UNIVERSITÀ DEGLI STUDI DI ROMA TRE
FACOLTÀ DI SCIENZE M.F.N.

Alcuni risultati sulla teoria dei Campi Finiti

Sintesi della tesi di Laurea in Matematica
di Alessandro Conflitti
Relatore: Francesco Pappalardi Co-relatore: Igor Shparlinski

I Campi Finiti, la cui teoria si è sviluppata principalmente negli ultimi 50 anni, vengono usati sia in matematica pura che in quella applicata, per esempio in algebra, teoria dei numeri e geometria algebrica, ed anche in informatica, calcolo simbolico, teoria algebrica dei codici e criptografia.
Lo scopo di questa Tesi è di fornire una rassegna delle proprietà fondamentali e di approfondire alcuni problemi dimostrando dei risultati originali.

Iniziamo il primo Capitolo, dedicato ai risultati classici della teoria, con lo studio della struttura dei campi finiti dimostrando che ogni campo finito ha sempre cardinalità uguale alla potenza di un numero primo e che due campi finiti aventi la stessa cardinalità sono isomorfi. Inoltre mostriamo come costruire un campo di cardinalità fissata e si forniscono esempi pratici. In seguito studiamo il gruppo moltiplicativo di un campo finito, che è ciclico, dimostriamo il teorema di Wedderburn[1] che afferma che ogni corpo finito è un campo e studiamo la struttura dei sottocampi di un campo finito ed il gruppo di Galois di un'estensione. Presentiamo inoltre formule per il numero

[1] 'A Theorem of Finite Algebras', *Transactions of the American Mathematical Society* v. 6 (1905), pagg. 349–352.

di elementi aventi ordine fissato, per il numero di polinomi irriducibili di un dato grado e per il numero dei polinomi primitivi e studiamo alcune proprietà dei polinomi su un campo finito e delle loro radici.
Nell'ultimo paragrafo si espongono alcuni risultati classici relativi alle equazioni sui Campi Finiti, come ad esempio il Teorema di Chevalley-Warning. Uno dei suoi Corollari è la proprietà che ogni elemento di un campo finito può essere espresso come somma di due quadrati.
Abbiamo scelto di includere molti esempi per rendere più chiara la trattazione ed illustrare le applicazioni della teoria.

Il secondo Capitolo contiene risultati originali; gli argomenti trattati sono stati elaborati durante una visita a Roma di Igor Shparlinski. Vengono definite le nozioni standard di Teoria Algoritmica e Computazionale dei Numeri e si dà una panoramica di tutti i risultati finora ottenuti nell'esame del problema di *esibire un algoritmo efficiente per la costruzione di elementi primitivi o di ordine elevato in un campo finito* $\mathbb{F}_q$.
Prendendo spunto da un articolo di S. Gao [Gao] generalizziamo e miglioriamo il suo risultato. Nell'articolo citato viene provato il seguente

Teorema 0.1 (Gao). *Sia* $g(X) \in \mathbb{F}_q[X]$ *tale che* $g(X)$ *non è della forma* $aX^k \quad o \quad aX^{p^l} + b \quad (a, b \in \mathbb{F}_q,\ k, l \geq 0,\ p = \mathrm{ch}\,(\mathbb{F}_q))$.
Sia $\alpha \in \mathbb{F}_{q^n}$ *tale che*

1. α *ha grado* n *su* $\mathbb{F}_q$;
2. *esiste* $q^s \geq \deg(g)$ *tale che* $\alpha^{q^s} = g(\alpha)$;
3. $2 \leq \deg\left(g(X)\right) \leq 2\log_q n$.

Allora

$$\mathrm{ord}(\alpha) \geq n^{\frac{log_q n}{4\log_q(2\log_q n)} - \frac{1}{2}}.$$

Nel secondo paragrafo del Capitolo 2 dimostriamo il seguente risultato che apparirà in [CNS].

Teorema 0.2 (Conflitti-Shparlinski). *Sia* $g(X) \in \mathbb{F}_q[X]$ *come nell'enunciato del Teorema 0.1, sia* $d = \deg(g)$ *e sia* $\alpha \in \mathbb{F}_{q^n}$ *tale che*

1. *α ha grado n su $\mathbb{F}_q$;*

2. *esiste $q^s \geq \deg(g)$ tale che $\alpha^{q^s} = g(\alpha)$.*

Allora

$$\operatorname{ord}(\alpha) \geq \left(\frac{nd}{\log_d^2 n}\right)^{\frac{1}{2}\log_d n - \frac{1}{2}}.$$

Ponendo $d \sim 2\log_q n$ nel Teorema 0.2 si ottiene una sottostima che è circa il quadrato di quella dell'articolo di S. Gao [Gao].

Nel terzo Capitolo dimostriamo che se si scelgono m polinomi random a coefficienti su $\mathbb{F}_q$ allora la probabilità che siano coprimi è $1 - \frac{1}{q^{m-1}}$.
Questo risultato che è noto agli esperti del settore anche se non ci risulta che apparire in letteratura, è una motivazione ai risultati del capitolo successivo che è stato sviluppato e scritto durante la permanenza del candidato presso il Departement of Computing della Macquarie University, Sydney, Australia, come visitatore di Igor Shparlinski ed apparirà in [CS].
Viene proposto un algoritmo probabilistico per ridurre il calcolo del massimo comun divisore di m polinomi su un campo finito $\mathbb{F}_q$ (che richiede il calcolo di $m-1$ massimi comun divisori di coppie di polinomi) al calcolo del massimo comun divisore di un'unica coppia di polinomi. Tale algoritmo è utile ad esempio nelle situazioni in cui m è grande ripetto a q o al grado dei polinomi. Seguendo l'idea dell'articolo Cooperman, Feisel, von zur Gathen e Havas [CFGH] che considera il problema analogo in $\mathbb{Z}$ al posto di $\mathbb{F}_q[X]$, proveremo il seguente

Teorema 0.3 (Conflitti-Shparlinski). *Siano $a_1, \ldots, a_m \in \mathbb{F}_q[X]$ e*

$$\gamma(q) = \sum_{k=1}^{\infty} I_k q^{-2k}$$

dove I_k è il numero di polinomi monici irriducibili di grado k.
Dato un intero $s \geq 1$, scelti in modo random $u_1, \ldots, u_m, v_1, \ldots, v_m \in \mathbb{F}_q[X]$ monici di grado s, sia P la probabilità che

$$\operatorname{MCD}\left(\sum_{j=1}^{m} u_j a_j, \sum_{j=1}^{m} v_j a_j\right) = \operatorname{MCD}(a_1, \ldots, a_m).$$

Allora

$$P \geq 1 - \gamma(q) - \frac{n+s+4}{s} q^{-s}$$

dove $n = \max_{1 \leq j \leq m}\{deg(a_j)\}$.
In particolare, se $s \geq \log_q n$ *si ottiene* $P \geq 1 - \gamma(q) - O(s^{-1})$.
Inoltre

$$\gamma(q) \leq \log\left(\frac{q}{q-1}\right).$$

Osserviamo che esiste un altro algoritmo probabilistico per ridurre il calcolo del massimo comun divisore di molti polinomi al calcolo del massimo comun divisore di una coppia di polinomi (cfr. Sezione 6.9 di von zur Gathen e Gerhard [vzGG] oppure [CFGH]) valido per polinomi in $\mathbb{K}[X]$, dove $\mathbb{K}$ è un campo generico. Nel caso dei campi finiti $\mathbb{F}_q$, se q è piccolo rispetto ad n il secondo algoritmo richiede il calcolo del massimo comun divisore su un'appropriata estensione del campo base $\mathbb{F}_q$. La realizzazione di questa estensione necessita di un polinomio irriducibile di dato grado la cui determinazione potrebbe richiedere un elevato costo computazionale; in questa circostanza il secondo algoritmo è inefficiente.
Presentiamo un dettagliato confronto di entrambi gli algoritmi. In particolare proviamo che se si utilizzano l'implementazione rapida delle operazioni aritmetiche di $\mathbb{F}_{q^r}$ tramite l'aritmetica di $\mathbb{F}_q$ e l'algoritmo euclideo rapido per calcolare il massimo comun divisore di due polinomi, allora il nostro algoritmo esibisce un miglior comportamento asintotico per $m = o(\log^2 n \log\log n)$ (dove si usano le notazioni del Teorema 0.3).
Se invece si utilizza l'aritmetica classica, che è probabilmente il caso di molte implementazioni pratiche, allora il nostro algoritmo esibisce un miglior comportamento asintotico per valori $m = O(n \log n)$.

Nel quinto Capitolo esporremo la teoria dei polinomi di permutazione (PP) su $\mathbb{F}_q$, cioè dei polinomi in $\mathbb{F}_q[X]$ che, come applicazioni da un campo finito in se stesso, rappresentano una permutazione degli elementi di $\mathbb{F}_q$.
Lo studio di questi oggetti non ha solo rilevanza teorica, ma anche applicazioni pratiche, per esempio in criptografia; a tale proposito si veda J. V. Brawley e J. Levine [BL].
Nel primo paragrafo, seguendo le trattazioni in R. Lidl e H. Niederreiter [LN],

G. L. Mullen [Mul1] e C. Wells [Wel1], illustriamo la teoria generale dei polinomi di permutazione e forniamo criteri per cui un generico polinomio sia un polinomio di permutazione.
Studiamo inoltre (cfr. l'articolo di L. Carlitz [Car]) delle condizioni per cui un polinomio di permutazione su $\mathbb{F}_q$ sia anche un polinomio di permutazione per un estensione $\mathbb{F}_{q^r}$ di $\mathbb{F}_q$.
Il secondo paragrafo è dedicato allo studio di un'importante classe di polinomi di permutazione, i polinomi di Dickson. Qui esponiamo i recenti risultati di G. L. Mullen in [Mul2] relativi ai polinomi di Dickson nelle variabili matriciali a coefficienti in $\mathbb{F}_q$.

Il sesto Capitolo è ispirato al seguente risultato di C. Wells [Wel2]

Teorema 0.4 (Wells). *Sia $N(q,r)$ il numero delle permutazioni su $\mathbb{F}_q$ che muovono r elementi ed hanno grado non massimale.*
Allora $N(q,2) = 0$ e

$$N(q,3) = \begin{cases} 0 & \text{se } q \equiv 2 \pmod 3; \\ \frac{2}{3}q(q-1) & \text{se } q \equiv 1 \pmod 3; \\ \frac{1}{3}q(q-1) & \text{se } 3 \mid q. \end{cases}$$

Seguendo le idee in [MP] esponiamo un approccio generale che permette di calcolare il numero di PP su $\mathbb{F}_q$ aventi grado non massimale, i.e. grado minore di $q-2$.
Correggiamo alcuni errori presenti nell'articolo [Wel2] e focalizzando la nostra attenzione su campi di caratteristica 2 diamo alcuni risultati originali; ad esempio dimostriamo formule per il numero di permutazioni con ordine 2 che muovono meno di 8 elementi e tali che il loro polinomio di permutazione abbia grado non massimale.

Bibliografia

[AMc] L. M. Adleman e K. S. McCurley, 'Open Problems in Number Theoretic Complexity, II', *Proceedings of the First Algorithmic Number Theory Symposium, Ithaca, New York, 6-9 Maggio 1994*, editori: L. M. Adleman e Ming-Deh Huang.

[AHU] A. V. Aho, J. E. Hopcroft e J. D. Ullman, *The Design and the Analysis of Computer Algorithms*, Addison-Wesley, 1974.

[Art] E. Artin, *Galois Theory*, Notre Dame Mathematical Lectures Numero 2, Notre Dame Indiana 1959.

[Ber] E. R. Berlekamp, *Algebraic Coding Theory*, Aegean Park Press, 1984.

[BM] I. F. Blake e R. C. Mullin, *The Mathematical Theory of Coding*, Academic Press, 1975.

[BCL] J. V. Brawley, L. Carlitz e J. Levine, 'Scalar Polynomial Functions on the $n \times n$ Matrices over a Finite Fields', *Linear Algebra and Its Applications* **10** (1975), pp. 199–217.

[BL] J. V. Brawley e J. Levine, 'Some Cryptographic Applications of Permutation Polynomials', *Cryptologia* **1** Number 1 (1977), pp. 76–92.

[Bur] D. M. Burton, *Elementary Number Theory*, Allyn and Bacon, Boston 1976.

[Car] L. Carlitz, 'Permutations in finite fields', *Acta Scientiarum Mathematicarum (Szeged, Acta Universitatis Szegediensis)* **24** (Szeged 1963), pp. 196–203.

[CNS] A. Conflitti, H. Niederreiter ed I. Shparlinski 'Elements of high orders in finite fields', in itinere.

[CS] A. Conflitti ed I. Shparlinski 'On computation of the greatest common divisor of several polynomials over a finite field', preprint.

[CFGH] G. Cooperman, S. Feisel, J. von zur Gathen e G. Havas, 'GCD of many integers', *Proc. 5th Intern. Computing and Combinatorics Conf.*, Tokyo 1999, Lect. Notes in Comp. Sci., Springer-Verlag, Berlino 1999 (da pubblicare).

[Gao] S. Gao, 'Elements of provable high orders in finite fields', *Proceedings of the American Mathematical Society* Vol. **127** n. 6 (Giugno 1999), pp. 1615–1623.

[vzGG] J. von zur Gathen e J. Gerhard, *Modern Computer Algebra*, Cambridge University Press, Cambridge 1999.

[GS1] J. von zur Gathen ed I. Shparlinski, 'Orders of Gauss Periods in Finite Fields', *AAECC (Applicable Algebra in Engineering, Communication and Computing)* **9** (1998), pp. 15–24.

[GS2] J. von zur Gathen ed I. Shparlinski, 'Constructing elements of large orders in finite fields', preprint.

[HW] G. H. Hardy e E. M. Wright, *An Introduction to the Theory of Numbers*, Clarendon Press, Oxford 1979.

[Her] I. N. Herstein, *Algebra*, Editori Riuniti, Roma 1994.

[Hun] T. W. Hungerford, *Algebra*, Springer Verlag, GTM 73, New York 1974.

[Koch] G. Koch, *La matematica del probabile*, Aracne, Roma 1997.

[Len] H. W. Lenstra Jr, 'Algorithms for finite fields', *Number Theory and Cryptography*, J. H. Loxton editore, London Mathematical Society Lecture Note Series 154, Cambridge University Press, Cambridge 1990, pp. 76–85.

[LMT] R. Lidl, G. L. Mullen e G. Turnwald, *Dickson polynomials*, Pitman Monographs and Surveys in Pure and Applied Mathematics 65, Longman Scientific and Technical, 1993.

[LN] R. Lidl e H. Niederreiter, *Finite Fields*, Cambridge University Press, Cambridge 1997.

[Macd] I. G. Macdonald, *Symmetric Functions and Hall Polynomials*, Clarendon Press, Oxford 1998.

[Mac1] A. Machi, *Introduzione alla Teoria dei Gruppi*, Feltrinelli, Milano 1974.

[Mac2] A. Machi, *Algebra per il Calcolo Simbolico*, Kappa, Roma 1995.

[MP] C. Malvenuto e F. Pappalardi, 'Enumerating Permutation Polynomials I: Permutation with non-maximal degree', in itinere.

[Map] Maple V Release 5.0 (1998), Waterloo Maple Inc.

[Mul1] G. L. Mullen, 'Permutational Polynomials over finite fields', *Finite fields, coding theory, and advances in communications and computing*, Lecture Notes in Pure and Appl. Math. 141, Dekker, New York 1993, pp. 131–151.

[Mul2] G. L. Mullen, 'Permutational Polynomials: A Matrix Analogue of Schur's Conjecture and a Survey of Recent Results', *Finite Fields and Their Applications* Vol. **1** n. 2 (Aprile 1995), pp. 242–258.

[MS] G. L. Mullen ed I. Shparlinski, 'Open problems and conjectures in finite fields', *Finite Fields and Applications (Proceedings of the third international conference, Glasgow, July 1995)*, editori: S. Cohen e H. Niederreiter, London Mathematical Society Lecture Note Series 233, Cambridge University Press, Cambridge 1996, pp. 243–268.

[Nie] H. Niederreiter, 'Finite Fields and Cryptology', *Finite fields, coding theory, and advances in communications and computing*, Lecture Notes in Pure and Appl. Math. 141, Dekker, New York 1993, pp. 359–373.

[Poh] M. E. Pohst, *Computational Algebraic Number Theory*, Birkhauser, DMV Seminar Volume 21, 1993.

[Pro] C. Procesi, *Elementi di Teoria di Galois*, Decibel Zanichelli, Bologna 1991.

[Ser] J. P. Serre, *A Course in Arithmetic*, Springer Verlag, GTM 7, New York 1973.

[Sho1] V. Shoup, *Removing Randomness from Computational Number Theory*, tesi di Ph.D. in Computer Science, University of Wisconsin-Madison, 1989.

[Sho2] V. Shoup, 'New Algorithms for Finding Irreducible Polynomials over Finite Fields', *Mathematics of Computation* **54** (1990), pp. 435–447.

[Sho3] V. Shoup, 'Searching for Primitive Roots in Finite Fields', *Mathematics of Computation* **58** (1992), pp. 369–380.

[Sho4] V. Shoup, 'Fast Construction of Irreducible Polynomials over Finite Fields', *Journal of Symbolic Computation* **17** (1994), pp. 371–391.

[Shp1] I. Shparlinski, 'On finding primitive roots in finite fields', *Theoretical Computer Science* **157** (1996), pp. 273–275.

[Shp2] I. Shparlinski, 'Approximate constructions in finite fields', *Finite Fields and Applications (Proceedings of the third international conference, Glasgow, July 1995)*, editori: S. Cohen e H. Niederreiter, London Mathematical Society Lecture Note Series 233, Cambridge University Press, Cambridge 1996, pp. 313–332.

[Ste] I. Stewart, *Galois Theory*, Chapman and Hall, 1989.

[Wae] B. L. van der Waerden, *Algebra*, Springer Verlag, New York 1991, due volumi.

[Wel1] C. Wells, 'Generators for groups of permutation polynomials over finite fields', *Acta Scientiarum Mathematicarum (Szeged, Acta Universitatis Szegediensis)* **29** (Szeged 1968), pp. 167–176.

[Wel2] C. Wells, 'The degrees of permutation polynomials over finite fields', *J. Combinatorial Theory* **7** (1969), pp. 49–55.

La Bibliografia si riferisce all'intera Tesi di Laurea.