Atti Accademia Nazionale dei Lincei

Classe Scienze Fisiche Matematiche Naturali

# Rendiconti

Reinaldo E. Giudici

## Residui quadratici in un campo di Galois

*Atti della Accademia Nazionale dei Lincei. Classe di Scienze Fisiche, Matematiche e Naturali. Rendiconti, Serie 8*, Vol. **52** (1972), n.4, p. 461–466.

Accademia Nazionale dei Lincei

<http://www.bdim.eu/item?id=RLINA_1972_8_52_4_461_0>

Atti della Accademia Nazionale dei Lincei. Classe di Scienze Fisiche, Matematiche e Naturali. Rendiconti, Accademia Nazionale dei Lincei, 1972.

**Algebra.** — *Residui quadratici in un campo di Galois* (*). Nota di REINALDO E. GIUDICI presentata (**) dal Socio B. SEGRE.

SUMMARY. — The present paper deals with quadratic residues in a field $GF(p^n)$, where $p$ is an odd prime and $n$ is a positive integer. Some particular results for $n = 3$ are pointed out.

## 1. INTRODUZIONE

Nel presente lavoro si definiscono e si studiano i *residui quadratici* in un campo di Galois di ordine $p^n$, dove $p$ è un numero primo dispari ed $n$ è un intero positivo. Esso costituisce una generalizzazione del lavoro di R. E. Giudici [3], ove vien trattato il caso $n = 2$. Si enunciano inoltre alcuni risultati particolari validi per $n = 3$.

## 2. IL CARATTERE $\chi(\alpha)$. TEOREMA DI EULERO

Sia $GF(p^n)$ il campo di Galois estensione d'ordine $n$ del campo fondamentale di caratteristica $p$, $GF(p)$, con $p$ numero primo maggiore o uguale a 3 ed $n$ intero positivo. Allora, $GF^*(p^n) = GF(p^n) - \{0\}$ risulta notoriamente un gruppo moltiplicativo ciclico d'ordine $p^n - 1$ (cfr. per esempio B. Segre [6, p. 62]). Sia $\lambda_n$ un generatore di $GF^*(p^n)$, cioè un elemento tale che $GF^*(p^n) = \{1, \lambda_n, \lambda_n^2, \cdots, \lambda_n^{p^n-2}\} = [\lambda_n]$. L'elemento $\lambda_1 = \lambda_n^{p^{n-1}+p^{n-2}+\cdots+p+1}$ risulta un generatore di $GF^*(p)$, ossia è, come si dice, una «radice primitiva del numero primo $p$»: invero $\lambda_1^{p-1} = 1$ e $p - 1$ è il più piccolo esponente con questa proprietà, giacché $\lambda_n$ genera $GF^*(p^n)$. Ciò premesso, detta $g$ la più piccola radice primitiva di $p$ (com'è abituale in teoria dei numeri), sarà $\lambda_1 = g^s$ con $s$ tale che $(s, p - 1) = 1$.

DEFINIZIONE 1. Sia $\alpha \in GF^*(p^n)$. Se la congruenza $\eta^2 \equiv \alpha \pmod p$ ammette una soluzione $\eta \in GF^*(p^n)$, si dirà che $\alpha$ è un *residuo quadratico* (r.q.) in $GF^*(p^n)$. Se invece la congruenza anzidetta non ammette soluzione in $GF^*(p^n)$, si dirà che $\alpha$ è un *non residuo quadratico* (n.r.q.) in $GF^*(p^n)$.

DEFINIZIONE 2. Se $\alpha \in GF(p^n)$, denotiamo con $\chi(\alpha)$ il carattere definito da

$$\chi(\alpha) = \begin{cases} +1 & \text{se } \alpha \text{ è un r.q. in } GF^*(p^n), \\ -1 & \text{se } \alpha \text{ è un n.r.q. in } GF^*(p^n), \\ 0 & \text{se } \alpha \notin GF^*(p^n). \end{cases}$$

(*) Lavoro eseguito presso l'Università di Roma, usufruendo di una borsa di studio del Ministero degli Affari Esteri Italiano.

(**) Nella seduta dell'8 aprile 1972.

Il seguente teorema costituisce una generalizzazione del Teorema di Eulero.

TEOREMA 1. $\chi(\alpha) \equiv \alpha^{(p^n-1)/2} \pmod{p}$.

DIMOSTRAZIONE. Se $\alpha = 0$, il teorema è banalmente vero. Se $\alpha \neq 0$, risulta $\alpha \in GF^*(p^n) = [\lambda_n]$. Pertanto $\alpha = \lambda_n^t$ con $0 \leq t \leq p^n - 2$, ed $\alpha$ è un r.q. o un n.r.q. a seconda che $t$ sia pari o dispari. Otteniamo allora

$$\alpha^{(p^n-1)/2} = \lambda_n^{t(p^n-1)/2} = (\lambda_n^{p^{n-1}+p^{n-2}+\cdots+p+1})^{t(p-1)/2} =$$

$$= (g^s)^{t(p-1)/2}, \qquad \text{con} \quad (s, p-1) = 1.$$

Dato che $g^{(p-1)/2} \equiv -1 \pmod{p}$ e che $s$ risulta dispari, si ha $\alpha^{(p^n-1)/2} \equiv (-1)^t \pmod{p}$, ossia $\chi(\alpha) \equiv \alpha^{(p^n-1)/2} \pmod{p}$, come asserito.

COROLLARIO. *Per ogni* $\alpha, \beta \in GF(p^n)$ *si ha* $\chi(\alpha\beta) = \chi(\alpha)\chi(\beta)$, *ossia* $\chi$ *risulta un morfismo fra i gruppoidi moltiplicativi di* $GF(p^n)$ *e di* $GF(3)$.

## 3. DISTRIBUZIONE DEI RESIDUI QUADRATICI IN $GF(p^n)$

Allo scopo di studiare la distribuzione degli elementi che sono r.q. in $GF(p^n)$, consideriamo $GF(p^n)$ come il campo di spezzamento di un polinomio

$$g_n(x) = x^n + a_1 x^{n-1} + \cdots + a_{n-1} x + a_n, \tag{1}$$

irriducibile sopra $GF(p)$ (cfr. ad esempio B. Segre [6, p. 66–67]).

OSSERVAZIONE. Risulta utile ed interessante determinare polinomi di tipo semplificato rispetto alla forma generale (1), che permettano di costruire le varie estensioni di $GF(p)$. Così, per esempio, per l'estensione $GF(p^2)$ si può usare (cfr. R. E. Giudici [3]) il polinomio $g_2(x) = x^2 - g$, con $g$ radice primitiva di $p$. Invece, per $GF(p^3)$ si hanno due casi da distinguere:

I) *Caso* $p \equiv 1 \pmod 6$. Si può usare il polinomio $g_3(x) = x^3 - g$, con $g$ radice primitiva di $p$. In effetti, il polinomio $x^3 - g$ risulta irriducibile in $GF(p)$, perché altrimenti esso ammetterebbe un fattore lineare $x - a$ con $a \in GF(p)$ e quindi con $a \equiv g^e$. Si avrebbe dunque $x^3 - g \equiv (x - g^e)(x^2 + \cdots) \pmod p$, da cui, prendendo $x = g^e$, risulterebbe $g^{3e} - g \equiv 0 \pmod p$, cioè $g^{3e} \equiv g \pmod p$; ma allora, dato che $g$ è radice primitiva di $p$, si otterrebbe $3e \equiv 1 \pmod{p-1}$ e quindi, essendo attualmente $p \equiv 1 \pmod 6$, si giungerebbe all'assurdo $3e \equiv 1 \pmod 3$.

II) *Caso* $p \equiv 5 \pmod 6$. È ben noto (cfr. H. Hasse [4, p. 171, 172]) che ogni elemento di $GF(p)$ è attualmente un cubo perfetto, cosicché, per costruire l'estensione $GF(p^3)$, non si può usare un polinomio del tipo $x^3 - a$ con $a \in GF(p)$. In questo caso è però possibile assumere, come polinomio irriducibile, un polinomio del tipo $x^3 - 3x - 2u$, in cui $u$ soddisfi alla relazione $\lambda_2 = u + v\mathrm{L}$, dove $\lambda_2$ è un generatore del campo $GF(p^2)$ di norma 1 e L è uno zero del polinomio $x^2 - g$ che definisce $GF(p^2)$. Si noti che l'elemento $u$ può assumere $(p+1)/3$ valori. Questi risultati possono venire ottenuti a partire da un teorema di L. E. Dickson [2, p. 2].

Tornando al caso generale del polinomio (1), sia $\theta \in GF^*(p^n)$ una qualunque delle $n$ radici dell'equazione $g_n(x) = 0$. Ne viene che $GF(p^n) = GF(p)(\theta)$ e si può porre

$$(2) \qquad GF(p^n) = \{ b_0 + b_1\theta + b_2\theta^2 + \cdots + b_{n-1}\theta^{n-1} \mid b_i \in GF(p) \}.$$

È ben noto che, se $\theta$ è una radice di $g_n(x)$, le altre radici sono $\theta^p, \theta^{p^2}, \cdots, \theta^{p^{n-1}}$ (cfr. ad esempio B. Segre [6, 72]). Per questo motivo, se $\alpha \in GF(p^n)$, gli elementi $\alpha^p, \alpha^{p^2}, \cdots, \alpha^{p^{n-1}}$ si chiamano i *coniugati* di $\alpha$; e si chiamerà *norma* di $\alpha$ l'elemento – manifestamente di $GF(p)$ – definito da

$$(3) \qquad N(\alpha) = \prod_{i=0}^{n-1} \alpha^{p^i}.$$

Il seguente teorema consente di esprimere il carattere $\chi(\alpha)$, in funzione del ben noto *simbolo di Legendre* $(\,|\,p)$.

TEOREMA 2. $\chi(\alpha) = (N(\alpha)\,|\,p)$.

DIMOSTRAZIONE.

$$\chi(\alpha) \equiv \alpha^{(p^n-1)/2} = (\alpha^{(1+p+p^2+\cdots+p^{n-1})})^{(p-1)/2} = \left(\prod_{i=0}^{n-1} \alpha^{p^i}\right)^{(p-1)/2} \equiv$$

$$\equiv (N(\alpha))^{(p-1)/2} \equiv (N(\alpha)\,|\,p),$$

conformemente al Teorema di Eulero.

Per studiare la distribuzione dei r.q. di $GF(p^n)$, risulta utile rappresentare l'insieme $GF(p^n)$ come un sottoinsieme dello spazio euclideo reale di dimensione $n$, $\mathbf{R}^n$, nel modo seguente. In primo luogo, conveniamo di rappresentare gli elementi $\alpha$ di $GF(p^n) = GF(p)(\theta)$ – anziché nella forma (2) – nella forma canonica

$$(4) \qquad \alpha = b_0 + b_1\theta + \cdots + b_{n-1}\theta^{n-1},$$

con $\qquad b_j \in \mathbf{Z} \quad , \quad |b_j| \leq (p-1)/2 \qquad (0 \leq j \leq n-1).$

Dette allora $(X_0, X_1, \cdots, X_{n-1})$ le coordinate di punto in $\mathbf{R}^n$, deponiamo l'elemento (4) nel punto $(b_0, b_1, \cdots b_{n-1})$ di $\mathbf{R}^n$. In tal modo gli elementi di $GF(p^n)$ sono situati nei punti a coordinate intere dell'ipercubo di dimensione $n$, di centro l'origine, di assi gli assi delle coordinate e con spigolo di lunghezza $p-1$.

Il seguente teorema consente di determinare il carattere quadratico degli elementi che sono situati sull'asse $X_i$, cioè degli elementi (4) della forma

$$b\theta^k \qquad (b \in \mathbf{Z}\,,\ |b| \leq (p-1)/2\,,\ 0 \leq k \leq n-1).$$

TEOREMA 3. *Sia* $b \in \mathrm{GF}^*(p)$ *e sia* $\theta$ *una radice in* $\mathrm{GF}(p^n)$ *del polinomio* $g_n(x) = x^n + a_1 x^{n-1} + \cdots + a_n$ *irriducibile su* $\mathrm{GF}(p)$. *Allora*

(i) $$\chi(b) = \begin{cases} 1 & \text{se } n \text{ è pari,} \\ (b \mid p) & \text{se } n \text{ è dispari.} \end{cases}$$

(ii) $$\underset{1 \le k \le n-1}{\chi(b\theta^k)} = \begin{cases} (a_n \mid p)^k & \text{se } n \text{ è pari,} \\ (b \mid p)\,(-a_n \mid p)^k & \text{se } n \text{ è dispari.} \end{cases}$$

DIMOSTRAZIONE. (i) Usando il teorema 2, si ottiene:

$$\chi(b) = (\mathrm{N}(b) \mid p) = \left(\prod_{i=0}^{n-1} b^{p^i} \mid p\right) = \left(\prod_{i=0}^{n-1} b \mid p\right),$$

dal momento che $b^{p^i} \equiv b \pmod p$, ossia

$$\chi(b) = (b^n \mid p) = (b \mid p)^n .$$

(ii) Poiché $\chi$ è un omomorfismo dal gruppo moltiplicativo $\mathrm{GF}^*(p^n)$ su $\mathrm{GF}^*(3)$, si ha

$$\chi(b\theta^k) = \chi(b)\,\chi(\theta)^k = (b \mid p)^n\,(\mathrm{N}(\theta) \mid p)^k , \qquad 1 \le k \le n-1 .$$

Ma (cfr. S. Lang [5, p. 132]),

$$\mathrm{N}(\theta) = \prod_{i=0}^{n-1} \theta^{p^i} = (-1)^n a_n ,$$

e pertanto

$$\chi(b\theta^k) = (b \mid p)^n\,((-1)^n a_n \mid p)^k , \qquad 1 \le k \le n-1 .$$

Come conseguenza del teorema 3, si può dire che, *quando k è pari*, il carattere quadratico sull'asse $\mathrm{X}_k$ è il seguente: *se n è pari*, tutti gli elementi dell'asse $\mathrm{X}_k$ sono r.q.; invece, se *n è dispari* il carattere quadratico di $bx^k$ uguaglia quello di $b$, ossia dipende dalla scelta di $b$ e cioè dalla posizione del punto $b\theta^k$ sull'asse $\mathrm{X}_k$: in questo caso, poiché $b$ appartiene a $\mathrm{GF}^*(p)$, si ottiene una distribuzione in $(p-1)/2$ r.q. e $(p-1)/2$ r.n.q. quando si prescinda dal punto origine.

*Se k è dispari*, il carattere quadratico degli elementi $b\theta^k$ sull'asse $\mathrm{X}_k$ è il seguente: *se n è pari*, esso uguaglia quello del termine noto $a_n$, mentre *se n è dispari*, esso uguaglia quello del prodotto $-ba_n$. Quest'ultimo risultato mostra, fra l'altro, l'importanza di determinare il coefficiente $a_n$ nel polinomio irriducibile che dà origine all'estensione $\mathrm{GF}(p^n)$ di $\mathrm{GF}(p)$.

Nel caso particolare $n = 2$, la distribuzione sugli assi dei r.q., indicata dal teorema 3, dà luogo al lemma 1 di R. E. Giudici [3]: gli elementi dell'asse $\mathrm{X}_0 = \mathrm{X}$ sono sempre r.q., mentre gli elementi dell'asse $\mathrm{X}_1 = \mathrm{Y}$ risultano r.q. se $p \equiv 3 \pmod 4$ e r.n.q. se $p \equiv 1 \pmod 4$.

Per $n = 3$, si ottiene il risultato seguente: gli elementi degli assi $X_0 = X$, $X_2 = Z$ hanno il medesimo carattere quadratico, che dipende dal simbolo di Legendre: $\chi(b) = \chi(b\theta^2) = (b\,|\,p)$.

Sull'asse $X_1 = Y$ la situazione è più complessa, e dipende dal termine costante del polinomio $x^3 + a_2 x + a_3$ irriducibile su $GF(p)$. La situazione è ottenuta specificando nei vari casi $\chi(b\theta)$, che risulta essere:

$$\chi(b\theta) = \begin{cases} -(b\,|\,p) & \text{se } p \equiv 1 \pmod{12}, \\ (ba_3\,|\,p) & \text{se } p \equiv 5 \pmod{12}, \\ -(b\,|\,p) & \text{se } p \equiv 7 \pmod{12}, \\ -(ba_3\,|\,p) & \text{se } p \equiv 11 \pmod{12}. \end{cases}$$

Il seguente teorema caratterizza quando i r.q. risultano distribuiti simmetricamente rispetto all'origine.

TEOREMA 4. *Sia* $\alpha \in GF(p^n)$. *Allora*

$$\chi(\alpha) = \begin{cases} \chi(-\alpha) & \textit{se } n \textit{ è pari}, \\ \chi(-\alpha) & \textit{se } n \textit{ è dispari e } p \equiv 1 \pmod 4, \\ -\chi(-\alpha) & \textit{se } n \textit{ è dispari e } p \equiv 3 \pmod 4. \end{cases}$$

DIMOSTRAZIONE. Poiché $\alpha = (-1)(-\alpha)$, $\chi(\alpha) = \chi(-1)\chi(-\alpha)$. Usando il teor. 2, si trova $\chi(-1) = (N(-1)\,|\,p) = ((-1)^n\,|\,p)$. Pertanto, quando $n$ è pari, si ha sempre simmetria rispetto all'origine; quando $n$ è dispari, si ha simmetria o antisimmetria rispetto all'origine, a seconda del carattere quadratico di $-1$ in $GF(p)$.

Il carattere quadratico dell'elemento $-1$ si può anche determinare in termini di $q = p^n$, come indicato ad esempio in S. Bruno e G. Tallini [1, p. 55, Prop. I.XIII].

TEOREMA 5. *Sia* $\alpha \in GF^*(p^n)$ *e siano* $\alpha^{p^k}$, $1 \le k \le n-1$ *i coniugati di* $\alpha$. *Allora* $\chi(\alpha^{p^k}) = \chi(\alpha)$.

DIMOSTRAZIONE.

$$\chi(\alpha^{p^k}) = (N(\alpha^{p^k})\,|\,p) = (N(\alpha)^{p^k}\,|\,p), \qquad 1 \le k \le n-1.$$

Ma $N(\alpha) \in GF(p)$, quindi $N(\alpha)^{p^k} \equiv N(\alpha) \pmod p$, ossia

$$\chi(\alpha^{p^k}) = (N(\alpha)\,|\,p) = \chi(\alpha).$$

Il seguente corollario mostra che, se $\alpha \neq 0$, il carattere $\chi(\alpha)$ è radice $(p^n - 1)$ - ma dell'unità.

COROLLARIO. $\chi(\alpha)$ *soddisfa all'equazione* $X^{p^n} - X = 0$.

DIMOSTRAZIONE. Dal teor. 5, $\chi(\alpha^{p^n}) = \chi(\alpha)$, si deduce che $\chi(\alpha^{p^n}) = \chi(\alpha)^{p^n}$, in virtù del corollario del teor. 1. Pertanto $\chi(\alpha)^{p^n} = \chi(\alpha)$.

Il teorema 5 risulta utile per lo studio della distribuzione dei r.q. sugli *n iperpiani fondamentali*, ossia su quelli di equazione $X_i = 0$ $(i = 0, 1, \cdots, n-1)$, e sugli $n(n-1)$ *iperpiani diagonali*, ossia su quelli di equazione $X_i \pm X_j = 0$ $(i \neq j\,,\ i\,,\ j = 0\,,\ 1\,,\ \cdots\,,\ n-1)$. Tale studio trovasi effettuato, nel caso $n = 2$, in R. E. Giudici [3, Teor. 2 e Teor. 4]. Per $n = 3$ l'Autore ha trovato per altra via, utilizzando il teor. 5, che tanto ciascun piano fondamentale quanto ciascun piano diagonale contiene $(p^2 - 1)/2$ elementi r.q. e $(p^2 - 1)/2$ elementi n.r.q., ove si escluda l'origine.

L'Autore esprime la propria gratitudine al prof. Beniamino Segre per la guida fornitagli nella stesura del presente lavoro ed al dott. P. V. Ceccherini per la revisione dell'italiano.

## Bibliografia

[1] S. Bruno e G. Tallini, *Geometria iperbolica in un piano di Galois* $S_{2,q}$ *con q dispari*, « Ricerche di Matematica », *19*, 48–78 (1970).
[2] L. E. Dickson, *Criteria for the irreducibility of functions in a finite field*, « Bull. Am. Math. Soc. », *12*, 1–8 (1906).
[3] R. E. Giudici, *Quadratic residues in* GF $(p^2)$, « Math. Mag. », *44*, 153–157 (1971).
[4] H. Hasse, *Vorlesungen über Zahlentheorie*, New York, Springer Verlag, 1964,2a.
[5] S. Lang, *Algebra*, New York, Addison Wesley, 1967.
[6] B. Segre, *Lezioni di geometria moderna*, Vol. I, Bologna, Zanichelli, 1948.