Numero massimo di punti razionali di curve di genere 3 su campi finiti

Elena Berardini

27 giugno 2016

Sintesi

Il numero di punti razionali di una curva C (algebrica, proiettiva, assolutamente irriducibile, liscia) di genere g definita sul campo finito $\mathbb{F}_q$, che verrà denotato $\#C(\mathbb{F}_q)$, è limitato in modulo dalla disuguaglianza di Weil ([23]) migliorata da Jean-Pierre Serre ([12]):

$$|\#C(\mathbb{F}_q) - (q+1)| \leq g\lfloor 2\sqrt{q} \rfloor$$

dove $\lfloor r \rfloor$ per $r \in \mathbb{R}$ è il più grande intero più piccolo di r.
Le curve il cui numero di punti razionali è uguale all'estremo superiore della disuguaglianza sopracitata, chiamata tradizionalmente disuguaglianza di Serre-Weil, vengono chiamate Serre-Weil massimali; le curve il cui numero di punti è vicino all'estremo superiore della disuguaglianza di Serre-Weil sono chiamate quasi-Serre-Weil massimali. Queste curve sono utilizzate, ad esempio, nella costruzione di codici correttori (codici di Goppa e codici Algebrici Geometrici, cfr.[19]) e in alcuni protocolli crittografici.
Definiamo la quantità $N_q(g)$ come il numero massimo di punti razionali che una curva algebrica, proiettiva, assolutamente irriducibile, liscia e di genere g, può avere su $\mathbb{F}_q$. Possiamo considerare questa quantità da due punti di vista diversi: fissando q, il cardinale del campo finito $\mathbb{F}_q$, e studiando questa quantità in funzione di g, o viceversa, fissando il genere g e studiando il valore di $N_q(g)$ al variare di q; in questa tesi è stato adottato quest'ultimo approccio.
Per $g = 1$, la quantità $N_q(g)$ è stata determinata da Deuring ([4]) e Waterhouse ([22]), e per $g = 2$ è stata determinata da Serre ([12]); se $g \geq 3$, trovare $N_q(g)$ diventa un problema difficile. In questa tesi ci interessiamo al caso $g = 3$ partendo dall'articolo di Roland Auer e Jaap Top «Some genus 3 curves with many points» ([2]).

La struttura della tesi è la seguente: nel Capitolo 1 viene fissata la notazione e vengono introdotte le nozioni di base sulle curve su un campo finito; vengono inoltre presentati alcuni risultati generali sulle curve e gli strumenti

che saranno utilizzati in tutta la trattazione.
Lo scopo del Capitolo 2 è quello di riassumere il lavoro già svolto sulle curve di genere 1 e 2, basandosi sulla tesi di Waterhouse ([22]) per il caso delle curve di genere 1 e sulla tesi di Shabat ([13]) per le curve di genere 2. Da questo secondo capitolo emergono due metodi interessanti: da un lato la discesa di Galois come metodo di prova di non esistenza di curve Serre-Weil massimali in alcuni campi finiti, dall'altro l'utilizzo delle curve ellittiche, i.e. curve di genere 1, per trovare curve di genere più grande con molti punti razionali; questi due metodi vengono ripresi nello studio delle curve di genere 3.
L'enunciato fondamentale di questo capitolo, che viene richiamato in tutta la trattazione, è la seguente proposizione che discende direttamente dal Teorema di Deuring:

Proposizione 1. *Sia $q = p^a$ e $m = \lfloor 2\sqrt{q} \rfloor$. Se a è dispari, $a \geq 3$ e p divide m allora $N_q(1) = q + 1 + m - 1$, altrimenti $N_q(1) = q + 1 + m$.*

Tale proposizione definisce esattamente qual è il numero massimo di punti razionali che una curva di genere 1 può avere su un campo finito, e quindi, in particolare, ci dice sotto quali condizioni è possibile trovare una curva ellittica Serre-Weil massimale.
Il Capitolo 3 è il cuore della tesi: qui vengono affrontate le curve lisce di genere 3 basandosi su un articolo di Auer e Top del 2002 ([2]) e su un articolo di Top del 2003 ([17]). Utilizzando un'isogenia tra la jacobiana di una particolare famiglia di quartiche piane, C_λ, e il triplo prodotto di una famiglia di curve ellittiche, $E_\lambda^{(\lambda+3)}$, otteniamo il seguente risultato che mette in relazione il numero di punti razionali della quartica e della curva ellittica:

Corollario 1. *Sia $q = p^e$ una potenza di un primo dispari e $\lambda \in \mathbb{F}_q \setminus \{-3, 0, 1\}$. Allora:*

$$\#C_\lambda(\mathbb{F}_q) = 3\#E_\lambda^{(\lambda+3)} - 2q - 2.$$

Grazie a questo risultato è possibile costruire curve lisce di genere 3 definite su un campo finito che siano Serre-Weil massimali o quasi-Serre-Weil massimali.
In caratteristica 3 la curva ellittica $E_\lambda^{(\lambda+3)}$ é equivalente alla curva $E_\lambda^{(\lambda)}$, la quale è isomorfa ad una curva ellittica in forma di Legendre, denotata E_μ. Partendo da questa osservazione, nella prima parte del capitolo, viene sviluppata la teoria delle curve ellittiche in forma di Legendre, per arrivare, nel caso dei campi finiti di caratteristica 3, ad un risultato generale dimostrato da Auer e Top in [2] e che è stato personalmente migliorato nella tesi:

Teorema 1. *Sia* $3^n + 1 + \lfloor 2\sqrt{3^n} \rfloor = N + r$, $N \in 4\mathbb{Z}$ *e* $0 \leq r \leq 3$. *Per tutti gli* $n \geq 1$ *abbiamo le seguenti disuguaglianze:*

$$3^n + 1 + 3\lfloor 2\sqrt{3^n} \rfloor - N_{3^n}(3) \leq \begin{cases} 0 & \text{se } n \equiv 2 \bmod 4 \\ 12 & \text{se } n \equiv 0 \bmod 4 \\ 21 & \text{se } n \equiv 1 \bmod 2 \text{ e } N \equiv 1 \bmod 3 \\ 9 & \text{se } n \equiv 1 \bmod 2 \text{ e } N \not\equiv 1 \bmod 3 \end{cases}$$

L'idea della dimostrazione è la seguente: utilizzando il corollario del Teorema di Deuring per le curve di genere 1, si mostra l'esistenza di una curva ellittica con il più gran numero possibile di punti razionali che sia anche un multiplo di 4 (ovvero compatibile con il numero di punti razionali di una curva ellittica in forma di Legendre); utilizzando la teoria delle curve di Legendre si mostra che tale curva ellittica è, in caratteristica 3, isogena ad una curva di Legendre, ovvero a $E_\lambda^{(\lambda)} \cong E_\mu$; infine, applicando il Corollario 1, si ottiene l'esistenza di una curva liscia di genere 3 nella famiglia C_λ, definita su $\mathbb{F}_{3^n}$, e con $3\#E_\mu(\mathbb{F}_{3^n}) - 2q - 2$ punti razionali.
Nella tesi la prova di questo teorema, presentato per la prima volta in [2], viene sviluppata in ogni dettaglio; inoltre, considerando anche il caso $N \not\equiv 1 \bmod 3$, viene proposta una stima più fine nel caso in cui n è dispari.
Sempre nel Capitolo 3, come in [2], viene mostrata l'esistenza di curve Serre-Weil massimali su $\mathbb{F}_{p^{2n}}$ nel caso in cui n è dispari e $p \equiv 3 \bmod 4$ e viene dato un metodo effettivo per trovare esplicitamente delle curve Serre-Weil massimali su $\mathbb{F}_p$ utilizzando la teoria sviluppata nel capitolo.
L'ultima sezione del capitolo è dedicata ad una proposizione presentata da Top in [17] che esplicita la quantità $N_q(3)$ per dei piccoli valori di q. Il lavoro di Top si ferma a $q = 97$ e in questa tesi si è cercato di andare più avanti ($q \leq 125$). In particolare i valori $N_{103}(3)$ e $N_{107}(3)$, trovati grazie ai metodi sviluppati nella tesi, non appaiono in *Table of Curves with Many Points* ([20]), il sito che raccoglie i valori noti per la quantità $N_q(g)$.

Proposizione 2. *Sia* $q \leq 125$. *La quantità* $N_q(3)$ *assume i seguenti valori:*

q	2	3	4	5	7	8	9
$N_q(3)$	7	10	14	16	20	24	28
q	11	13	16	17	19	23	25
$N_q(3)$	28	32	38	40	44	48	56
q	27	29	31	32	37	41	43
$N_q(3)$	56	60	62	64	72	78	80
q	47	49	53	59	61	64	67
$N_q(3)$	87	92	96	102	107	113	116
q	71	73	79	81	83	89	97
$N_q(3)$	120	122	131	136	136	144	155
q	101	103	107	109	113	121	125
$N_q(3)$	≤ 160	164	168	≤ 170	≤ 174	188	192

Nella tesi la proposizione non viene interamente dimostrata, ma viene presa come spunto per presentare la teoria di Stöhr e Voloch sulle curve Frobenius non-classiche, una classe di curve che hanno la caratteristica di avere, in generale, molti punti razionali.

Riferimenti bibliografici

[1] R. Auer e J. Top. «Legendre elliptic curves over finite fields». In: *Journal of Number Theory* 95.2 (2002), pp. 303–312.

[2] R. Auer e J. Top. «Some genus 3 curves with many points». In: *Algorithmic number theory (Sydney, 2002)*. Vol. 2369. Lecture Notes in Comput. Sci. Springer, Berlin, 2002, pp. 163–171.

[3] H. Borges e M. Homma. «Points on singular Frobenius nonclassical curves». Preprint. 2015.

[4] M. Deuring. «Die Typen der Multiplikatorenringe elliptischer Funktionenkörper». In: *Abh. Math. Sem. Univ. Hamburg* 14.1 (1941), pp. 197–272.

[5] R. Hartshorne. *Algebraic Geometry*. Graduate Texts in Mathematics, No. 52. Springer-Verlag, New York-Heidelberg, 1977.

[6] A. Hefez e J. F. Voloch. «Frobenius non classical curves». In: *Archiv der Mathematik* 54.3 (1990), pp. 263–273.

[7] K. Lauter. «The maximum or minimum number of rational points on genus three curves over finite fields». In: *Compositio Math.* 134.1 (2002). With an appendix by Jean-Pierre Serre, pp. 87–111.

[8] F. Oort e K. Ueno. «Principally polarized abelian varieties of dimension two or three are Jacobian varieties». In: *Journal of the Faculty of Science. University of Tokyo. Section IA. Mathematics* 20 (1973), pp. 377–381.

[9] C. Ritzenthaler. «Optimal curves of genus 1, 2 and 3». In: *Actes de la Conférence "Théorie des Nombres et Applications"*. Publ. Math. Besançon Algèbre Théorie Nr. Presses Univ. Franche-Comté, Besançon, 2011, pp. 99–117.

[10] J.-P. Serre. *Rational points on curves over finite fields*. Lectures given at Harvard University, Notes by F.Q. Gouvêa. Springer-Verlag, New-York-Heidelberg, 1985.

[11] J.-P. Serre. «Résumé des cours de 1983-1984». In: *Jean-Pierre Serre, Œuvres, Collected Papers*. Vol. 3. Springer-Verlag, New York, 1985.

[12] J.-P. Serre. «Sur le nombre des points rationnels d'une courbe algébrique sur un corps fini». In: *C. R. Acad. Sci. Paris Sér. I Math.* 296.9 (1983), pp. 397–402.

[13] G. V. Shabat. «Curves with many points». Tesi di dott. Amsterdam, 2001.

[14] J. H. Silverman. *The arithmetic of elliptic curves*. Vol. 106. Graduate Texts in Mathematics. Springer-Verlag, New York, 1986.

[15] J. H. Silverman e J. Tate. *Rational points on elliptic curves*. Undergraduate Texts in Mathematics. Springer-Verlag, New-York, 1992.

[16] K.-O. Stöhr e F. Voloch. «Weiestrass points and curves over finite fields». In: *Proc. London Math. Soc. (3)* 52.1 (1986), pp. 1–19.

[17] J. Top. «Curves of genus 3 over small finite fields». In: *Indag. Math. (N.S.)* 14.2 (2003), pp. 275–283.

[18] J. Top. «Hecke L-series related with algebraic cycles or with Siegel modular form». Tesi di dott. Utrecht, 1969.

[19] M. Tsfasman, S. Vladuts e D. Nogin. *Algebraic Geometric Codes: Basic Notions, Vol. 139*. Mathematical Surveys and Monographs. American Mathematical Society, Providence, 2007.

[20] G. van der Geer et al. *Tables of Curves with Many Points*. 2009, Retrieved [2016]. URL: http://www.manypoints.org.

[21] L. C. Washington. *Elliptic curves*. Second. Discrete Mathematics and its Applications (Boca Raton). Number theory and cryptography. Chapman & Hall/CRC, Boca Raton, FL, 2008.

[22] W. C. Waterhouse. *Abelian varieties over finite fields*. Thesis (Ph.D.)–Harvard University. ProQuest LLC, Ann Arbor, MI, 1968.

[23] A. Weil. *Variétés abéliennes et courbes algébriques*. Actualités Sci. Ind., no. 1064 = Publ. Inst. Math. Univ. Strasbourg 8 (1946). Hermann & Cie., Paris, 1948, p. 165.