Elements of large order in finite fields

Felipe Voloch

University of Texas at Austin

Talk at University of Canterbury, NZ, May 2015

Abstract

Galois showed (in 1830) that the multiplicative groups of finite fields are cyclic. The problem of explicitly exhibiting a generator is still unsolved. After setting the stage, we present explicit constructions of elements of large multiplicative order in finite fields.

Fields

A field is a set with two operations "plus" and "times" where the regular rules of algebra apply.

Examples: $\mathbb{Q}, \mathbb{R}, \mathbb{C}$.

Finite fields: Examples $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}, p$ a prime number.

$\mathbb{F}_2 = \{0, 1\}, 1 + 1 = 0.$

Finite fields

$f(x)$ irreducible polynomial with coefficients in $\mathbb{F}_p$

$\mathbb{F}_p[x]/(f(x))$ finite field with p^d elements, $d = \deg f(x)$.

Construction produces all finite fields. Works for all $d \geq 1$ and all primes p.

All finite fields with the same number of elements are isomorphic.

$\mathbb{F}_q$ denotes (unique) finite field with q elements.

Multiplicative group

$\mathbb{F}_q^*(= \mathbb{F}_q \setminus \{0\})$ is cyclic.

$\exists \gamma \in \mathbb{F}_q^*, \mathbb{F}_q^* = \{1, \gamma, \gamma^2, \ldots, \gamma^{q-2}\}$

Such γ is a generator or primitive root.

Main problem: find a generator.

Many generators, so trial and error works if we have a check for being generator. Can be done if a factorization of $q-1$ is known.

Galois

Si l'on élève successivement α aux puissances 2^e, 3^e, ..., on aura une suite de quantités de même forme [parce que toute fonction de i peut se réduire au $(\nu-1)^{ième}$ degré]. Donc on devra avoir $\alpha^n = 1$, n étant un certain nombre; soit n le plus petit nombre qui soit tel que l'on ait $\alpha^n = 1$. On aura un ensemble de n expressions, toutes différentes entre elles,

$$1, \alpha, \alpha^2, \alpha^3, \ldots, \alpha^{n-1}.$$

Multiplions ces n quantités par une autre expression θ de la même forme. Nous obtiendrons encore un nouveau groupe de quantités toutes différentes des premières et différentes entre elles. Si les quantités (A) ne sont pas épuisées, on multipliera encore les puissances de α par une nouvelle expression γ, et ainsi de suite. On voit donc que le nombre n divisera nécessairement le nombre total des quantités (A). Ce nombre étant $p^\nu - 1$, on voit que n divise $p^\nu - 1$. De là suit encore que l'on aura

$$\alpha^{p^\nu - 1} = 1, \qquad \text{ou bien} \qquad \alpha^{p^\nu} = \alpha.$$

Ensuite on prouvera, comme dans la théorie des nombres, qu'il y a des racines primitives α pour lesquelles on ait précisément $p^\nu - 1 = n$, et qui reproduisent par conséquent, par l'élévation aux puissances, toute la suite des autres racines.

Galois II

Il faut maintenant trouver une racine primitive, c'est-à-dire une forme de l'expression (3) qui, élevée à toutes les puissances, donne toutes les racines de la congruence

$$x^{2^2-1} = 1, \qquad \text{savoir} \qquad x^{2^1.3^1.19} = 1 \pmod 7,$$

et nous n'avons besoin pour cela que d'avoir une racine primitive de chaque congruence

$$x^2 = 1, \qquad x^{3^1} = 1, \qquad x^{19} = 1.$$

La racine primitive de la première est -1; celles de $x^{3^1} - 1 = 0$ sont données par les équations

$$x^3 = 2, \qquad x^3 = 4,$$

en sorte que i est une racine primitive de $x^{3^1} = 1$.

Il ne reste qu'à trouver une racine de $x^{19} - 1 = 0$, ou plutôt de

$$\frac{x^{19} - 1}{x - 1} = 0,$$

A more modest problem

No explicit construction of generators known.

Descriptions of explicit "small" sets containing a generator are known.

More modest problem: Find an element of $\mathbb{F}_q$ of "large" multiplicative order.

We will give explicit constructions of such elements in several cases.

Explicit examples I

Let p, ℓ be primes with p a primitive root modulo ℓ. Then $(x^\ell - 1)/(x-1)$ irreducible over $\mathbb{F}_p$.

Let ζ be a root of this polynomial and $\alpha = \zeta + \zeta^{-1}$. Then $\mathbb{F}_p(\alpha) = \mathbb{F}_{p^{(\ell-1)/2}}$ and α has order at least $e^{\sqrt{\ell}}$. (Ahmadi, Shparlinski, V.)

General result (V.): If $r(x)$ is a rational function w/ coeffs. in $\mathbb{F}_p$, not a monomial, then whenever $\zeta \in \mathbb{F}_{p^d}$ has "small" order, then $r(\zeta)$ has "large" order.

Explicit examples II

Let β be a root of $x^p - x - 1$, which is irreducible over $\mathbb{F}_p$. Then $\beta \in \mathbb{F}_{p^p}$ has order at least $2^{2.54p}$ (Conjecturally $(p^p - 1)/(p - 1)$).

Let $a_0 = 1 \in \mathbb{F}_2$ and for $n \geq 1$, a_n root of $x^2 + a_{n-1}x + 1$. Then $\mathbb{F}_2(a_n) = \mathbb{F}_{2^{2^n}}$ and a_n has order at least $\exp 2^{cn}$ for some $c > 0$.

Special case of general result (V.): If $E/\mathbb{F}_p$ is an elliptic curve and $P = (x, y) \in E(\mathbb{F}_{p^d})$ has has "small" order, then x has "large" order.

Idea of a proof

If $\zeta \in \mathbb{F}_{p^d}$ has "small" order, then $r(\zeta)^{p^i} = r(\zeta^{n_i})$, n_i small.

$r(\zeta)^{\sum_{i\in I} p^i} = \prod_{i\in I} r(\zeta^{n_i})$

$\prod_{i\in I} r(\zeta^{n_i}) \neq \prod_{i\in I'} r(\zeta^{n_i})$ if $(\deg r)\sum_{i\in I} n_i, (\deg r)\sum_{i\in I'} n_i < d$.

So, many $r(\zeta)^{\sum_{i\in I} p^i}$ are distinct and $r(\zeta)$ has "large" order.

THANK YOU

More information at

http://www.ma.utexas.edu/users/voloch/