorema 2.1 non è più valido.

Infatti se β è un elemento non nullo di Z_m tale che $\beta\alpha_n=0$ il prodotto $\beta f(y)$ è un elemento di [0] di grado minore di n e, in genere, è diverso da 0.

Se f(y) è tale che α_n è invertibile si può sempre supporre, ai fini della costruzione dell'algebra quoziente S, che $\alpha_n=1$. In caso contrario basta sostituire ad f(y) il polinomio $f_1(y)=\alpha_n^{-1} f(y)$. Esso è tale che $(f(y))=(f_1(y))$.

Supponiamo, dunque, da ora in poi, che il polinomio f(y) sia monico.

Teorema 2.2 L'Algebra S soddisfa gli assiomi (P1), (P2), (P3) e, se α_0 è invertibile in Z_m, anche l'assioma (P4).

Dimostrazione Consideriamo gli elementi [1], [y], $[y^2]$...$[y^{n-1}]$. Essi sono indipendenti. Infatti, data una loro combinazione lineare a coefficienti in Z_m

$$\beta_0[1] + \beta_1[y] + \beta_2[y^2] + \ldots + \beta_{n-1}[y^{n-1}], \tag{2.3}$$

risulta

$$\beta_0[1] + \beta_1[y] + \ldots + \beta_{n-1}[y^{n-1}] = [0] \Leftrightarrow$$
$$\Leftrightarrow [\beta_0 + \beta_1 y + \ldots + \beta_{n-1}y^{n-1}] = [0].$$

Per il teorema 2.1 ciò implica che $\beta_0 + \beta_1 y + \ldots + \beta_{n-1}y^{n-1}$ è il polinomio nullo, ossia che $\beta_0 = \beta_1 = \ldots = \beta_{n-1} = 0$.

Se [g(y)] è un qualsiasi elemento di S, esiste, per il teorema 2.1, un $r(y)\in[g(y)]$ di grado minore di n.

Sia $r(y) = \rho_0 + \rho_1 y + \ldots + \rho_m y^m$, con $m<n$. Allora $[g(y)] = [r(y)] = \rho_0[1] + \rho_1[y] + \ldots + \rho_m[y^m]$, per cui [g(y)] è combinazione lineare di [1], $[y]^m$, ..., $[y^{n-1}]$.

L'insieme $\mathscr{B} = \{[1], [y], \ldots, [y^{n-1}]\}$ costituisce quindi una base di S.

Poiché, per ogni $[g(y)]\in S$, risulta, per le (2.1), $[g(y)]\bullet[1] = [g(y)]$, [1] è l'elemento unitario di S e quindi vale la (P2).

Sempre per le (2.1) si ha, per ogni intero non negativo i, $[y]^i = [y^i]$. Ciò implica la (P3).

Infine, se α_0 è invertibile in Z_m , poiché

$$[f(y)] = \alpha_0[1] + \alpha_1[y] + \ldots + \alpha_n[y^n] = [0], \tag{2.4}$$

si ha

$$-\alpha_0^{-1}(\alpha_1[y] + \alpha_2[y^2] + \ldots + \alpha_n[y^n]) = [1],$$

ossia

$$[y]\,(-\alpha_0^{-1})([\alpha_1] + \alpha_2[y] + \ldots + \alpha_n[y^{n-1}]) = [1],$$

il che dimostra che [y] è invertibile rispetto alla moltiplicazione in S. ◊◊◊

In conclusione, per f(y) monico e α_0 invertibile, S è un'algebra di supporto di dimensione n.

Poniamo x=[y], u=[1], 0=[0]. Tale algebra ha la base $\mathscr{B}$= {x=u, x, x^2, ..., x^{n-1}}.

La (2.4) implica, essendo α_n=1,

$$x^n = (-\alpha_0)u + (-\alpha_1)x + \ldots + (-\alpha_{n-1})x^{n-1}. \tag{2.5}$$

Dalla (2.5) segue che tale algebra coincide con quella ottenuta introducendo, nel modulo S su Z_m, la moltiplicazione in S individuata dalle costanti caratteristiche

$$\beta_i = -\alpha_i, \quad \text{per } i = 0, 1, \ldots, n-1. \tag{2.6}$$

Consideriamo l'insieme $V = Z_m^n$ delle n-ple di elementi di Z_m. Introduciamo, in V una addizione $\oplus$ e una moltiplicazione $\bullet$ di un elemento V per un elemento di Z_m, ponendo, per $x = (\alpha_0, \alpha_1, \ldots \alpha_{n-1})$, $y = (\beta_0, \beta, \ldots \beta_{n-1})$ in V e ω in Z_m,

$$x \oplus y = (\alpha_0+\beta_0, \alpha_1+\beta_1, \ldots, \alpha_{n-1}+\beta_{n-1}), \tag{2.7}$$

$$\omega \bullet x = (\omega\alpha_0, \omega\alpha_1, \ldots, \omega\alpha_{n-1}) \tag{2.8}$$

Rispetto alle operazioni così definite, V è un modulo su Z_m. Esso possiede basi formate da n elementi.

Sia $\mathscr{B}$={x_0=u, x_1, ..., x_{n-1}} una di tali basi.

Ogni x∈S è esprimibile, in una sola maniera, nella forma:

$$x = \sum_{i=0}^{n-1} \alpha_i x_i \tag{2.9}$$

con opportuni $\alpha_i \in Z_m$.

Se x_r e x_t sono due elementi qualsiasi della base esistono, allora, in Z_m, degli elementi γ_{sti} tali che:

$$x_s \bullet x_t = \sum_{i=0}^{n-1} \gamma_{sti} x_i \tag{2.10}$$

Al variare di s,t,i si ottengono n^3 elementi γ_{sti}, detti *costanti di struttura*

dell'algebra, dai quali è possibile determinare ogni prodotto x•y con x e y scelti arbitrariamente in S.

Infatti se

$$x=\sum_{i=0}^{n-1}\alpha_i x_i, \quad y=\sum_{i=0}^{n-1}\beta_i x_i, \tag{2.11}$$

risulta:

$$x\bullet y=\sum_{s=0}^{n-1}\alpha_s x_s\bullet\sum_{t=0}^{n-1}\beta_t x_t=\sum_{s=0}^{n-1}\sum_{t=0}^{n-1}\alpha_s\beta_t x_s\bullet x_t$$

e, per la (2.10)

$$x\bullet y=\sum_{i=0}^{n-1}\left(\sum_{s=0}^{n-1}\sum_{t=0}^{n-1}\alpha_s\beta_t\gamma_{sti}\right)x_i \tag{2.12}$$

Tenuto conto dei teoremi 4.1 e 4.2 di [9] possiamo precisare il teorema 4.3 di [9] enunciando il seguente

Teorema 2.3 Sia $V = Z_m^n$ il modulo di dimensione n su Z_m con le operazioni (2.7) e (2.8) e sia $\mathscr{B} = \{x_0, x_1, \ldots, x_{n-1}\}$ una sua base.

Le condizioni

$$x_1x_s = x_{s+1} \quad \text{per } s = 0, 1, \ldots, n-2 \tag{2.13}$$

$$x^n=\sum_{i=0}^{n-1}\beta_i x_i \tag{2.14}$$

con β_0 invertibile, definiscono, per mezzo della (2.12) un'unica algebra di supporto, tale che $x_i=x_1^i$ per i=0, 1, ..., n-1.

Essa è isomorfa all'algebra quoziente S=P(y)/(f(y)), dove

$$f(y)=y^n-\sum_{i=0}^{n-1}\beta_i y^i. \tag{2.15}$$

3. SUL PERIODO DELLE SUCCESSIONI DI NUMERI PSEUDOCASUALI OTTENUTE, CON PARTICOLARE *RIFERIMENTO AI CASI N=1 E N=2*

Siano S un'algebra di supporto di dimensione n su Z_m, $\mathcal{B}=\{x_0=u, x, x^2, \ldots, x^{n-1}\}$ una sua base e

$$x^n = \sum_{i=0}^{n-1} \beta_i x^i. \qquad (3.1)$$

Se z è un elemento di S invertibile rispetto alla moltiplicazione le potenze z^h costituiscono un gruppo ciclico moltiplicativo, sottogruppo del gruppo moltiplicativo I costituito dall'insieme degli elementi di S invertibili rispetto alla moltiplicazione. In particolare ciò avviene per z=x, dato che x è invertibile.

Definizione 3.1 Sia z un elemento di S invertibile rispetto alla moltiplicazione e sia ψ una funzione di supporto.

Definisco *successione canonica* ottenuta a partire da z di S per mezzo della ψ la successione $\{y_k = \psi(z^k)\}_{k\in N_0}$ in Z_m.

Data una successione $\{y_k\}_{k\in N_0}$ di elementi di Z_m, perché essa possa essere considerata successione di numeri pseudocasuali (più precisamente trasformabile in una successione di numeri pseudocasuali per mezzo di una funzione ausiliaria) occorre che soddisfi determinati requisiti matematici e statistici, alcuni di carattere generale, altri di carattere particolare relativi ai problemi per i quali viene utilizzata la successione.

Di fondamentale importanza è il fatto che la successione sia periodica con le seguenti proprietà:

(PP1) l'antiperiodo è nullo;
(PP2) il periodo è noto e sufficientemente lungo (in pratica, per i problemi più comuni, basta che sia dell'ordine di 10^{10}).

La (PP1) è certamente soddisfatta per le successioni canoniche. Per quanto riguarda la (PP2) cominciamo con l'osservare che se $|I|$ è il numero di elementi di I, il periodo $\mu(z)$ del gruppo ciclico generato da un $z\in I$ è, per il teorema di Lagrange, un divisore di $|I|$. Il periodo $\lambda(z,\psi)$ della successione canonica ottenuta a partire da z per mezzo della ψ è un divisore di $\mu(z)$ e quindi anche di $|I|$.

Definizione 3.2 Sia z un elemento di I. Dico che z è *primitivo in S* se risulta $\mu(z)=|I|$.

Dico che z è *massimale in S* se, per ogni $v \in I$, risulta $\mu(v) \leq \mu(z)$.

I problemi più importanti relativi al periodo delle successioni canoniche sono:

(PS1) calcolo di $|I|$;
(PS2) ricerca di valori $\beta_0, \beta_1, \ldots, \beta_{n-1}$ delle costanti caratteristiche che massimizzano $|I|$;
(PS3) ricerca di valori $\beta_0, \beta_1, \ldots, \beta_{n-1}$ delle costanti caratteristiche che rendono $|I|$ numero primo oppure tali che i divisori di $|I|$ abbiano proprietà assegnate;
(PS4) ricerca degli elementi primitivi di S o, se non vi sono elementi primitivi, di quelli massimali;
(PS5) ricerca di condizioni su ψ o sulle β_i tali che sia $\lambda(z,\psi)=\mu(z)$.

Ovviamente le successioni canoniche prese in maggiore considerazione sono quelle ottenute a partire da x. Di conseguenza ha molta importanza la determinazione di costanti caratteristiche che rendono x elemento primitivo o massimale.

Tutti i problemi sono risolti se si riesce a trovare che $|I|$ è un numero primo. In tal caso, infatti, per ogni $z \neq u$, $\lambda(z,\psi)=\mu(z)=|I|$.

Vediamo ora alcuni risultati relativi ai casi n=1 e n=2.

Caso n=1. Come si è visto in [9], si può assumere $S=Z_m$ e la successione $\{x^k\}_{k\in N_0}$ si riduce alla $\{\beta_0^k\}_{k\in N_0}$.

Rinviando a [8] per le dimostrazioni, si vede che valgono i seguenti teoremi:

(T1) $|I|=\Phi(m)$, dove Φ è l'indicatore di Eulero-Gauss;
(T2) se m è primo $\Phi(m)=m-1$. Gli elementi primivi sono $\Phi(m-1)$;
(T3) se $m=p^s$, con $p\neq 2$, $\Phi(m)=m-(m/p)$. Il numero di elementi primitivi è $\Phi(m-(m/p))$;
(T4) se $m=2^s$, $\Phi(m)=m/2$. Per $s>2$ non vi sono elementi primitivi. Gli elementi massimali hanno periodo $\mu=m/4$ e, per $s>3$ sono i $\beta_0 \in I$ tali che $r(\beta_0)\equiv 3 \pmod 8$ o $r(\beta_0)\equiv 5 \pmod 8$;
(T5) se $m = p_1^{s1} p_2^{s2} \ldots p_r^{sr}$, con $p_1, p_2, \ldots, p_r$ numeri primi, $\Phi(m)=m[1-(1/p_1)][1-(1/p_2)]\ldots[1-(1/p_r)]$. Se $\mu_1, \mu_2, \ldots, \mu_r$ sono i massimi periodi ottenibili in corrispondenza dei moduli $p_1^{s1}, p_2^{s2}, \ldots, p_r^{sr}$, gli elementi massimali hanno periodo μ uguale al minimo comune multiplo di $\mu_1, \mu_2, \ldots, \mu_r$. Nel caso di maggior interesse, in cui $m=10^s$, risulta, perciò, $\Phi(m)=2m/5$ e, per $s\geq 4$, $\mu=m/20$. Per $s\geq 5$ si trovano $16m/100$ elementi massimali.

Caso n=2. Sia $\mathscr{B}=\{u,x\}$, $x^2=\beta_0 u+\beta_1 x$.

In base ai teoremi 2.1, 2.2, 2.3, gli elementi di S si possono identificare con le classi di equivalenza dei polinomi $\alpha_0+\alpha_1 y$ su Z_m di grado inferiore a 2, determinate dall'ideale generato dal polinomio

$$f(y) = y^2-\beta_1 y-\beta_0 \tag{3.1}$$

e risulta $[\alpha_1 y+\alpha_0] = \alpha_1 x+\alpha_0 u$.

Poiché il monoide $(S,\bullet)$ è finito, i suoi elementi non invertibili sono le classi $[\alpha_1 y+\alpha_0]$ tali che esiste un polinomio $\delta_1 y+\delta_0$ con δ_1 e δ_0 non entrambi nulli per cui $[\alpha_1 y+\alpha_0]\bullet[\delta_1 y+\delta_0]=[0]$.

Ciò avviene se e solo se esiste un $\gamma_0 \in Z_m$ tale che

$$\gamma_0(y^2-\beta_1 y-\beta_0) = (\alpha_1 y+\alpha_0)\,(\delta_1 y+\delta_0). \tag{3.2}$$

Limitiamoci, per semplicità, a considerare i casi in cui m è primo oppure $m=p^s$ con p numero primo.

(a) Se γ_0 è invertibile, moltiplicando, eventualmente, ambo i membri della (3.2) per γ_0^{-1}, si può supporre $\gamma_0=1$.

In tal caso la (3.2) equivale alle

$$\begin{cases} \alpha_1\delta_1 = 1 \\ \alpha_0\delta_0 = -\beta_0 \\ \alpha_1\delta_0 + \alpha_0\delta_1 = -\beta_1 \end{cases} \tag{3.3}$$

Si deduce che la (3.2) ammette soluzioni se e solo se α_0 e α_1 sono entrambi invertibili ed inoltre

$$f(-\alpha_0\alpha_1^{-1}) = 0 \tag{3.4}$$

(b) Se $\gamma_0=0$ la (3.2) equivale alle

$$\begin{cases} \alpha_1\delta_1 = 0 \\ \alpha_0\delta_0 = 0 \\ \alpha_1\delta_0 + \alpha_0\delta_1 = 0 \end{cases} \tag{3.5}$$

con δ_0 e δ_1 non entrambi nulli.

Le (3.5) ammettono soluzioni non banali se e solo se nè α_1 nè α_0 sono invertibili.

Infatti, se α_1 fosse invertibile, per la prima di esse sarebbe $\delta_1=0$ e per la terza sarebbe $\delta_0=0$. Analogamente, se α_0 fosse invertibile, per la seconda e la terza delle (3.5) sarebbe $\delta_1=\delta_0=0$.

Viceversa, se nè α_1 nè α_0 sono invertibili, allora o $\alpha_1=\alpha_0=0$, oppure, se $m=p^s$ con $s>1$, esiste un intero r tale che $0<r<s$ e α_0 e α_1 hanno entrambi il divisore $[p^r]$. Nel primo caso la (3.5) è soddisfatta da ogni coppia (δ_0,δ_1), nel secondo caso da tutte le coppie tali che sia δ_0 che δ_1 sono multipli di $[p^{s-r}]$.

(c) se γ_0 è un divisore dello zero non nullo, ciò che può verificarsi solo se $m=p^s$ con $s>1$, valgono le

$$\begin{cases} \alpha_1\delta_1 = \gamma_0 \\ \alpha_0\delta_0 = -\beta_0\gamma_0 \\ \alpha_1\delta_0 + \alpha_0\delta_1 = -\beta_1\gamma_0 \end{cases} \tag{3.6}$$

Escludiamo il caso in cui sia α_0 che α_1 sono non invertibili, dato che, in tali ipotesi, si è già visto che la (3.2) ammette una soluzione $(\gamma_0,\delta_0,\delta_1)$, con $\gamma_0=0$.

Moltiplicando, eventualmente, la (3.2) per un fattore invertibile si può sempre porre $\gamma_0=[p^r]$ per un certo intero r tale che $0<r<s$.

Se α_1 è invertibile, dalle (3.6) si vede che δ_0 e δ_1 hanno entrambi γ_0 come divisore.

Esistono, quindi, due elementi δ'_0 e δ'_1 tali che $\delta_0=\delta'_0\gamma_0$, $\delta_1=\delta'_1\gamma_0$.

Poniamo $c_0=r(\gamma_0)$, $b_i=r(\beta_i)$, $a_i=r(\alpha_i)$, $d'_i=r(\delta'_i)$, rispetto al modulo m.

Le (3.6) si possono scrivere

$$\begin{cases} a_1 d'_1 c_0 \equiv c_0 \pmod m \\ a_0 d'_0 c_0 \equiv -c_0 b_0 \pmod m \\ (a_1 d'_0 + a_0 d'_1) c_0 \equiv -c_0 b_1 \pmod m \end{cases} \tag{3.7}$$

Esse implicano le

$$\begin{cases} a_1 d'_1 \equiv 1 \pmod{m / c_0} \\ a_0 d'_0 \equiv -b_0 \pmod{m / c_0} \\ a_1 d'_0 + a_0 d'_1 \equiv -b_1 \pmod{m / c_0} \end{cases} \tag{3.8}$$

e possono scriversi nella forma (3.3) in Z_{m/c_0}.

Poiché $m=p^s$, e b_0 è primo con m, per le (3.7) a_0, d'_0, d'_1 non possono essere divisibili per p, per cui α_0, δ'_0, δ'_1 sono invertibili in Z_m.

Alle medesime formule e considerazioni si perviene partendo dall'ipotesi che α_0 è invertibile.

Si deduce che le (3.6) ammettono soluzioni se e solo se α_1 e α_0 sono entrambi invertibili ed inoltre esiste un intero k tale che

$$f(-\alpha_0\alpha_1^{-1}) = k[m / c_0] \tag{3.9}$$

In conclusione, quindi, la (3.2) è soddisfatta con γ_0 divisore dello zero se e solo se α_1 e α_0 sono elementi invertibili tali che

$$f(-\alpha_0\alpha_1^{-1}) \text{ è un divisore dello zero.} \tag{3.10}$$

Possiamo allora enunciare il seguente

Teorema 3.1 Se $m=p^s$ con p primo, un polinomio $\alpha_1 y+\alpha_0$ è tale che $[\alpha_1 y+\alpha_0]$ è un divisore dello zero in S se e solo se è soddisfatta una delle seguenti condizioni

(D1) α_1 e α_0 sono entrambi invertibili in Z_m e $f(-\alpha_0\alpha_1^{-1})$ è nullo o è un divisore dello zero;
(D2) nè α_1 nè α_0 sono invertibili in Z_m.

Esempio 3.1 Si consideri il polinomio $f(y)=y^2-y-2$ in Z_m con $m=3^2$. Gli elementi di S sono 81.

Determiniamo i polinomi $\alpha_1 y+\alpha_0$ soddisfacenti la (D1).

Posto $h=-\alpha_0\alpha_1^{-1}$, si vede che f(h) è nullo o divisore dello zero con h invertibile per h=2,5,8. In corrispondenza, facendo variare α_1 fra i $\Phi(9)=6$ elementi invertibili di Z_m, si ottengono 18 polinomi. Facendo variare α_0 e α_1 fra i 3 elementi non invertibili di Z_m si ottengono 9 polinomi soddisfacenti la (D2).

Segue che $|I| = 81-27 = 54$.

Poniamo x=[y]. Il periodo di x è un divisore di 54. Precisamente, essendo

$$x^3=3x+2, \quad x^6=3x+4, \quad x^9=9, \quad x^{18}=1,$$

risulta $\mu(x) = 18$.

Esempio 3.2 Si consideri il polinomio $f(y)=y^2-y-1$ in Z_m con $m=3^2$. Non esistono polinomi soddisfacenti la (D1). La (D2) è, ovviamente, sempre

soddisfatta da 9 polinomi.

Segue che $|I| = 81-9 = 72$.

Poniamo x=[y]. Essendo

$$x^4=3x+2,\quad x^6=8x+5,\quad x^8=3x+4,\quad x^{12}=8,$$
$$x^{18}=8x+8,\quad x^{24}=1,$$

risulta $\mu(x) = 24$.

Esempio 3.3 Si consideri il polinomio $f(y)=y^2-y-1$ e sia m=5. Risulta f(1)=4, f(2)=1, f(3)=0, f(4)=1. I divisori di f(y) sono i 4 polinomi $\alpha_1(y-3)$, con $\alpha_1=1, 2, 3, 4$.

La (D2) è verificata solo per $\alpha_1=0$ e $\alpha_0=0$.

Gli elementi di I sono allora $5^2-5=20$ e il periodo di x=[y] è un divisore di 20.

Risulta $x^2=x+1$, $x^4=3x+2$, $x^5=3$, $x^{10}=4$, $x^{20}=1$.

L'elemento x è primitivo in S.

Prendiamo S=V e scegliamo in V la base usuale. La successione $\{x^k\}_{k\in N_0}$ si riduce alla

(1,0), (1,1), (2,1), (3,2), (0,3), (3,0), (3,3), (1,3), (4,1), (0,4), (4,0), (4,4), (3,4), (2,3), (0,2), (2,0), (2,2), (4,2), (1,4), (0,1), ...

4. CASO IN CUI m È PRIMO

Sia m un numero primo. Allora Z_m è un campo. Con riferimento alle notazioni utilizzate nel paragrafo 2., si deduce che

(C1) S=P(y)/(f(y)) è uno spazio vettoriale su Z_m;
(C2) P(y) è un anello euclideo e quindi anche un anello principale.

La (C2) implica che ogni $f(y)\in P(y)$ verifica il teorema 2.1. Il fatto che Z_m è un campo implica che la condizione "a_0 invertibile" del teorema 2.2 si riduce alla "$a_0\neq 0$".

Per il calcolo di $|I|$ vale il seguente

Teorema 4.1 Gli elementi di S-I sono tutti e soli quelli del tipo [g(y)] con g(y) polinomio di grado minore di n e tali che D(f(y),g(y)) ha grado maggiore o uguale ad 1.

Dimostrazione Se $[g(y)]\in$ S-I devono esistere un polinomio h(y) non nullo e di grado minore di n e un polinomio r(y) tali che

$$g(y)\, h(y) = f(y)\, r(y). \qquad (4.1)$$

Se f(y) fosse primo con g(y), per la (C2) f(y) sarebbe un divisore di h(y), il che è assurdo poiché il grado di h(y) è minore di quello di f(y).

Viceversa, se g(y) è non nullo e ha grado minore di n e D(f(y), g(y)) = d(y), ha grado maggiore o uguale ad 1, detti h(y) e k(y) i quozienti delle divisioni di f(y) e g(y) per d(y), essi sono non nulli e di grado minore di n.

Risulta $g(y)\bullet h(y) = k(y)\bullet d(y)\bullet h(y) = k(y)\bullet f(y)$. Posto r(y)=k(y), h(y) e r(y) soddisfano la (4.1). Allora $[g(y)]\bullet[h(y)]=0$ e quindi $[g(y)]\in S\text{-}I$. ◊◊◊

Corollario 4.1.1 Risulta $|I| = m^n-1$ se e solo se f(y) è irriducibile.

Dimostrazione Basta osservare che le condizioni su g(y) del teorema 4.1 sono, in tal caso, soddisfatte solo se g(y) è il polinomio nullo. ◊◊◊

Corollario 4.1.2 S=P(y)/(f(y)) è un campo se e solo se f(y) è irriducibile.

Dimostrazione Basta osservare che ogni g(y) non nullo e di grado minore di n è tale che [g(y)] è invertibile. ◊◊◊

Nel seguito del paragrafo ammettiamo che m è primo e che f(y) è un polinomio su Z_m di grado $n\geq 1$. Indichiamo, inoltre, con k il numero m^n-1.

Vale il seguente

Teorema 4.2 Se f(y) è irriducibile, il campo S è un campo di riducibilità completa del polinomio y^k-1 su Z_m. Le radici di tale polinomio sono tutte distinte e ogni $z\in S-\{0\}$ coincide con una di esse.

Dimostrazione Se $z\in S-\{0\}$, il periodo di z è un divisore di k, per cui $z^k-1=0$. Il polinomio y^k-1 ha dunque, in S, k radici distinte e poichè k è il massimo numero delle sue radici segue il teorema ◊◊◊

I problemi (PS1), (PS2) e, talvolta, (PS3) sono risolti dall'imporre che il polinomio f(y) sia irriducibile. Il problema (PS4) è, invece, risolto dal seguente

Teorema 4.3 Se f(y) è irriducibile esistono, in S, $\Phi(m^n-1)$ elementi primitivi.

Dimostrazione Sia $k = q_1^{r1} q_2^{r2} \ldots q_s^{rs}$, con $q_1, q_2, \ldots, q_s$ numeri primi distinti.

Il polinomio $y^{q_i^{ri}}-1$ è, per ogni i=1, 2, ..., s, un divisore di y^k-1 ed ha quindi, per il teorema 4.2, q_i^{ri} radici distinte. Esse formano rispetto alla moltiplicazione in S un gruppo ciclico C_i. Infatti, posto $g=q_i^{ri}$, risulta

$$(a^g = 1 \text{ e } b^g = 1) \Rightarrow ((ab^{-1})^g = a^g(b^g)^{-1} = 1).$$

Se il massimo ordine degli elementi di C_i non fosse $q_i^{r_i}$, sarebbe un suo divisore $q_i^{r_i-h}$, con h intero positivo.

Allora si avrebbe, per ogni $a \in C_i$,

$$a^{q_i^{r_i-h}} = 1$$

e quindi ogni $a \in C_i$ sarebbe radice del polinomio $y^{q_i^{r_i-h}} - 1$.
Poiché quest'ultimo ha, al più, $q_i^{r_i-h}$ radici distinte risulterebbe $|C_i| \leq q_i^{r_i-h}$. Ciò è assurdo in quanto $|C_i| = q_i^{r_i}$.

Scegliamo ora, in S, per ogni i, un elemento $a_i \in C_i$ di massimo ordine e si consideri l'elemento $a = a_1 \bullet a_2 \bullet \ldots \bullet a_s$.

L'ordine h di a è uguale a k. Infatti, se così non fosse, poiché h è un divisore di k, esisterebbe almeno un q_i tale che k/q_i è multiplo di h, ossia, per un certo intero d, $hd = k/q_j$.

Allora sarebbe

$$a^{k/q_j} = a^{hd} = 1^d = 1$$

e, d'altra parte

$$a^{k/q_j} = a_1^{k/q_j} a_2^{k/q_j} \ldots a_s^{k/q_j} = a_j^{q_j^{r_j-1}} \neq 1,$$

il che è assurdo

Gli elementi di C_i di ordine $q_i^{r_i}$ sono, per i ragionamenti appena visti, le radici di $y^{q_i^{r_i}} - 1$ che non sono radici di $y^{q_i^{r_i-1}} - 1$ e quindi sono in numero di $q_i^{r_i} - q_i^{r_i-1} = \Phi(q_i^{r_i})$.

Allora gli elementi di S del tipo $a = a_1 \bullet a_2 \bullet \ldots \bullet a_s$, con a_i di ordine massimo in C_i, sono

$$\Phi(q_1^{r_1}) \bullet \Phi(q_2^{r_2}) \ldots \Phi(q_s^{r_s}) = \Phi(q_1^{r_1} \bullet q_2^{r_2} \ldots q_s^{r_s}) = \Phi(m^n - 1). \Diamond\Diamond\Diamond$$

Il teorema 4.3 generalizza al caso in cui n è un intero positivo qualsiasi la proprietà (T2) relativa al caso in cui n=1.

Il corollario 4.1.2 e i teoremi 4.2 e 4.3 ci assicurano che, se esiste un polinomio f(y) su Z_m, irriducibile di ordine n, allora esiste un campo S, ampliamento di Z_m che ha le seguenti proprietà:

(K1) è un campo di riducibilità completa del polinomio y^k-1 su Z_m;
(K2) ha m^n elementi.

I teoremi di isomorfismo fra campi di riducibilità completi di uno stesso polinomio sul campo Z_m ci assicurano, inoltre, che ogni campo K che goda della proprietà (K1) è un ampliamento di Z_m formato da m^n elementi ed è isomorfo ad S.

I teoremi visti, però, non ci assicurano che effettivamente esiste, per ogni n, un polinomio g(y) su Z_m irriducibile e quindi un campo S che gode delle proprietà (K1) e (K2).

Per motivi di completezza riportiamo due teoremi che mostrano che, per ogni n, esistono un tale polinomio e un tale campo.

Teorema 4.4 Sia m un numero primo ed n un intero positivo. Se S è un campo di riducibilità completa del polinomio, su Z_m, y^k-1, con $k=m^n-1$ allora

(GF1) S ha m^n elementi;
(GF2) esiste, in S, un elemento di ordine moltiplicativo k.

Dimostrazione Il polinomio derivato di y^k-1 è ky^{k-1}. Una radice x di y^k-1, essendo diversa da zero, è tale che $x^{k-1}\neq 0$. Inoltre, poiché S ha caratteristica m e k è primo con m è $kx^{k-1}\neq 0$. Segue che le radici di y^k-1 sono tutte semplici.

Indichiamo con T l'insieme di tali radici. Se x e z sono elementi di T risulta $(xz^{-1})^k = x^k(z^{-1})^k = 1$ e quindi xz^{-1} è elemento di T.

Inoltre se x e z sono elementi di $T\cup\{0\}$ risulta, poiché S ha caratteristica m,

$$(x-z)^{m^n} = x^{m^n}-z^{m^n} = x-z,$$

per cui anche x-z è elemento di $T\cup\{0\}$. Sia $T^*=T\cup\{0\}$.

Allora T^* è un campo contenente tutte le radici di y^k-1 e contenuto in S. Poiché S è campo di riducibilità completa di tale polinomio deve essere $T^*=S$.

Dato che T^* ha m^n elementi vale la (GF1).

Ragionando come nel teorema 4.3 si deduce anche la (GF2). ◊◊◊

Teorema 4.5 Se m è un numero primo ed n è un intero positivo qualsiasi esiste un polinomio f(y) irriducibile di grado n su Z_m.

Dimostrazione Sia S un campo di riducibilità completa del polinomio, su Z_m, y^k-1, con $k=m^n-1$.

Per il teorema 4.4 esiste, in S, un elemento primitivo x.

S, essendo un ampliamento di Z_m, è uno spazio vettoriale su Z_m. Gli elementi $1, x, x^2, \ldots, x^{n-1}$ formano una base.

Infatti sono linearmente indipendenti, perché, se così non fosse, x sarebbe radice di un polinomio di grado $n_1\leq n-1$ e l'insieme delle potenze di x, essendo

ognuna di esse combinazione lineare di $1, x, x^2, \ldots, x^{n_1-1}$ sarebbe formato al più di $m^{n_1}-1$ elementi, contro l'ipotesi che x è primitivo. Inoltre, ogni elemento di S è combinazione lineare di essi dato che S ha m^n elementi, tanti quante sono le combinazioni lineari distinte di $1, x, x^2, \ldots, x^{n-1}$.

Siano ora $\beta_0, \beta_1, \ldots, \beta_{n-1}$ elementi di Z_m tali che

$$x^n = \beta_0 u + \beta_1 x + \ldots + \beta_{n-1} x^{n-1}, \tag{4.2}$$

e si consideri il polinomio

$$f(y) = y^n - \beta_{n-1} y^{n-1} - \beta_{n-2} y^{n-2} - \ldots - \beta_1 y - \beta_0. \tag{4.3}$$

Esso è irriducibile in Z_m, poiché altrimenti x sarebbe radice di una sua componente $f_1(y_2)$ di grado n_1 tale che $1 \leq n_1 \leq n-1$ e gli elementi $1, x^1, x^2, \ldots, x^{n-1}$ non sarebbero linearmente indipendenti. ◊◊◊

In base ai teoremi di isomorfismo fra campi di riducibilità completi dello stesso polinomio su Z_m il campo di riducibilità completa del polinomio y^k-1 con $k=m^n-1$ è unico a meno di isomorfismi.

Per il teorema 4.5 esso può, per ogni n, pensarsi ottenuto come quoziente P(y)/(f(y)) con f(y) polinomio irriducibile di grado n su Z_m.

Poiché il suo ordine è m^n esso coincide con il campo di Galois $GF(m^n)$.

In riferimento alle notazioni utilizzate nel teorema 4.4 e al polinomio f(y) definito dalla (4.3) un isomorfismo fra il campo S e il campo T=P(y)/(f(y)) è dato dalla applicazione

$$\rho: \sum_{i=0}^{n-1} \delta_i x^i \in S \rightarrow \left[\sum_{i=0}^{n-1} \delta_i y^i \right] \in T, \tag{4.4}$$

dove $\delta_0, \delta_1, \ldots, \delta_{n-1}$ sono generici elementi di Z_m.

In particolare, essendo x primitivo in S, $\rho(x)=[y]$ lo è in T.

In seguito identifichiamo elementi corrispondenti tramite la (4.4) e scriviamo, in particolare, x=[y].

Immediata conseguenza dei teoremi 4.4 e 4.5 è il

Teorema 4.6 Esiste, in P(y), un polinomio irriducibile f(y) tale che, nel campo S=P(y)/(f(y)), x=[y] è un elemento primitivo. ◊◊◊

Delle caratterizzazioni delle radici di un polinomio f(y) irriducibile in Z_m sono fornite dai seguenti

Teorema 4.7 Se f(y) è un polinomio irriducibile di grado n ed S è il campo

di riducibilità completa del polinomio, in Z_m, y^k-1, allora
(R1) f(y) è un divisore di y^k-1 ed ha le radici distinte;
(R2) se $z \in S$ è una radice di f(y), allora 1, z, z^2, ..., z^{n-1} sono linearmente indipendenti.

Dimostrazione Per il teorema 4.2, S coincide, a meno di isomorfismi, con P(y)/(f(y)). Poniamo allora S=P(y)/(f(y)) e x=[y]. I polinomi y^k-1 e f(y) hanno, in S, entrambi la radice x. Il massimo comune divisore fra f(y) e y^k-1, che appartiene a P(y), ha allora grado positivo. Poiché f(y) è irriducibile in Z_m, esso divide y^k-1 e, dato che quest'ultimo ha radici distinte sono tali anche quelle di f(y).

Sia ora z una radice di f(y).

Se 1, z, z^2, ..., z^{n-1} non fossero linearmente indipendenti, z sarebbe radice di un polinomio g(y) a coefficienti in Z_m di grado $n_1<n$. Allora D(f(y), g(y)) avrebbe grado positivo e quindi f(y) non sarebbe irriducibile. ◊◊◊

Teorema 4.8 Sia f(y) un polinomio irriducibile, S=P(y)/(f(y)) e z una radice di f(y) in S. Le radici di f(y) sono le potenze

$$z,\ z^m,\ z^{m^2},\ \ldots,\ z^{m^{n-1}}. \tag{4.5}$$

Esse hanno tutte lo stesso ordine.

Dimostrazione Sia $f(y) = y^n+\alpha_{n-1}y^{n-1}+\alpha_{n-2}y^{n-2}+ \ldots +\alpha_0$ e sia z una sua radice.
Risulta

$$0 = f(z) = f(z)^m = (z^m)^n + \alpha_{n-1}^m (z^m)^{n-1}+\ldots+\alpha_1^m (z^m) + \alpha_0 =$$
$$= (z^m)^n + \alpha_{n-1}(z^m)^{n-1}+\ldots+\alpha_1(z^m)+\alpha_0 = f(z^m).$$

Allora anche z^m è radice di f(y). Per induzione si vede che sono radici tutte le (4.5). Esse sono a due a due distinte.

Infatti, se così non fosse, esisterebbero due interi j e i con $0 \le j < i < n$ tali che $z^{m^j}=z^{m^i}$.

Allora sarebbe

$$z=z^{m^n}=(z^{m^i})^{m^{n-i}}=(z^{m^j})^{m^{n-i}}=z^{m^{n+j-i}}$$

e quindi

$$z^{m^{n+j-i}-1}=1.$$

Posto quindi q=n+j-i, z sarebbe radice del polinomio $x^{m^q}-1$, con q<n. Allora le sue potenze, per il teorema 4.4, sarebbero elementi di un campo di ordine m^q,

e gli elementi 1, z, z^2, ..., z^{n-1} sarebbero linearmente dipendenti, ciò che contraddice il teorema 4.7.

Poiché f(y) ha n radici, esse sono tutti e soli gli elementi (4.5).

Allora, se x e t sono due radici di f(y), risulta per certi i e j

$$x=t^{m^i}, \quad t=x^{m^j}.$$

Se x ha ordine p risulta

$$t^p=(x^{m^j})^p=(x^p)^{m^j}=1,$$

per cui l'ordine di t non supera quello di x. Scambiando i ruoli di x e t segue la seconda parte del teorema. ◊◊◊

Definizione 4.1 *Un polinomio irriducibile di grado n si dice appartenente* all'ordine d se le sue radici hanno nel campo $GF(m^n)$, ordine moltiplicativo d.

Definizione 4.2 Un polinomio irriducibile di grado n si dice primitivo se le sue radici hanno, nel campo $GF(m^n)$, ordine moltiplicativo $k=m^n-1$.

Il teorema 4.6 ci assicura che, per ogni n, esiste un polinomio primitivo di ordine n.

Inoltre, dal teorema 4.5 segue il

Teorema 4.9 Un polinomio f(y) di grado $n\geq 1$ su Z_m che ha come radice un elemento x primitivo di $GF(m^n)$ è irriducibile e primitivo.

Dimostrazione Il polinomio f(y) è irriducibile. Infatti, se così non fosse, x sarebbe radice di un polinomio di grado $n_1<n$. Le potenze di x sarebbero allora combinazioni lineari di 1, x, x^2, ..., x^{n_1-1} e sarebbero al più m^{n_1}. Allora, per il teorema 4.8 f(y) è primitivo. ◊◊◊

Se f(y) appartiene all'ordine d ogni sua radice è radice di x^d-1, per cui f(y), essendo irriducibile, divide x^d-1.

Poiché d deve dividere $k=m^n-1$, segue il

Teorema 4.10 Un polinomio f(y) su Z_m, irriducibile e di grado n, è primitivo se e solo se non è divisore di alcun polinomio x^d-1 con k divisore proprio di m^n-1.

Teorema 4.11 Un polinomio f(y) su Z_m di grado n è irriducibile e primitivo se e solo se sono soddisfatte le seguenti condizioni:

(IP1) per ogni $n_1<n$ il massimo comune divisore di $f(y)$ e $y(y^{k_1}-1)$ con $k_1=m^{n_1}-1$ è uguale a 1,
(IP2) $f(y)$ non divide alcun polinomio del tipo y^d-1 con d divisore non banale di m^n-1.

Dimostrazione Se $f(y)$ è irriducibile e primitivo le condizioni (IP1) e (IP2) sono evidenti. Viceversa, se vale (IP1), $f(y)$ non ha fattori irriducibili di grado $n_1<n$, per cui è irriducibile.

Allora la (IP2) implica che esso è primitivo. ◊◊◊

Esempio 4.1 Riprendiamo il polinomio $f(y) = y^2-y-1$ su Z_5.

Risulta $k=5^2-1=24$. Per $n_1=1$, $k_1=5-1=4$. Per vedere se $f(y)$ è irriducibile o riducibile, essendo il termine noto diverso da zero, si può considerare $\delta(y)=D(f(y), y^4-1)$. Risulta $\delta(y)=y-3$, per cui $f(y)$ è riducibile.

Esempio 4.2 Determiniamo i polinomi $f(y)= y^2+\alpha_1 y+\alpha_0$ irriducibili in Z_5 e, fra essi, quelli primitivi.

Il polinomio $f(y)$ è riducibile se e solo se o ha il termine noto $\alpha_0=0$ oppure ha un divisore comune con y^4-1.

Risulta

$$\begin{cases} f(1)=0 & \text{per } \alpha_1 = -\alpha_0 - 1 \\ f(2)=0 & \text{per } \alpha_1 = -3\alpha_0 - 2 \\ f(3)=0 & \text{per } \alpha_1 = -2\alpha_0 + 2 \\ f(4)=0 & \text{per } \alpha_1 = -\alpha_0 + 1 \end{cases} \tag{4.6}$$

Al variare di α_0 si ottengono, al più, 20 coppie distinte (α_0,α_1) che soddisfano una delle (4.6).

Poiché le possibili coppie (α_0,α_1) sono 25, ci sono almeno 5 polinomi irriducibili.

Per $\alpha_0=1$ si ottengono polinomi irriducibili per $\alpha_1=1,4$.

Per $\alpha_0=2$ si ottengono per $\alpha_1=1,4$. Per $\alpha_0=3$ si ottengono per $\alpha_1=2,3$. Per $\alpha_0=4$ si ottengono per $\alpha_1=2,3$. I polinomi irriducibili sono 8.

I divisori non banali di $m^2-1=24$ sono 2, 3, 4, 6, 8, 12.

Se $f(y)$ divide y^2-1 oppure y^4-1 è riducibile. Si tratta quindi di vedere, fra gli 8 polinomi irriducibili, quali di essi dividono y^3-1, y^6-1 oppure $y^{12}-1$.

Posto $S=P(y)/(f(y))$ e $x=[y]$, risulta

$$x^2=-\alpha_1 x-\alpha_0. \tag{4.7}$$

Vediamo i vari casi

(1) $\alpha_1=1$, $\alpha_0=1$, $x^2=4x+4$.
Risulta $x^3=1$ e il polinomio appartiene al periodo 3.
(2) $\alpha_1=4$, $\alpha_0=1$, $x^2=x+4$.
Risulta $x^3=4$, $x^6=1$ e il polinomio appartiene al periodo 6.
(3) $\alpha_1=1$, $\alpha_0=2$, $x^2=4x+3$.
Risulta $x^3=4x+2$, $x^6=2$, $x^8=3x+1$, $x^{12}=4$, $x^{24}=1$, il polinomio è primitivo.
(4) $\alpha_1=4$, $\alpha_0=2$, $x^2=x+3$.
Risulta $x^3=4x+3$, $x^6=2$, $x^8=2x+1$, $x^{12}=4$, $x^{24}=1$, il polinomio è primitivo.
(5) $\alpha_1=2$, $\alpha_0=3$, $x^2=3x+2$.
Risulta $x^3=x+1$, $x^6=3$, $x^8=4x+1$, $x^{12}=4$, $x^{24}=1$, il polinomio è primitivo.
(6) $\alpha_1=3$, $\alpha_0=3$, $x^2=2x+2$.
Risulta $x^3=x+4$, $x^6=3$, $x^8=x+1$, $x^{12}=4$, $x^{24}=1$, il polinomio è primitivo.
(7) $\alpha_1=2$, $\alpha_0=4$, $x^2=3x+1$.
Risulta $x^3=3$, $x^6=4$, $x^8=2x+4$, $x^{12}=1$, il polinomio appartiene al periodo 12.
(8) $\alpha_1=3$, $\alpha_0=4$, $x^2=2x+1$.
Risulta $x^3=2$, $x^6=4$, $x^8=3x+4$, $x^{12}=1$, il polinomio appartiene al periodo 12.

10. PRIME CONSIDERAZIONI STATISTICHE ED ESEMPI ELEMENTARI

Tenuto conto dei teoremi di omomorfismo fra gruppi e di quelli sui gruppi quozienti si vede subito che il fatto che ψ sia un epimorfismo implica che, per ogni α di Z_m, i sottoinsiemi di S del tipo $\psi^{-1}(\alpha)$ hanno lo stesso numero di elementi.

Poiché $|S| = m^n$ e le classi laterali del nucleo $N=\psi^{-1}(0)$ sono m, risulta allora, per ogni α, $|\psi^{-1}(\alpha)| = m^{n-1}$.

In conseguenza di ciò c'è da attendersi che, se la successione di termine generale x^h ha periodo dell'ordine di $|S|$, ossia se il rapporto $\rho=\mu(x)/|S|$ è vicino all'unità, allora la successione $y_h=\psi(x^h)$ ha una distribuzione delle frequenze assimilabile a quella ottenuta, per mezzo di prove casuali e indipendenti, a partire da una variabile casuale UD(m), uniforme discreta di parametro m.

Il caso più favorevole è quello in cui S è un campo e x è un elemento primitivo. Infatti, in tali ipotesi $\mu(x)=|S|-1$ e 0 l'unico elemento di S non appartenente alla successione canonica generata da x.

Detta $fr(\alpha)$ la frequenza assoluta con cui è raggiunto il valore α nella successione di termine generale y_h, risulta allora

$$fr(\alpha)=\begin{cases} m^{n-1} \text{ per } \alpha \neq 0 \\ m^{n-1}-1 \text{ per } \alpha = 0 \end{cases} \qquad (5.1)$$

La discrepanza della distribuzione delle corrispondenti frequenze relative rispetto alla variabile casuale UD(m) è del tutto soddisfacente rispetto ad un qualsiasi test sulle frequenze.

Le precedenti considerazioni non escludono, comunque, un buon comportamento statistico delle successioni canoniche ottenute nel caso in cui S non è un campo e il rapporto $\rho=\mu(x)/|S|$ è piuttosto basso.

Basta, ad esempio, ricordare che il generatore moltiplicativo è stato sempre usato con successo con il modulo $m=2^s$, pur essendo $\rho=1/4$ per gli elementi massimali e con il modulo $m=10^s$ in cui, sempre per gli elementi massimali, $\rho=1/20$.

In [10] abbiamo mostrato come, anche con tali valori di ρ, con una opportuna scelta dei parametri il generatore moltiplicativo soddisfi ampiamente ai più importanti tests statistici.

La preferenza data, nella pratica, a tali generatori moltiplicativi rispetto a quello con modulo primo per il quale $\rho \cong 1$, fa ritenere che, anche per $n>1$, non è detto che sia da preferire il caso in cui S è un campo.

Requisiti come la rapidità e la semplicità delle elaborazioni, l'uso del sistema di numerazione binario o decimale, considerazioni statistiche o matematiche di vario genere possono portare a scegliere anelli S con divisori dello zero in cui gli elementi massimali abbiano periodo piccolo rispetto a m^n.

Concludiamo esaminando due esempi elementari, allo scopo di illustrare qualche applicazione della teoria svolta. Le successioni ottenute, data la brevità del periodo, non sono significative dal punto di vista statistico, anche se la prima di esse già presenta degli aspetti interessanti.

Esempio 5.1 Consideriamo il caso in cui m=5. Nel paragrafo 4 abbiamo visto che il polinomio y^2+4y+2 è primitivo. Il sostegno di $GF(5^2)$ può essere preso uguale a $V=Z_5^2$. Le costanti caratteristiche dell'algebra $S=P(y)/(y^2+4y+2)$ sono $\beta_1=1$ e $\beta_0=3$.

Costruiamo, in S, la successione $\{x^k\}_{k\in N_0}$, ponendo

$$1=\begin{bmatrix}1\\0\end{bmatrix},\quad x=[y]=\begin{bmatrix}0\\1\end{bmatrix}.$$

Dato che x è primitivo in S la successione è formata da 24 vettori distinti. Essi sono i seguenti

$$\begin{vmatrix}1\\0\end{vmatrix}, \begin{vmatrix}0\\1\end{vmatrix}, \begin{vmatrix}3\\1\end{vmatrix}, \begin{vmatrix}3\\4\end{vmatrix}, \begin{vmatrix}2\\2\end{vmatrix}, \begin{vmatrix}1\\4\end{vmatrix}, \begin{vmatrix}2\\0\end{vmatrix}, \begin{vmatrix}0\\2\end{vmatrix}$$
$$\begin{vmatrix}1\\2\end{vmatrix}, \begin{vmatrix}1\\3\end{vmatrix}, \begin{vmatrix}4\\4\end{vmatrix}, \begin{vmatrix}2\\3\end{vmatrix}, \begin{vmatrix}4\\0\end{vmatrix}, \begin{vmatrix}0\\4\end{vmatrix}, \begin{vmatrix}2\\4\end{vmatrix}, \begin{vmatrix}2\\1\end{vmatrix}$$
$$\begin{vmatrix}3\\3\end{vmatrix}, \begin{vmatrix}4\\1\end{vmatrix}, \begin{vmatrix}3\\0\end{vmatrix}, \begin{vmatrix}0\\3\end{vmatrix}, \begin{vmatrix}4\\3\end{vmatrix}, \begin{vmatrix}4\\2\end{vmatrix}, \begin{vmatrix}1\\1\end{vmatrix}, \begin{vmatrix}3\\2\end{vmatrix}.$$

Fra le possibili applicazioni (LO) scegliamo quella, ψ, che ad ogni $v \in V$ associa la somma delle componenti.

La successione di termine generale $y_k=\psi(x^k)$ è

$$\begin{cases}1,1,4,2,4,0,2,2,3,4,3,0,\\ 4,4,1,3,1,0,3,3,2,1,2,0,\ldots\end{cases} \tag{5.2}$$

di periodo 24.

Le frequenze assolute sono, per ogni α appartenente a Z_5,

$$\mathrm{fr}(\alpha)=\begin{cases}5 \text{ per } \alpha \neq 0\\ 4 \text{ per } \alpha = 0\end{cases} \tag{5.3}$$

conformemente con la (5.1).

Pur con le riserve dovute alla estrema brevità della successione appare opportuno rilevare che oltre alla buona distribuzione delle frequenze dei singoli elementi sono chiaramente visibili altre buone proprietà statistiche, ad esempio la distribuzione della frequenza delle coppie e quella dei runs totali.

Esempio 5.2 Consideriamo, per m=3, il polinomio $f(y)=y^3-y^2-y-1$ e l'algebra $S=P(y)/(f(y))$. Poiché $f(1)=f(2)=1$, $f(y)$ è irriducibile e quindi S è un campo con $3^3=27$ elementi.

Il periodo di x=[y] è un divisore di 26.

Risulta

$x^3=x^2+x+1$, $x^{13}=(x^3)^4x=(x^2+1)^2x=(x^2+2x+2)x=1$,

per cui la successione $\{x^k\}_{k\in N_0}$ ha periodo 13 e l'elemento x non è primitivo.

Prendendo S=V e la base usuale si ottiene la successione di vettori

$$\begin{vmatrix}1\\0\\0\end{vmatrix}, \begin{vmatrix}0\\1\\0\end{vmatrix}, \begin{vmatrix}0\\0\\1\end{vmatrix}, \begin{vmatrix}1\\1\\1\end{vmatrix}, \begin{vmatrix}1\\2\\2\end{vmatrix}, \begin{vmatrix}2\\0\\1\end{vmatrix}, \begin{vmatrix}1\\0\\1\end{vmatrix}, \begin{vmatrix}1\\2\\1\end{vmatrix}, \begin{vmatrix}1\\2\\0\end{vmatrix},$$

$$\begin{vmatrix}0\\1\\2\end{vmatrix}, \begin{vmatrix}2\\2\\0\end{vmatrix}, \begin{vmatrix}0\\2\\2\end{vmatrix}, \begin{vmatrix}2\\2\\1\end{vmatrix}, \begin{vmatrix}1\\0\\0\end{vmatrix}\ldots$$

Per ogni v appartenente a V, prendiamo $\psi(v)$ come nell'esercizio precedente.

La successione di termine generale $y_t=\psi(x^t)$ è

1, 1, 1, 0, 2, 0, 2, 1, 0, 0, 1, 1, 2.

La distribuzione delle frequenze non è buona come nel caso precedente, in cui x era primitivo.

BIBLIOGRAFIA

1. G. Ascoli *Lezioni di Algebra*. Editrice Tirrenia. Torino. 1965
2. A.C. Arvillas and D.G. Matitsas *Partitioning the period of a class of m-sequences and application to pseudorandom number generation*. Journal of the Association for Computing Machinery. Vol. 25. 1978.
3. M. Curzio *Lezioni di Algebra*. Liguori Editore Napoli. 1967.
4. I. Glazman, Y. Luibitch *Analyse linèare dans le espaces de dimensions finies*. Editions Mir Moscou. 1974.
5. S.W. Golomb *Shift register sequences*. Holden-Dsy, Inc. London. 1965.
6. D.E. Knuth *The art of computer programming*. Vol. 2. Seminumerical Algorithms. Addison-Wesley. London. 1969.
7. T.G. Lewis and W.H. Payne *Generalized feedback shift register pseudorandom number algorithm*. Journal of the Association for Computing Machinery. Vol. 20. 1973.
8. A. Maturo *Numeri pseudocasuali*. Montefeltro Edizioni Urbino. 1982.
9. A. Maturo *Numeri pseudocasuali ottenuti a partire da successioni in algebre finite su* Z_m. Ratio Mathematica 1. 1990.
10. A. Maturo, N. Cera *Confronto fra alcuni generatori di numeri pseudocasuali* Periodico di Matematiche 2, 1991.
11. A. Maturo, N. Cera *Generazione di numeri pseudocasuali per mezzo di relazioni di ricorrenza su campi di Galois*. Periodico di Matematiche 2, 1990.
12. W.W. Peterson, E.F. Weldon *Error-correcting codes*. Massachusetts Institute of Technology Press. Cambridge. 1972.