Generators of elliptic curves over finite fields

Felipe Voloch

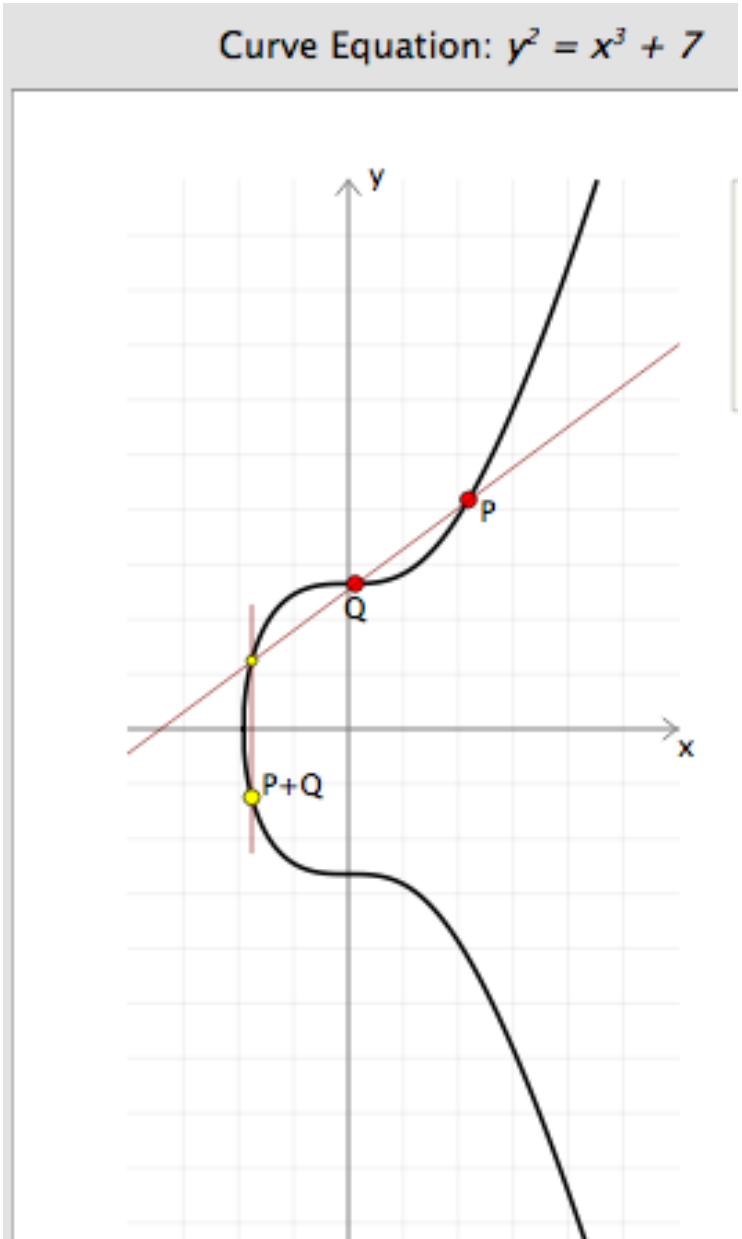
Talk at Univ. of Auckland

2016

Abstract

Abstract: We will discuss some problems and results connected with finding generators for the group of rational points of elliptic curves over finite fields and connect this with the analogue for elliptic curves over function fields of Artin's conjecture for primitive roots.

Elliptic curve



Group structure

$\mathbb{F}_q$ finite field of q elements and characteristic p and $E/\mathbb{F}_q$ an elliptic curve.

$$E(\mathbb{F}_q) \cong \mathbb{Z}/M \times \mathbb{Z}/N$$

Where $M|(N, q-1)$. Want generators. There is no simple formula. Open problem: find generators deterministically in polynomial time (in $\log q$).

Small set containing a generator

Theorem 1

(Shparlinski-V.) If $q = q_0^n, n \ll \log q_0$ *and* $\mathbb{F}_q = \mathbb{F}_{q_0}(\alpha)$, $E(\mathbb{F}_q)$ *has an element of order N with x-coordinate* $\alpha + c, c \in \mathbb{F}_{q_0}$.

Proof uses the curve "$x = \alpha + t$" in the abelian variety $R_{\mathbb{F}_q/\mathbb{F}_{q_0}}(E)$.

Artin's conjecture

Conjecture 1

Set of primes p for which 10 *is a primitive root mod p has density* $\prod_p(1 - 1/p(p-1)) = 0.37...$

Conjecture 2

If $E_t/\mathbb{F}_q(t), P_t \in E_t(\mathbb{F}_q(t))$ then, (under obvious conditions) given n large, for a positive proportion of $c \in \mathbb{F}_{q^n}$, P_c generates $E_c(\mathbb{F}_{q^n})$.

(Analogous question was asked by Lang and Trotter for number fields)

Artin's conjecture II

Progress on the above conjectures by looking instead at groups of larger rank (idea of Gupta and Murty).

Theorem 2

(Hall-V.) If $\Gamma \subset E_t(\mathbb{F}_q(t))$ *subgroup of rank at least* 6 *then, (under obvious conditions) given* n *large, for a positive proportion of* $c \in \mathbb{F}_{q^n}$, Γ *surjects onto* $E_c(\mathbb{F}_{q^n})$.

Characteristic 2

(Part of work in progress with M. Ciperiani and A. Cojocaru)

$E_t/\mathbb{F}_2(t)$ with equation $y^2 + xy = x^3 + t^3, P_t = (t,0) \in E_t(\mathbb{F}_2(t))$.

(There is interest in determining when $E_a(\mathbb{F}_{2^n})$ has order 2^n from a connection with the so-called Kloosterman sum zeros.)

Theorem 3

If $a \in \mathbb{F}_{2^n}, a \neq 0$, with n odd then $(a,0)$ is divisible by 2 in $E_a(\mathbb{F}_{2^n})$ if and only if $E_a(\mathbb{F}_{2^n})$ has a point of order 3.

Corollary 4

If n is odd and $\#E_a(\mathbb{F}_{2^n}) = 2^n$, then P_a is a generator of $E_a(\mathbb{F}_{2^n})$.

Another approach

A conjecture of Poonen predicts that, if $E/\mathbb{F}_q$ is an elliptic curve, f is a non-constant function on E (e.g. the x coordinate of a Weierstrass equation), then for $P \in E(\mathbb{F}_{q^n})$ (not in a subfield) either P has large order or $f(P)$ has large order in $\mathbb{F}_{q^n}^*$ where "large" means $\geq q^{n\varepsilon}$. I've obtained weak results in this direction. So, can get P of large order by forcing $f(P)$ of small order.

Example

$E/\mathbb{F}_2$ with equation $y^2 + xy = x^3 + 1$.

p prime, 2 non-square mod p, ζ primitive p-th root of 1.

$\beta = \zeta \sum_{j=0}^{(p-1)/2} \zeta^{2^j}$, $P = (\zeta, \beta) \in E$.

If 2 is a primitive root mod p, $2P$ has large order in $E(\mathbb{F}_{2^{(p-1)/2}})$.

THANK YOU