

Sui piani costruiti su anelli

Franco Eugeni¹, Elvira Galiè²

Sunto: In questo lavoro si analizzano classi di piani affini generalizzati su un anello di resti *mod n*. Si ripete la nozione di piano affine generalizzato introdotta in “*Generalized Affine Planes*” F.Eugeni, A. Maturo (ved. bibliografia) iniziando una revisione sistematica con l'utilizzo di esempi appropriati. Nella seconda parte si introduce la nozione di piano proiettivo generalizzato e se ne deducono le prime immediate proprietà.

Parole chiave: anelli, δ -vicinanza, piano affine, piano proiettivo.

Introduzione

La geometria costruita su anelli non ha ricevuto grande attenzione in letteratura e sono veramente pochi i lavori scritti sull'argomento.

Come approccio iniziale intendiamo occuparci di piani affini e proiettivi costruibili su una classe molto particolare di anelli e precisamente quelli delle “classi resto modulo n ”

Se da un lato questa classe è piuttosto ridotta, dall'altra presenta il pregio di essere una classe concreta, nel senso che la si può utilizzare nelle applicazioni alla crittografia.

L'assioma euclideo che in questa geometria “cade” per primo è quello dell'unicità della retta per due punti.

Il solo esame di questa difficoltà ci conduce ad uno studio complesso e articolato e solo parzialmente noto in letteratura.

¹ Dipartimento M.E.T., Università di Teramo, e-mail: eugenif@tin.it

² Dipartimento M.E.T., Università di Teramo, e-mail: elviragalie@libero.it

1. Generalità e simbolismo su $\mathbb{Z}_n$

Sia $\mathbb{Z}_n$ l'anello degli interi modulo n .

Denotiamo con Ω l'insieme dei divisori dello zero più lo zero stesso e con U l'insieme degli elementi invertibili di $\mathbb{Z}_n$.

Ricordiamo che gli elementi invertibili di $\mathbb{Z}_n$ sono le classi $[a] \in \mathbb{Z}_n$ tali che $([a], n) = 1$. E' ovvio che $(U, \cdot)$ è un gruppo, mentre tutte le classi che non verificano questa condizione, cioè per le quali $([a], n) = \delta > 1$ sono divisori dello zero. Infatti:

$$a = h\delta, n = k\delta \quad h, k > 1 \Rightarrow ak = hk\delta = hn \text{ da cui } [a][k] = [0] \text{ in } \mathbb{Z}_n.$$

Nel seguito, per rendere la notazione più agevole, quando questo non dia luogo ad equivoci, per ogni intero δ tale che $1 \leq \delta \leq n$, denoteremo ancora con δ l'elemento $[\delta]$ di $\mathbb{Z}_n$ a cui δ appartiene e con a la $[a]$.

E' interessante notare che gli elementi invertibili di $\mathbb{Z}_n$ sono tanti quanti i numeri a tali che:

- i) $0 < a < n$;
- ii) $(a, n) = 1$

cioè sono esattamente $\varphi(n)$, dove φ è la funzione di Eulero; tale funzione, come ben noto, soddisfa il Teorema di Eulero sulle congruenze asserente che: $(a, n) = 1 \Rightarrow a^{\varphi(n)} \equiv 1 \pmod{n}$.

Ne segue che $[a][a^{\varphi(n)-1}] = [1]$ in $\mathbb{Z}_n$ e cioè che $[a^{-1}] = [a^{\varphi(n)-1}]$ in $\mathbb{Z}_n$.

Segue ancora che gli elementi di $\Omega \subset \mathbb{Z}_n$ verificano la condizione

$$|\Omega| = n - \varphi(n).$$

Sussiste per $\mathbb{Z}_n$, quando $n=2m$, il seguente:

Teorema 1. (dell'annullatore) Sia $\mathbb{Z}_n$ l'anello delle classi resto mod n e sia n pari. Allora, se $a \in \mathbb{Z}_n$ è un elemento invertibile,

$$[a][n/2] = [n/2].$$

La classe $[n/2]$ si chiama *annullatore* di $\mathbb{Z}_n$.

Dim. Osserviamo che $n = 2m$ e quindi:

$a \in U \Rightarrow (a, n) = 1 \Rightarrow (a, 2m) = 1 \Rightarrow a$ dispari $\Rightarrow (a - 1)$ pari da cui segue $(a - 1)m = 2km \Rightarrow am - m = 2km \Rightarrow am = m \pmod{2m}$ ovvero $[a] [m] = [m] \quad \forall a \in U$.

Il concetto di annullatore verrà utilizzato nella definizione di retta di un piano proiettivo, in quanto un annullatore si comporta esattamente come lo zero nel caso di equazioni omogenee definite su anelli di classi resto di ordine pari.

Per la risoluzione delle equazioni di 1° grado in $\mathbb{Z}_n$ occorre far riferimento al seguente classico teorema.

Teorema 2. Una congruenza $ax + b \equiv 0 \pmod{n}$, nell'ipotesi che sia $(a, n) = \delta$, ha esattamente δ classi di soluzioni definite a meno di multipli di n , delle quali $\delta - 1$ si scrivono, a partire da una soluzione particolare x_0 , nella forma seguente:

$$x_0, x_1 = x_0 + n/\delta, x_2 = x_0 + 2n/\delta, \dots, x_{\delta-1} = x_0 + (\delta - 1)n/\delta.$$

Osservazione. Segue da ciò che un'equazione di 1° grado $[a][x] + [b] = 0$ in $\mathbb{Z}_n$ ha esattamente δ soluzioni ciascuna delle quali individuata da una classe di soluzioni della congruenza associata.

Esempio. Sia data la congruenza $3x \equiv 0 \pmod{n}$. Questa congruenza ha come soluzioni le $\delta = (n, 3) = (6, 3) = 3$ classi. $\delta - 1 = 2$ di queste classi, definite a meno di multipli di $n = 6$, si costruiscono a partire da $x_0 = 0$, soluzione particolare, come segue:

$$x_0 = 0, x_1 = n/\delta = 2, x_2 = 2n/\delta = 4.$$

Le classi sono: $\rho n, 2 + \rho n, 4 + \rho n: \quad \rho \in \mathbb{Z}$

L'equazione $3x = 0$ in $\mathbb{Z}_6$ ha come soluzioni le classi 0, 2, 4, cioè i divisori complementari di 3.

2. Piani affini generalizzati

Ricordiamo che uno *spazio geometrico* è una coppia $(S, \mathbf{B})$ dove S è il v -insieme di elementi detti *punti* e $\mathbf{B}$ è la famiglia di sottoinsiemi di S chiamati *blocchi*.

Inoltre supponiamo che $\forall B \in \mathbf{B}, |B| \leq 2$.

Nel nostro caso, poniamo $S = \mathbb{Z}_n \times \mathbb{Z}_n$ e chiamiamo *punti* i suoi elementi.

Per ogni $[a] \in \mathbb{Z}_n$, denotiamo con $r(a)$ il minimo intero positivo appartenente ad $[a]$. In particolare sia $r(0) = n$.

Diciamo che $[a] \in \mathbb{Z}_n$ divide $[b] \in \mathbb{Z}_n$ e scriveremo $[a] | [b]$ se $r(a) | r(b)$.

Sia δ un intero positivo tale che $\delta | n$. Due punti $P = (x', y')$ e $Q = (x'', y'')$ di S sono chiamati δ -vicini, e scriveremo $P R_\delta Q$ se

$$\exists k_1, k_2 \in \mathbb{Z}_n : x' - x'' = k_1 \delta, \quad y' - y'' = k_2 \delta.$$

Se due punti sono δ -vicini ma non sono δ' -vicini con δ' intero, $\delta' | n$ e $\delta | \delta'$, diciamo che essi sono *strettamente* δ -vicini. È facile provare che la δ -vicinanza è una relazione di equivalenza.

Notiamo che la 1-vicinanza porta alla unica classe di equivalenza S .

Sia P un punto di S . Denotiamo con $V_\delta(P)$ la δ -vicinanza di P , cioè l'insieme dei punti di S δ -vicini a P . Abbiamo

Teorema 3. Vale la seguente: $|V_\delta(P)| = (n/\delta)^2$.

Dim. Determiniamo i punti δ -vicini di $P = (x', y')$. Sia $Q = (x, y)$ un punto di S . Risulta $P R_\delta Q \Leftrightarrow x' - x = k_1 \delta, \quad y' - y = k_2 \delta$, dove $k_1, k_2 \in \mathbb{Z}_n$.

Ciò implica che punti δ -vicini di P soddisfano le seguenti equazioni parametriche: $x = x' - k_1 \delta, \quad y = y' - k_2 \delta$ con $k_1, k_2 \in \mathbb{Z}_n$, che hanno $(n/\delta)^2$ soluzioni.

Notiamo che ci sono due casi particolari:

$$|V_1(P)| = n^2, \quad |V_n(P)| = 1.$$

Abbiamo:

Teorema 4. Siano $P, Q \in S$, denotiamo con δ_1, δ_2 due divisori di n tali che $\delta_1 | \delta_2$. Allora: $V_{\delta_2} \subseteq V_{\delta_1}$

Dim. Evidente.

Teorema 5. Siano δ_1, δ_2 due divisori di n . Se $\delta_1 | \delta_2$ allora $V_{\delta_1}(P)$ contiene $(\delta_2 / \delta_1)^2$ classi di δ_2 -vicini. Perciò
 $|V_{\delta_1}(P)| / |V_{\delta_2}(P)| = (\delta_2 / \delta_1)^2$.

Dim. Evidente.

Introduciamo ora l'"idea" di δ -retta in S . Siano $P = (x_0, y_0)$ e $D = (u, v)$ due punti di S . Consideriamo l'insieme L di punti (x, y) tale che

$$L := \begin{cases} x = x_0 + ut \\ y = y_0 + vt \end{cases} \quad \text{con } t \in \mathbb{Z}_n$$

Il punto D definisce la direzione di L e due punti che differiscono per un coefficiente invertibile di proporzionalità definiscono la stessa direzione. L'insieme L è una δ -retta, e la indicheremo con L_δ , se ci sono due elementi u', v' con $u' \in U$ oppure $v' \in U$ e δ divisore di n tale che $u = \delta u', v = \delta v'$. Per $\delta = 1$ è $u \in U$ oppure $v \in U$ ed L è una 1 -retta, che chiameremo anche *retta lunga*. Per $\delta = n$, L è un punto. Notiamo che una retta lunga può essere rappresentata (eliminando t dalle equazioni parametriche) da un'equazione del tipo
 $ax + by + c = 0, \quad (a, b) \notin \Omega^2$ e contiene, naturalmente, n punti.

Teorema 6. Consideriamo due rette lunghe con equazioni a coefficienti in $\mathbb{Z}_n$.

Se tali due rette lunghe hanno determinante delle loro equazioni pari a Δ , allora esse si intersecano in una r -retta dove $r = (n/(n, \Delta))$.

Dim. Consideriamo il sistema costituito dalle due rette lunghe

$$\begin{cases} ax + by + c = 0 \\ a'x + b'y + c' = 0 \end{cases} \quad (*)$$

Supponiamo che sia $\Delta = \begin{vmatrix} a & b \\ a' & b' \end{vmatrix} \notin \Omega$. Allora il sistema ha un'unica

soluzione e quindi l'intersezione è un unico punto o, se si preferisce, è una n -retta. Essendo $(n; \Delta) = 1$, l'asserto è provato in questo primo caso.

Se invece $\Delta \in \Omega$, vogliamo provare che l'intersezione è costituita da una $(n/(n, \Delta))$ -retta, con $(n; \Delta) > 1$.

Con riferimento al sistema (*), supponiamo che nella seconda retta, essendo $(a', b') \notin \Omega^2$, sia $b' \notin \Omega$, così che la seconda retta si può scrivere nella forma $y = mx + k$, con $m \notin \Omega$. (Diversamente si risolve rispetto ad x e si procede per analogia).

Modificata così la seconda retta, alla equazione della prima retta sostituiamo una combinazione lineare che cancella la y . Ciò si ottiene moltiplicando la prima equazione per b' e sottraendo a questa la seconda equazione moltiplicata per b . Dal sistema (*) allora si ottiene

$$\text{il sistema equivalente } \begin{cases} \Delta x + (cb' - c'b) = 0 \\ y = mx + k \end{cases}.$$

La prima equazione si può interpretare in $\mathbb{Z}$ con la seguente congruenza di primo grado $\Delta x \equiv c'b - cb' \pmod{n}$ che, come è ben noto, possiede $r = (n/(n, \Delta))$ soluzioni $x_1, x_2, \dots, x_r$ per la x e che dà luogo alle classi corrispondenti di $\mathbb{Z}_n$ e quindi agli r punti (x_i, y_i) con $y_i = mx_i + k$, $i = 1, 2, \dots, r$ che costituiscono una (n/r) -retta, in quanto due qualsiasi soluzioni della congruenza di primo grado differiscono per un multiplo di r . Così, scelti due degli r punti, le equazioni della r -retta sono $x = x_i + (x_i - x_j)t$, $y = mx_i + m(x_i - x_j)t$.

Pertanto, per definizione, chiameremo *blocchi* le δ -rette al variare di δ e porremo:

$$\mathbf{B} := \{L_\delta : a, \delta \in \mathbb{Z}, 1 \leq a \leq n, \delta = (a, n)\}.$$

La coppia $(S, \mathbf{B})$, è uno spazio geometrico che noi chiameremo *piano affine generalizzato*.

Nel paragrafo seguente proveremo alcune proprietà dei blocchi.

3. Proprietà dei blocchi di un piano affine generalizzato

Innanzitutto osserviamo che dalla definizione segue:

Teorema 7. Una δ -retta $L_\delta(P)$ per un punto P è contenuta nella δ -vicinanza di P , ossia $L_\delta(P) \subseteq V_\delta(P)$.

Dim. Evidente.

Assumiamo che δ, δ' siano due interi positivi divisori di n .

Teorema 8. $L_{\delta'}(P) \subseteq V_\delta(P) \Leftrightarrow \delta \mid \delta'$.

Dim. Supponiamo che, dato $P = (x_0, y_0)$, $L_{\delta'}(P) \subseteq V_\delta(P) \Rightarrow$ un punto (x, y) di L soddisfa:

$$\begin{cases} x = x_0 + \delta' u' t \\ y = y_0 + \delta' v' t \end{cases} \quad t \in \mathbb{Z}_n \quad \text{dove } \{u', v'\} \cap U \neq \emptyset \text{ e } \delta' \mid n.$$

Poiché $L_{\delta'}(P) \subseteq V_\delta(P) \Rightarrow$ se $t=1$ abbiamo che:

$$\begin{cases} x - x_0 = \delta' u' = k_1 \delta \\ y - y_0 = \delta' v' = k_2 \delta \end{cases} \quad k_1, k_2, t \in \mathbb{Z}_n$$

Assumendo che $u' \in U$, risulta:

$$\delta' u' = k_1 \delta \Rightarrow \delta' = k_1 \delta (u')^{-1} \Rightarrow \delta \mid \delta'.$$

Viceversa, se $\delta \mid \delta'$, allora, per il Teorema 7,

$$L_{\delta'}(P) \subseteq V_{\delta'}(P) \subseteq V_\delta(P).$$

Consideriamo ora le due rette:

$$L_1 := \begin{cases} x = x_0 + ut \\ y = y_0 + vt \end{cases} \quad t \in \mathbb{Z}_n$$

$$L_2 := \begin{cases} x = x_0 + u' t' \\ y = y_0 + v' t' \end{cases} \quad t' \in \mathbb{Z}_n$$

Si ha:

Teorema 9. $L_2 \subseteq L_1 \Leftrightarrow \exists k \in \mathbb{Z}_n : u' = k u, \quad v' = k v.$

Dim. Supponiamo che $L_2 \subseteq L_1$. Allora ogni punto

$(u_0 + u' t', y_0 + v' t')$ di L_2 è un elemento $(x_0 + u t, y_0 + v t)$ di L_1 .

Ne segue che per $t'=1$ esiste un elemento $t = k$ di $\mathbb{Z}_n$ tale che

$x_0 + u' = x_0 + u k$ e $y_0 + v' = y_0 + v k$. Perciò $u' = k u$ e $v' = k v$.

Assumiamo ora che esista un elemento $k \in \mathbb{Z}_n$ tale che

$u' = k u$ e $v' = k v$.

Allora ogni punto di L_2 può essere scritto come $(x_0 + u k t', y_0 + v k t')$ che è un elemento di L_1 .

Una conseguenza immediata del Teorema 9 è la seguente:

Teorema 10. $L_2 = L_1 \Leftrightarrow \exists k \in U : u' = k u, \quad v' = k v.$

Dim. Evidente.

Sia δ un divisore di n . Denotiamo con ϕ l'indicatore di Eulero-Gauss. Abbiamo:

Teorema 11. Le δ -rette per un punto P sono $(2n/\delta) - \phi(n/\delta)$.

Dim. Sia $P = (x_0, y_0)$ un punto di S. $L_\delta(P)$ è un insieme di punti soddisfacenti le seguenti equazioni parametriche:

$$\begin{cases} x = x_0 + ut \\ y = y_0 + vt \end{cases} \quad t \in \mathbb{Z}_n, \quad \{u, v\} \cap U \neq \emptyset$$

Il numero di δ -rette per P è il numero di coppie distinte $(\delta u, \delta v)$ dove $u \in U$ oppure $v \in U$.

Se $u \in U$, per $t = (u)^{-1}$ la direzione può essere scritta come

$$D = (\delta, \delta v(u)^{-1}).$$

Quindi il numero di δ -rette per un punto P con $u \in U$ è il numero di $\delta v(u)^{-1}$ distinti di $\mathbb{Z}_n$ che sono esattamente n/δ .

Allora abbiamo n/δ direzioni differenti del tipo $(\delta u, \delta v)$ con $u \in U$. Supponiamo ora $u \notin U$. Se $u \notin U$, necessariamente dovrà essere $v \in U$. Per $t = (v)^{-1}$, $D = (\delta u(v)^{-1}, \delta)$ è la direzione della δ -retta.

Per ogni $v \in U$ risulta $u(v)^{-1} \notin U$ oppure $u \in U$. Quindi il numero di δ -rette per un punto P con $u \notin U$ è il numero di $\delta u(v)^{-1}$ distinti di $\mathbb{Z}_n$ con $u(v)^{-1} \notin U$. Poniamo $w = u(v)^{-1}$. Risulta :

$$\delta w_1 \equiv \delta w_2 \pmod{n} \Leftrightarrow w_1 \equiv w_2 \pmod{n/\delta}.$$

Poichè w è non invertibile i valori di w che danno origine a valori differenti di δw sono gli elementi non invertibili di $\mathbb{Z}_{n/\delta}$ che sono $n/\delta - \phi(n/\delta)$. Quindi il numero di δ -rette per un punto P è $(2n/\delta) - \phi(n/\delta)$.

Teorema 12. Siano dati $\delta_1, \delta_2, h, h'$, divisori di n , tali che $n = \delta_2 h$, $\delta_2 = \delta_1 h'$. Se vale la seguente proprietà:

i) ogni divisore primo di n lo è anche di h ;

allora ogni δ_2 -retta $L_{\delta_2}(P)$ per un punto P è contenuta esattamente in $h' \delta_1$ -rette per P.

Dim. Sia $L_{\delta_2}(P)$ la δ_2 -retta per $P = (x_0, y_0)$ avente equazioni:

$$\begin{cases} x = x_0 + \delta_2 u t \\ y = y_0 + \delta_2 v t \end{cases} \quad t \in \mathbb{Z}_n, \quad \{u, v\} \cap U \neq \emptyset$$

Una δ_1 -retta per P $L_{\delta_1}(P)$ di equazioni:

$$\begin{cases} x = x_0 + \delta_1 u' t' \\ y = y_0 + \delta_1 v' t' \end{cases} \quad t' \in \mathbb{Z}_n, \quad \{u', v'\} \cap U \neq \emptyset$$

contiene $L_{\delta_2}(P)$ se e solo se

$$\exists k \in \mathbb{Z}_n : \delta_2 u = k \delta_1 u', \quad \delta_2 v = k \delta_1 v'. \quad (1)$$

Ci sono due possibilità:

I) al più una delle coppie (u, u') , (v, v') appartiene a U^2 ;

II) nessuna delle coppie appartiene a U^2 .

Se vale la I), senza perdere di generalità, possiamo porre

$(u, u') \in U^2$. Ciò implica $\delta_2 = k \delta_1$, $\delta_2 v = k \delta_1 v'$, da cui segue che:

$$\delta_2 (v - v') = 0 \quad (2)$$

Essendo $n = \delta_2 h$, $\delta_2 = \delta_1 h'$, si ha che la (2) è equivalente a

$\delta_1 v' \equiv \delta_1 v \pmod{\delta_1 h}$. Il numero di direzioni ($\delta_1 w = \delta_1 v'$) che da origine a δ_1 -rette differenti, è il numero delle soluzioni di $w \equiv \delta_1 v \pmod{\delta_1 h}$ il che vale h' , essendo $n = h' \delta_1 h$.

Se vale il caso II), solo uno tra u e v è invertibile e così anche uno solo tra u' e v' .

Senza perdere di generalità, possiamo porre $u = v' = 1$, mentre u' e v sono non invertibili, in cui è $\text{MCD}(u', n) = d_1 > 1$,

$\text{MCD}(v, n) = d_2 > 1$. Tenendo conto della (1) segue che $\delta_2 = k \delta_1 u'$, $\delta_2 v = k \delta_1$, da cui $\delta_2 = \delta_2 v u'$, $\delta_2 (1 - v u') = 0$.

Essendo $n = \delta_2 h$, si ha

$$v u' = 1 \pmod{h}. \quad (3)$$

La (3) implica quindi che $\text{MCD}(h, u') = 1$, $\text{MCD}(h, v) = 1$.

Dall'ipotesi (a), se p è un primo divisore di d_1 , risulta che $p \mid n$ e $p \mid u'$, quindi $p \mid h$ e $p \mid u'$, cioè $p \mid \text{MCD}(h, u')$. Questa è una contraddizione.

Da ciò, non ci sono δ_1 -rette per P che soddisfano la II) contenenti $L_{\delta_2}(P)$. Quindi le δ_1 -rette per P contenenti $L_{\delta_2}(P)$ sono esattamente h' . *cvd*

Osserviamo che la condizione (a) è necessaria per dimostrare la seconda parte del Teorema.

Per esempio, per $n = 12$, $h = 3$, $\delta_1 = 2$, $\delta_2 = 4$, poniamo

$$L_{\delta_2} := \begin{cases} x = x_0 + \delta_2 ut \\ y = y_0 + \delta_2 vt \end{cases} \quad t \in \mathbb{Z}_n, \quad L_{\delta_1} := \begin{cases} x = x_0 + \delta_1 u' t' \\ y = y_0 + \delta_1 v' t' \end{cases} \quad t' \in \mathbb{Z}_n,$$

Per $u = v' = 1, u' = v = 2, k = 4, I$) è soddisfatta. Allora $L_{\delta_1} \supseteq L_{\delta_2}$ solo se vale la II).

Teorema 13. Sia $P_0 = (x_0, y_0)$ un punto di S . Siano δ_1, δ_2 ed h tre divisori di n , tali che $\delta_2 = \delta_1 h$, e sia L_{δ_1} una δ_1 -retta per P_0 . Allora esiste esattamente una δ_2 -retta per P_0, L_{δ_2} , contenuta in L_{δ_1} .

Dim. Denotiamo con L_{δ_1} una δ_1 -retta per P_0 di equazioni:

$$L_{\delta_1} := \begin{cases} x = x_0 + \delta_1 ut \\ y = y_0 + \delta_1 vt \end{cases} \quad t \in \mathbb{Z}_n, \quad \{u, v\} \cap U \neq \emptyset$$

Allora, L_{δ_2} di equazioni:

$$L_{\delta_2} := \begin{cases} x = x_0 + \delta_2 ut \\ y = y_0 + \delta_2 vt \end{cases} \quad t \in \mathbb{Z}_n, \quad \{u, v\} \cap U \neq \emptyset,$$

dal Teorema 9, è una δ_2 -retta per P_0 contenuta in L_{δ_1} . Siano $L_{\delta_2}, L_{\delta_2}^*$ le due δ_2 -rette per P_0 contenute in L_{δ_1} aventi direzioni (u_1, v_1) e (u_2, v_2) rispettivamente. Poiché $\delta_2 = \delta_1 h$, dal Teorema 9 esisteranno due elementi invertibili k_1 e k_2 tali che $(u_1, v_1) = k_1 h(\delta_1 u, \delta_1 v)$, $(u_2, v_2) = k_2 h(\delta_1 u, \delta_1 v)$. Ciò implica che $k_1^{-1}(u_1, v_1) = k_1^{-2}(u_2, v_2)$ e quindi dal Teorema 10 segue che $L_{\delta_2} = L_{\delta_2}^*$.

Teorema 14. Sia $P_0 = (x_0, y_0)$ un punto di S . Assumiamo che $P_1 = (x_1, y_1)$ sia strettamente δ_2 -vicino di P_0 e che δ_1 e δ_2 siano due divisori di n tali che $\delta_1 \mid \delta_2$. Allora ogni δ_1 -retta L_{δ_1} per P_0 e P_1 contiene la δ_2 -retta L_{δ_2} per P_0 e P_1 avente equazioni:

$$\begin{cases} x = x_0 + (x_1 - x_0)t \\ y = y_0 + (y_1 - y_0)t \end{cases} \quad t \in \mathbb{Z}_n.$$

Dim: Sia L_{δ_1} la δ_1 -retta per P_0 e P_1 avente equazioni:

$$\begin{cases} x = x_0 + ut' \\ y = y_0 + vt' \end{cases} \quad t' \in \mathbb{Z}_n, \quad (**)$$

Poiché $P_1 \in L_{\delta_1}$, abbiamo che per alcuni $t' \in \mathbb{Z}_n$:

$$\begin{cases} x_1 - x_0 = ut' \\ y_1 - y_0 = vt' \end{cases}$$

Dal Teorema 9 segue che $L_{\delta_2} \subseteq L_{\delta_1}$.

Teorema 15. Siano δ_1 e δ_2 due divisori di n tali che $\delta_1 | \delta_2$. L'intersezione di una δ_1 -retta per P_0 con $V_{\delta_2}(P_0)$ è una δ_2 -retta per P_0 .

Dim. Tenendo conto del Teorema 13, una δ_1 -retta L_{δ_1} per P_0 contiene esattamente una δ_2 -retta L_{δ_2} per P_0 . Proviamo che non esiste nessun punto di $V_{\delta_2}(P_0) \cap L_{\delta_1}$ che non appartiene a L_{δ_2} . Infatti, al contrario, denotiamo con P_1 uno di questi punti. La δ_1 -retta deve contenere L_{δ_2} e la δ_2 -retta di equazioni (**) congiungente P_0 e P_1 . Questa, tenendo conto del Teorema 13, è una contraddizione.

Conseguenza immediata dei Teoremi 7 e 15 ottenuta per $\delta_1 = \delta_2$ è:

Teorema 16. Per due punti strettamente δ -vicini $P_0 = (x_0, y_0)$ e $P_1 = (x_1, y_1)$ c'è esattamente una δ -retta ed esattamente la δ -retta L_δ di equazioni:

$$\begin{cases} x = x_0 + (x_1 - x_0)t \\ y = y_0 + (y_1 - y_0)t \end{cases} \quad t \in \mathbb{Z}_n.$$

Teorema 17. Ogni δ -retta ha esattamente n/δ punti.

Dim. Denotiamo con L_δ una δ -retta per un punto $P_0 = (x_0, y_0)$ di S .

Essa ha equazioni:

$$L_\delta := \begin{cases} x = x_0 + \delta ut \\ y = y_0 + \delta vt \end{cases} \quad t \in \mathbb{Z}_n, \quad \{u, v\} \cap U \neq \emptyset$$

Assumiamo che $u \in U$. Due punti P e P' , associati a t e t' rispettivamente, sono uguali se e solo se

$$\begin{cases} \delta ut = \delta ut' \\ \delta vt = \delta vt' \end{cases} \Leftrightarrow \begin{cases} \delta u(t - t') = 0 \\ \delta v(t - t') = 0 \end{cases}$$

Poiché $u \in U$ abbiamo:

$$\begin{cases} \delta u(t - t') = 0 \\ \delta v(t - t') = 0 \end{cases} \Leftrightarrow \delta(t - t') = 0 \Leftrightarrow t \equiv t' \pmod{n/\delta}$$

Così il numero di punti di una δ -retta è n/δ .

La δ -vicinanza, generando una classe di equivalenza in S , opera una partizione dell'insieme di partenza.

Sia ad esempio $n = 4$: il nostro anello di partenza sarà $\mathbb{Z}_4$, $\Omega = \{0, 2\}$, $U = \{1, 3\}$, $S = \mathbb{Z}_4 \times \mathbb{Z}_4$; δ può essere 1 oppure 2.

Se $\delta = 1$, la 1-vicinanza genera tutto S .

Se $\delta = 2$, la 2-vicinanza genera una partizione di S in 4 insiemi:

(0,0) (2,0)	(1,0) (3,0)
(0,2) (2,2)	(1,2) (3,2)
(1,1) (3,1)	(0,1) (2,1)
(1,3) (3,3)	(0,3) (2,3)

Ogni 1-retta per un punto contiene 4 punti (retta lunga);

Ogni 2-retta per un punto contiene 2 punti (retta corta).

Se invece $n = 6$, l'anello di partenza sarà $\mathbb{Z}_6$,

$\Omega = \{0, 2, 3, 4\}$, $U = \{1, 5\}$, $S = \mathbb{Z}_6 \times \mathbb{Z}_6$. δ può essere 1, 2 oppure 3.

Se $\delta = 1$, la 1-vicinanza genera tutto S.

Se $\delta = 2$, la 2-vicinanza genera la partizione di S:

(0,0) (2,0) (4,0)	(1,0) (3,0) (5,0)
(0,2) (2,2) (4,2)	(1,2) (3,2) (5,2)
(0,4) (2,4) (4,4)	(1,4) (3,4) (5,4)
(1,1) (3,1) (5,1)	(0,1) (2,1) (4,1)
(1,3) (3,3) (5,3)	(0,3) (2,3) (4,3)
(1,5) (3,5) (5,5)	(0,5) (2,5) (4,5)

Mentre la 3-vicinanza genera 9 insiemi:

(0,0) (3,0)	(0,1) (0,4)	(0,2) (0,5)
(0,3) (3,3)	(3,1) (3,4)	(3,2) (3,5)
(1,0) (4,0)	(1,1) (4,1)	(1,2) (4,2)
(1,3) (4,3)	(1,4) (4,4)	(1,5) (4,5)
(2,0) (5,0)	(2,1) (5,4)	(2,2) (5,2)
(2,3) (5,3)	(5,1) (2,4)	(5,5) (2,5)

Ogni 1-retta per un punto contiene 6 punti;

Ogni 2-retta per un punto contiene 3 punti;

Ogni 3-retta per un punto contiene 2 punti.

Riguardo alle problematiche aperte, sono da completare le valutazioni seguenti e le loro conseguenze:

- a) Valutare l'intersezione di due rette corte, confrontando le parametriche in t e τ ;
- b) Valutare l'intersezione di una δ -retta con una δ' -vicinanza;
- c) Valutare il numero di δ' -rette per una δ -retta;
- d) Valutare il numero globale delle δ -rette, tenendo conto che, al variare di δ , alcune δ -rette sono contenute in altre δ' -rette, con $\delta \mid \delta'$.

Nell'ordine di idee indicato, ci limitiamo a provare che:

Teorema 18. Sia B_1 l'insieme di tutte le 1-rette (rette lunghe) del piano affine generalizzato $(S, \mathbf{B})$. Allora: $|B_1| = n^2 + (n - \varphi(n))n$.

Dim. Sia $ax + by + c = 0$ (a, b) $\notin \Omega^2$ l'equazione di una retta lunga.

Se $a \notin \Omega$, ho esattamente n^2 rette del tipo $x = -a^{-1}by - a^{-1}c$.

Se $a = \omega \in \Omega$ e quindi $b \notin \Omega$, segue che la retta è del tipo

$\omega b^{-1}x + y + c b^{-1} = 0$ e poiché al variare di ω , ωb^{-1} descrive biettivamente Ω , segue che tali rette sono per ogni ω in numero di n . Poiché $|\Omega| = n - \varphi(n)$, segue l'asserto.

Osservazione. Ogni δ -retta con $\delta > 1$ è contenuta in almeno una 1-retta.

4. Definizione di piano proiettivo su $\mathbb{Z}_n$

Consideriamo ora le terne (x_0, x_1, x_2) di elementi di $\mathbb{Z}_n$ con $(x_0, x_1, x_2) \notin \Omega^3$ (cioè non tutti e tre contemporaneamente in Ω) e definite a meno di un fattore invertibile. Queste terne si diranno *punti*. Denotiamo con S l'insieme di detti punti. Consideriamo le equazioni

$$a x_0 + a_1 x_1 + a_2 x_2 = 0 \tag{4}$$

dove (a_0, a_1, a_2) è un punto. Ciascun insieme di punti del piano proiettivo che soddisfa una di queste equazioni si dirà *retta lunga*.

Se $n = 2m$ definiamo due classi di rette: le (4) definite sopra che chiameremo *rette lunghe di 1° specie* e i luoghi dei punti di equazione:

$$a x_0 + a_1 x_1 + a_2 x_2 = n/2 \quad (5)$$

che chiameremo *rette lunghe di 2° specie*.

Denotiamo con $B_{1,I}$ e $B_{1,II}$ rispettivamente l'insieme delle rette lunghe di 1° e 2° specie e poniamo

$$B_1 = B_{1,I} \cup B_{1,II}.$$

Introduciamo i parametri seguenti ai fini di una valutazione dell'aritmetica del piano proiettivo:

Poniamo:

$\mathbf{b}_1$:= numero delle rette lunghe del piano proiettivo;

$\mathbf{b}_{1,I}$:= numero delle rette lunghe di 1° specie del piano proiettivo;

$\mathbf{b}_{1,II}$:= numero delle rette lunghe di 2° specie del piano proiettivo;

$\mathbf{v}$:= numero dei punti del piano;

$\mathbf{k}$:= numero dei punti di una retta;

$\mathbf{r}$:= numero delle rette per un punto.

Ci proponiamo allora di determinare, $\mathbf{b}_1, \mathbf{b}_{1,I}, \mathbf{b}_{1,II}, \mathbf{v}, \mathbf{k}, \mathbf{r}$.

Teorema 19. Risulta

$$\mathbf{b}_{1,I} + \mathbf{b}_{1,II} = \mathbf{b}_1 = \mathbf{v} = \frac{n^3 - (n - \varphi(n))^3}{\varphi(n)}.$$

Dim. Sia (x_0, x_1, x_2) un generico punto di $\mathbb{Z}_n^3$. Le possibili terne di $\mathbb{Z}_n$ sono n^3 e se da queste escludo le terne aventi tutte e tre le componenti in Ω , abbiamo in totale $n^3 - (n - \varphi(n))^3$ terne.

Ora, se si tiene conto che due terne (a_i) e (b_i) sono equivalenti se e solo se $\exists k \in U$ tale che $b_i = ka_i$ in $\mathbb{Z}_n$, ne risulta che $(\mathbb{Z}_n)^3 - \Omega^3$ è

ripartito in classi di equivalenza, ciascuna delle quali contiene una terna con le $\varphi(n)-1$ terne ad essa equivalenti.

Allora gli elementi del quoziente $(\mathbb{Z}_n)^3 - \Omega^3 / \cong$ sono

$$\frac{n^3 - (n - \varphi(n))^3}{\varphi(n)}$$

e questo quoziente è, per definizione, il piano proiettivo denotato con $\text{PG}(2, \mathbb{Z}_n)$.

Notiamo che il numero delle rette di un piano (eventualmente solo di 1° specie o di 2° specie), il numero dei piani dello spazio 3-dimensionale e più in generale il numero degli iperpiani di uno spazio r -dimensionale eguagliano il numero di punti dello spazio,

$$\text{per cui } \mathbf{b}_{\text{I,I}} + \mathbf{b}_{\text{I,II}} = \mathbf{b}_1 = \mathbf{v} = \frac{n^3 - (n - \varphi(n))^3}{\varphi(n)}.$$

Per quanto riguarda il calcolo di $\mathbf{k}$ ed $\mathbf{r}$, abbiamo:

$$\textbf{Teorema 20. Risulta: } \mathbf{k} = \mathbf{r} = \frac{n^2 - (n - \varphi(n))^2}{\varphi(n)}.$$

Dim. Riferendoci al Teorema precedente, osserviamo che la valutazione va fatta non più sulla terna (x_0, x_1, x_2) ma sulla coppia (x_0, x_1) , per cui le coppie in totale saranno n^2 ; se escludo le coppie aventi tutte e due le componenti in Ω , avremo in totale

$$n^2 - (n - \varphi(n))^2 \text{ coppie, da cui } \mathbf{k} = \mathbf{r} = \frac{n^2 - (n - \varphi(n))^2}{\varphi(n)}.$$

Il primo problema che si pone in questo tipo di piano proiettivo è il seguente:

“Sotto quali condizioni e in che senso due punti del piano distinti sono congiungibili?”

Come sappiamo, ciò è sempre vero nei piani proiettivi su un campo.

Nel nostro caso, supponiamo di avere due punti $Y = (y_i), Z = (z_i)$ tali che y_i non è proporzionale a z_i ; l'eventuale equazione della retta che li congiunge $\sum_{i=0}^2 a_i x_i = 0$ può essere assegnata mediante il determinante:

$$\begin{vmatrix} x_0 & x_1 & x_2 \\ y_0 & y_1 & y_2 \\ z_0 & z_1 & z_2 \end{vmatrix} = 0$$

Pertanto i due punti sono congiungibili con una retta lunga se e solo se i minori della matrice

$$\begin{pmatrix} y_0 & y_1 & y_2 \\ z_0 & z_1 & z_2 \end{pmatrix}$$

non sono tutti e tre divisori dello zero.

Esistono allora coppie di punti distinti non congiungibili in questo senso. Ad esempio, presi in $\mathbb{Z}_6 \times \mathbb{Z}_6$ i due punti $Y = (0, 2, 1)$, $Z = (2, 1, 2)$, si ha che i minori della matrice delle componenti sono

$$\begin{vmatrix} 2 & 1 \\ 1 & 2 \end{vmatrix} = 3; \quad \begin{vmatrix} 0 & 1 \\ 2 & 2 \end{vmatrix} = -2 = 4; \quad \begin{vmatrix} 0 & 2 \\ 2 & 1 \end{vmatrix} = 2 \quad \text{che sono tutti in } \Omega.$$

Le problematiche che si aprono in questo contesto sono molto ampie:

- 1) Ricerca dei punti impropri di una retta: dipende naturalmente dalla definizione. Chiamiamo $Y = (y_0, y_1, y_2)$ improprio quando $y_0 = 0$, o più in generale quando $y_0 \in \Omega$?

In questo secondo caso vi sono dei luoghi di punti come quelli di equazione $x_0 = \omega \in \Omega - \{0\}$ che non sono rette. Lo studio di un sistema retta – luogo improprio non sembra a priori facile.

2) Definizione di un punto proprio con la condizione $y_0 \notin \Omega$.
 Questa zona dovrebbe realizzare un ovvio isomorfismo con la parte affine $(y_0, y_1, y_2) \leftrightarrow (y_1 y_0^{-1}, y_2 y_0^{-1})$ e quindi permettere di rileggere in termini proiettivi i risultati della parte affine e quindi della nozione di δ -vicinanza.
 Si aprono problematiche tipo:

a) Congiungere un punto “proprio” $Y = (y_0, y_1, y_2)$ con $y_0 \notin \Omega$ con un punto della forma $(0, l, m)$ che dovrebbe condurre ad una retta lunga $y - y_2 y_0^{-1} = m(x - y_2 y_0^{-1})$ che certamente contiene nella “sua versione omogenea” entrambi i punti $mx - y - (my_1 y_0^{-1} - y_2 y_0^{-1})t = 0$ ma non è chiaro, al momento, il senso di un punto del tipo $Y = (y_0, y_1, y_2) \quad y_0 \in \Omega - \{0\}$.

b) Scrivere delle equazioni del tipo:

$$x_i = \lambda y_i + \mu z_i$$

significa dare delle parametriche in campo proiettivo. Sono utili queste per generalizzare il concetto di δ -retta?

3) Sono aperti tutti i possibili conteggi di tipo combinatorio ai fini di completare lo studio dei vari parametri di interesse in questo piano.

4) Lo studio dell'intersezione di due rette lunghe, ben definito nel caso affine, come si traduce in campo proiettivo?

5) Il passaggio, da costruire, da affine a proiettivo e viceversa, come e in che senso può essere una generalizzazione di quello classico?

Queste problematiche chiudono il nostro lavoro e costituiscono il punto di partenza di una ulteriore indagine che si rivela articolata e con varie difficoltà per le complessità di calcolo.

Bibliografia

- [1] Berardi L., Eugeni F.. (1988) Blocking sets e teoria dei giochi: origini e problematiche, in: *Atti sem. Mat. e Fis.Univ. Modena*, Vol. XXXIV, 165-196
- [2] Cerasoli M., Eugeni F., Protasi M. (1988) *Elementi di matematica discreta*, Zanichelli
- [3] Gionfriddo M., (1986) Sui sistemi di Steiner, in: *Sem. Geom. Comb. Univ. L'Aquila*, Vol. 9
- [4] Segre B. (1961) *Lectures on modern geometry*, Cremonese
- [5] Tallini G. (1979) Spazi combinatori e sistemi di Steiner, *Riv. Mat. Univ. Parma*, Vol. 5, 221-248
- [6] Eugeni F., Maturo A. (1991) *Generalized Affine Planes*, in: *Journal of information & Optimization Sciences*, Vol. 12, Nr.3, 431-439