Atti Accademia Nazionale dei Lincei

Classe Scienze Fisiche Matematiche Naturali

Rendiconti

Umberto Bartocci, Emanuela Ughi

Terne di quadrati consecutivi in un campo di Galois

Atti della Accademia Nazionale dei Lincei. Classe di Scienze Fisiche, Matematiche e Naturali. Rendiconti, Serie 8, Vol. **71** (1981), n.6, p. 151–155.

Accademia Nazionale dei Lincei

<http://www.bdim.eu/item?id=RLINA_1981_8_71_6_151_0>

Atti della Accademia Nazionale dei Lincei. Classe di Scienze Fisiche, Matematiche e Naturali. Rendiconti, Accademia Nazionale dei Lincei, 1981.

RENDICONTI

DELLE SEDUTE

DELLA ACCADEMIA NAZIONALE DEI LINCEI

Classe di Scienze fisiche, matematiche e naturali

Seduta del 12 dicembre 1981

Presiede il Presidente della Classe GIUSEPPE MONTALENTI

SEZIONE I

(Matematica, meccanica, astronomia, geodesia e geofisica)

Teoria dei numeri. — *Terne di quadrati consecutivi in un campo di Galois.* Nota di UMBERTO BARTOCCI e EMANUELA UGHI (*), presentata (**) dal Socio E. MARTINELLI.

SUMMARY. — Explicit formulae for the number of triplets of consecutive squares in a Galois field F_q are given.

Lo studio delle successioni di quadrati consecutivi in un campo di Galois è stato oggetto di vari recenti lavori soprattutto in vista delle possibili applicazioni a questioni di geometria combinatoria. In realtà, alla questione generale della distribuzione dei simboli di Legendre – almeno nel caso F_p (con p primo arbitrario dispari) – sono state dedicate moltissime ricerche sin dagli inizi del secolo, e ne è stata evidenziata la connessione con il problema del numero dei punti di una curva algebrica su un campo finito (vedi al proposito l'ampia bibliografia contenuta in L. Guerra ed E. Ughi, [1]). Ciò nonostante, non ci sembra sia ancora possibile reperire nella letteratura una formula esplicita per il numero delle terne di quadrati consecutivi (il caso delle coppie è ben più facile e completamente conosciuto), anche se già nel 1906 E. Jacobsthal, [2], osservava la dipendenza tra il numero delle terne di non quadrati consecutivi in F_p e la decomposizione di p come somma di due quadrati nel caso «più difficile» $p \equiv 1 \bmod 4$.

(*) Lavoro eseguito nell'ambito delle attività dei gruppi di ricerca matematica del C.N.R.

(**) Nella seduta del 12 dicembre 1981.

È sembrato pertanto agli Autori di far cosa utile nel fornire la seguente tabella, mostrando come essa si possa dedurre facilmente dalla teoria delle curve ellittiche su un campo finito (per la quale si può fare ad esempio riferimento al testo di A. Robert, [4]).

Notazioni: F_q, $q = p^h$, campo di Galois qualsiasi di caratteristica dispari $p = 4k \pm 1$

$E(q) =$ numero delle terne di quadrati consecutivi in $F_q^* = F_q - \{0\}$

VALORI DI $E(q)$

	$p \equiv 1 \bmod 4$	$p \equiv -1 \bmod 4$
h dispari	$\frac{1}{8}\left[q-7-2\sum_{j=0}^{(h-1)/2}\binom{h}{2j}a^{h-2j}(a^2-p)^j-4(1+(-1)^k)\right]$	$\frac{1}{8}[q-3-2(1+(-1)^k)]$
h pari	$\frac{1}{8}\left[q-15-2\sum_{j=0}^{h/2}\binom{h}{2j}a^{h-2j}(a^2-p)^j\right]$	$\frac{1}{8}[q-15-2(-p)^{h/2}]$

ove nel caso $p \equiv 1 \bmod 4$ a designi quell'unico intero dispari tale che esista un altro intero b soddisfacente alla $p = a^2 + b^2$ e sia $p + 1 - 2a \equiv 0 \bmod 8$.

Dimostrazione. Cominciamo con l'osservare che

$$E(q) = \frac{1}{8}\sum_{x\in F_q}\left[1+\left(\frac{x}{q}\right)\right]\left[1+\left(\frac{x+1}{q}\right)\right]\left[1+\left(\frac{x-1}{q}\right)\right] -$$

$$-\frac{1}{8}\sum_{x=0,1,-1}\left[1+\left(\frac{x}{q}\right)\right]\left[1+\left(\frac{x+1}{q}\right)\right]\left[1+\left(\frac{x-1}{q}\right)\right] =$$

$$= \frac{1}{8}\sum_{x\in F_q}\left[1+\left(\frac{x}{q}\right)+\left(\frac{x+1}{q}\right)+\left(\frac{x-1}{q}\right)+\left(\frac{x^2+x}{q}\right)+\right.$$

$$\left.+\left(\frac{x^2-x}{q}\right)+\left(\frac{x^2-1}{q}\right)+\left(\frac{x(x^2-1)}{q}\right)\right] -$$

$$-\frac{1}{8}\left[2\left(1+\left(\frac{-1}{q}\right)\right)+2\left(1+\left(\frac{2}{q}\right)\right)+\right.$$

$$\left.+\left(1+\left(\frac{-2}{q}\right)\right)\left(1+\left(\frac{-1}{q}\right)\right)\right].$$

Ora, come ben noto, si ha

$$\sum_{x\in F_q}\left(\frac{f(x)}{q}\right) = N(q) - q$$

ove $f(x) \in F_q[x]$ è un polinomio di grado positivo senza radici multiple, ed $N(q)$ è il numero dei punti al finito razionali su F_q della curva algebrica (assolutamente irriducibile su F_q) di equazione $y^2 = f(x)$.

Se ne deduce quindi subito che

$$E(q) = \frac{\nu(q) - 3}{8} - \frac{1}{8} C$$

ove $\nu(q)$ designi il numero dei punti al finito razionali su F_q della curva ellittica di equazione $y^2 = x(x^2 - 1)$, e C l'espressione contenuta fra parentesi quadre nel secondo addendo della formula prima fornita per $E(q)$.

Caso $p \equiv -1 \ mod\ 4$, *h dispari.*

In questo caso, che è il più facile, risulta evidentemente $y^2 = x(x^2 - 1)$ isomorfa su F_q a $y^2 = -x(x^2 - 1)$, e -1 è un non quadrato in F_q, sicchè, detto $\bar{\nu}(q)$ il numero dei punti al finito razionali su F_q di quest'ultima curva ellittica, risulta $\nu(q) = \bar{\nu}(q)$ e $(\nu(q) + 1) + (\bar{\nu}(q) + 1) = 2q + 2$ d'onde

$$2\nu(q) + 2 = 2q + 2 \Rightarrow \nu(q) = q,$$

dal che segue la conclusione (essendo in questo caso il carattere quadratico di 2 in F_q dato dalla

$$\left(\frac{2}{q}\right) = \left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8} = (-1)^k).$$

Caso $p \equiv -1 \ mod\ 4$, *h pari.*

Dalla teoria generale delle curve ellittiche su un campo finito, sappiamo che il numero dei punti di una tale curva è uguale a $q + 1 - Tr(\varphi)$ ove φ designi l'endomorfismo di Frobenius relativo ad F_q, e sappiamo che φ soddisfa all'equazione

$$x^2 - (Tr(\varphi))\, x + q = 0.$$

Diciamo ora ψ l'endomorfismo di Frobenius della curva $y^2 = x(x^2 - 1)$ relativo ad F_p. Sappiamo già dal caso precedente che

$$p + 1 - Tr(\psi) = \nu(p) + 1 = p + 1$$

e quindi che $Tr(\psi) = 0$, sicchè $\psi^2 + p = 0$.

Poichè

$$\varphi = \psi^h \quad , \quad \psi^2 = -p \Rightarrow \varphi = (-p)^{h/2},$$

si ha

$$\nu(q) + 1 = q + 1 - Tr(\varphi) = q + 1 - 2(-p)^{h/2}$$

dal che segue la conclusione.

Caso $p \equiv 1$ *mod 4.*

È questo invero il caso più difficile.

Da quanto precedentemente detto si ha che

$$\nu(q) + 1 = q + 1 - (\varphi + \overline{\varphi})$$

(ove $\overline{\varphi}$ designi il coniugato di φ sul campo $\mathbf{Q}$ dei numeri razionali), e $\varphi\,\overline{\varphi} = q$.

Inoltre, poichè ora risulta

$$E(q) = \frac{\nu(q) - 3}{8} - \frac{1}{8}\left[4 + 4\left(1 + \left(\frac{2}{q}\right)\right)\right],$$

ed $E(q)$ è un intero (addirittura pari, come si deduce subito dal fatto che -1 è attualmente un quadrato in F_q), si ha che

$$\nu(q) + 1 \equiv 0 \mod 8\,.$$

Ora, è ben noto che la curva ellittica X di equazione $y^2 = x(x^2 - 1)$ pensata sul campo complesso $\mathbf{C}$ ammette moltiplicazione complessa, e che

$$\mathrm{End}\,(X) \otimes_{\mathbf{Z}} \mathbf{Q} = \mathbf{Q}(i)\,.$$

Presa allora la curva ellittica X_p definita dalla stessa equazione $y^2 = x(x^2 - 1)$ pensata però sul campo $\overline{F}_p$ (chiusura algebrica di F_p), sappiamo che

$$\mathrm{End}\,(X_p) \otimes_{\mathbf{Z}} \mathbf{Q} \supseteq \mathbf{Q}(i), \quad \text{ma anzi} \quad \mathrm{End}\,(X_p) \otimes_{\mathbf{Z}} \mathbf{Q} = \mathbf{Q}(i),$$

poichè dalla teoria generale si sa che il membro di sinistra non può essere più grande (se lo fosse, sarebbe X_p supersingolare, ed il suo numero dei punti razionali su F_p soddisferebbe la ben nota congruenza $\nu(p) + 1 \equiv 1$ mod p, in quanto l'invariante di Hasse di X_p su F_p sarebbe zero; da qui si dedurrebbe $\nu(p) = p$, poichè

$$|\nu(p) + 1 - (p + 1)| \leq 2\sqrt{p}$$

a norma del teorema di Hasse–Weil, e quindi $\nu(p) + 1 = p + 1$, il quale ultimo numero non è però divisibile per 8 nelle attuali ipotesi).

Possiamo allora scrivere, detto come prima ψ l'endomorfismo di Frobenius di X_p relativo ad F_p, $\psi = a + bi$, con a, b interi, e quindi

$$\psi\,\overline{\psi} = p = a^2 + b^2\,.$$

Ora, come ben noto, la suddetta decomposizione del numero p come somma di due quadrati è essenzialmente unica (a meno dell'ordine degli addendi e del loro segno), sicchè la conclusione segue dall'osservare che nell'identità

$$\nu(p) + 1 = p + 1 - \mathrm{Tr}\,(\psi) = p + 1 - 2a$$

il numero a resta univocamente determinato dalla condizione di essere dispari e tale che $p + 1 - 2a \equiv 0 \bmod 8$ (oltre che naturalmente $p - a^2$ quadrato).

Nel caso generale, essendo $\varphi = \psi^h$, si ha subito che

$$\nu(q) + 1 = q + 1 - 2\,\mathrm{Re}\,((a + bi)^h)$$

e sviluppando il binomio nell'ultima espressione si trova subito la formula indicata nella tabella, avuto riguardo come prima al carattere quadratico di 2.

Osserviamo per finire che dalle formule appena dimostrate conseguono subito le seguenti ben note proposizioni (cfr. ad esempio L. Guerra ed E. Ughi, *loc. cit.*; per la seconda anche G. Pellegrino, [3]):

PROPOSIZIONE 1. *Risulta* $\lim_{p\to\infty} \mathrm{E}(q) = \lim_{h\to\infty} \mathrm{E}(q) = +\infty$.

PROPOSIZIONE 2. *Esistono terne di quadrati consecutivi in* F_q *per ogni* $q \geq 19$.

BIBLIOGRAFIA

[1] L. GUERRA e E. UGHI – *On the distribution of Legendre symbols in Galois fields*, « Discrete Mathematics », (in corso di stampa).

[2] E. JACOBSTHAL (1906) – *Anwendung einer Formel aus der Theorie der quadratischen Reste*, « Diss. Univ. Berlin ».

[3] G. PELLEGRINO (1980) – *Sui campi di Galois d'ordine dispari che ammettono terne di elementi quadrati (non quadrati) consecutivi*, « Boll. Un. Mat. It. », *17 B*, 1482–1495.

[4] A. ROBERT (1973) – *Elliptic Curves*, « Lecture Notes in Mathematics », 326.