Group Structure of Elliptic Curves over Finite Fields

Igor E. Shparlinski

Macquarie University

Introduction

Notation

$\mathbb{F}_q$ = finite field of q elements.

An elliptic curve $\mathbb{E}$ is given by a *Weierstraß equation* over $\mathbb{F}_q$ or $\mathbb{Q}$

$$y^2 = x^3 + Ax + B$$

(if $\gcd(q, 6) = 1$).

$A \ll B$ and $B \gg A$ (I. M. Vinogradov)

$\Updownarrow$

$A = O(B)$ (E. Landau)

Main Facts

- Hasse–Weil bound: $|\#\mathbb{E}(\mathbb{F}_q) - q - 1| \leq 2q^{1/2}$
- $\mathbb{E}(\mathbb{F}_q)$ is an Abelian group, with a special "point at infinity" $\mathcal{O}$ as the neutral element.

Some Questions

- What are possible group structures which can be represented by elliptic curves?

- Is it typical for $\mathbb{E}$ to be have a large exponent $\mathbf{e}_q(\mathbb{E})$ (=the size of the largest cyclic subgroup of $\mathbb{E}(\mathbb{F}_q)$)?

- How often a "random" curve $\mathbb{E}$ is cyclic?

- What is a typical arithmetic structure of $\#\mathbb{E}(\mathbb{F}_q)$?

- How many $N \in [q - 2q^{1/2} + 1, q + 2q^{1/2} + 1]$ are taken as cardinalities $\#\mathbb{E}(\mathbb{F}_q)$?

What is a "random" curve?

Typically we consider "statistical" results in the following situations:

- The field $\mathbb{F}_q$ is fixed, the curve $\mathbb{E}$ runs through all elliptic curves over $\mathbb{F}_q$ (or over some natural classes of curves).

- The field $\mathbb{F}_q$ and the curve $\mathbb{E}$ are both fixed, we consider $\mathbb{E}(\mathbb{F}_{q^n})$ in the extension fields

- The curve $\mathbb{E}$ is defined over $\mathbb{Q}$ (and fixed). We consider reductions $\mathbb{E}(\mathbb{F}_p)$ modulo consecutive primes p

Remark: They are described in the increasing order of hardness.

Group Structure of $\mathbb{E}(\mathbb{F}_q)$ and Arithmetic Properties of $\#\mathbb{E}(\mathbb{F}_q)$

. . . are closely related. E.g. the question about the size of $\gcd(\#\mathbb{E}(\mathbb{F}_q), q-1)$ appears very frequently.

Some Motivation

The following questions are of mathematical interest and also have various cryptographic applications.

Florian Hess, Tanja Lange, Joe Silverman, I.S., **1999–2004**:

Bounds on the discrepancy of many pseudorandom number generators on elliptic curves are nontrivial only if the exponent

$$\mathbf{e}_q(\mathbb{E}) \geq q^{1/2+\varepsilon}.$$

Complex Multiplication

If $\mathbb{E}$ is an elliptic curve over an algebraic number field, $\mathbb{K}$ then endomorphism ring $\mathrm{End}_{\mathbb{K}}(\mathbb{E})$ of $\mathbb{E}$ over $\mathbb{K}$, contains a copy of the integers corresponding to the morphisms $x \mapsto nx$ for each $n \in \mathbb{Z}$. If $\mathrm{End}_{\mathbb{K}}(\mathbb{E})$ is strictly bigger than $\mathbb{Z}$, we say $\mathbb{E}$ has *complex multiplication* (CM) for in that case, it is a classical result that the ring is isomorphic to an order in an imaginary quadratic field. Otherwise, we say $\mathbb{E}$ is a non-CM curve.

Many of the questions about elliptic curves fall naturally into these two categories, the CM case and the non-CM case.

Typically, the CM case is the easier since there is an additional structure.

Group Structure of $\mathbb{E}(\mathbb{F}_q)$

Classical Results

$\mathbb{E}(\mathbb{F}_q)$ is

- either cyclic
- or isomorphic to a product of two cyclic groups $\mathbf{Z}/M \times \mathbf{Z}/L$ with $L|M = \mathbf{e}_q(\mathbb{E})$.

Max Deuring, **1941**:

All values $N \in [q-2q^{1/2}+1, q+2q^{1/2}+1]$, except for a small number of explicitly described exceptions, are taken as cardinalities $\#\mathbb{E}(\mathbb{F}_q)$ (for $q = p$ there is no exception).

Note: About q^2 Weierstraß equations, about $4q^{1/2}$ possible values for N.

More Precise Results

Michael Tsfasman; Filipe Voloch; Hans-George Rück, **1988**:

Roughly speaking, with only few fully described exceptions, for any L and M with

$$L \mid \gcd(M, q-1)$$

and such that LM can be realised as a cardinality of an elliptic curve over $\mathbb{F}_q$, there is also $\mathbb{E}$ for which

$$\mathbb{E}(\mathbb{F}_q) \cong \mathbf{Z}/L\mathbf{Z} \times \mathbf{Z}/M\mathbf{Z}.$$

Hendrik Lenstra, **1987**:

- For any $N \in [p - 2p^{1/2} + 1, p + 2p^{1/2} + 1]$, the probability that $\#\mathbb{E}(\mathbb{F}_p) = N$ for a random curve $\mathbb{E}$ is $O\left(p^{-1/2} \log p (\log \log p)^2\right)$.

- For any, but at most two values, in the *half interval* $N \in [p - p^{1/2} + 1, p + p^{1/2} + 1]$, the probability that $\#\mathbb{E}(\mathbb{F}_p) = N$ for a random curve $\mathbb{E}$ is at least $cp^{-1/2}(\log p)^{-1}$ for an absolute constant $c > 0$.

  Under the **ERH**, there are no exceptions and the bound becomes $cp^{-1/2}(\log \log p)^{-1}$.

Moral: Cardinalities are uniformly distributed, more or less.

Question: Study the distribution of group structures. It is **not** expected to be uniform.

Exponent $\mathbf{e}_q(\mathbb{E})$

Clearly

- if $\mathbb{E}(\mathbb{F}_q)$ is cyclic, then $\mathbf{e}_q(\mathbb{E}) = \#\mathbb{E}(\mathbb{F}_q) \sim q$ — as good as it gets;

- if $\mathbb{E}(\mathbb{F}_q)$ is isomorphic to a product of two cyclic groups $\mathbb{Z}/M \times \mathbb{Z}/L$ with $L|M$, then

$$\mathbf{e}_q(\mathbb{E}) = M \geq \#\mathbb{E}(\mathbb{F}_q)^{1/2} \sim q^{1/2}$$

  ... falls below the threshold $q^{1/2+\varepsilon}$.

Better Bounds?

Rene Schoof, **1991**:

If $\mathbb{E}$ (defined over $\mathbb{Q}$) has no complex multiplication then

- for all primes

$$\mathbf{e}_p(\mathbb{E}) \gg p^{1/2}\frac{\log p}{\log\log p}$$

... still below the threshold $p^{1/2+\varepsilon}$.

- under the **ERH**, for infinitely many primes,

$$\mathbf{e}_p(\mathbb{E}) \ll p^{7/8}\log p.$$

If $\mathbb{E} : y^2 = x^3 - x$ then $\mathbb{E}$ has complex multiplication over $\mathbf{Z}[i]$. On the other hand, $\mathbf{e}_p(\mathbb{E}) = k \sim p^{1/2}$ for every prime p of the form $p = k^2 + 1$.

Bill Duke, **2003**:
For almost all primes p (i.e., for all but $o(\pi(x))$ primes $p \le x$) and **all** curves $\mathbb{E}$ over $\mathbb{F}_p$

$$\mathbf{e}_p(\mathbb{E}) \ge p^{3/4-\varepsilon}$$

... comfortably above the $p^{1/2+\varepsilon}$ threshold!!

Kevin Ford and I.S., **2005**:

- The above bound is tight.

- A similar bound for Jacobians of curves of genus $g \ge 2$.

Even Better Bounds?

The bounds on the discrepancy of many sequences from elliptic curves attain their full strength when $\mathbf{e}_p(\mathbb{E})$ is of order close to q.

Question: Is it typical for $\mathbf{e}_q(\mathbb{E})$ to be close to q?

Bill Duke, **2003**:
For any curve $\mathbb{E}$ (defined over $\mathbb{Q}$) and almost all primes p

$$\mathbf{e}_p(\mathbb{E}) \geq p^{1-\varepsilon}$$

unconditionally if E has complex multiplication and under the **ERH**, otherwise.

I.S., **2003**:
For any prime p and almost all curves $\mathbb{E}$ (defined over $\mathbb{F}_p$)

$$\mathbf{e}_p(\mathbb{E}) \geq p^{1-\varepsilon}.$$

Florian Luca and I.S., **2004**:

Let $\mathbb{E}$ be an ordinary curve defined over $\mathbb{F}_q$. Then

- for almost all integers n,

$$\mathbf{e}_{q^n}(\mathbb{E}) \geq q^{n-2n(\log n)^{-1/6}}.$$

- for all integers n,

$$\mathbf{e}_{q^n}(\mathbb{E}) \geq q^{n/2+c(q)n/\log n}$$

The proofs are based of some deep facts of the theory of Diophantine Approximations

- Subspace Theorem;
- Lower bounds of linear forms of p-adic logarithms;
- Upper bounds on the number of zeros of linear recurrence sequences.

Essentially the proof of the first bound follows the ideas of *P. Corvaja and U. Zannier,* **2004**.

It also gives a subexponential upper bound on

$$d(q^n) = \gcd(\#\mathbb{E}(\mathbb{F}_{q^n}), q^n - 1)$$

which also appears in the estimate of the complexity of the structure finding algorithm of *Victor Miller,* **1984-2004**.

Florian Luca, James McKee and I.S., **2004**:

Let $\mathbb{E}$ be an ordinary curve defined over $\mathbb{F}_q$. Then for infinitely many integers n,

$$\mathbf{e}_{q^n}(\mathbb{E}) \ll q^n \exp\left(-n^{c/\log\log n}\right).$$

for some $c > 0$ depending only on q.

The proof is based on:

- studying the degree $d(r)$ of the extension of $\mathbb{F}_q$ generated by points of r-torsion groups (i.e. groups of points P on $\mathbb{E}$ in the algebraic closure $\overline{\mathbb{F}}_q$ with $rP = \mathcal{O}$) for distinct primes r;

- a modification of a result of Adleman–Pomerance–Rumely (1983) on constructing integers n which have exponentially many divisors of the form $r - 1$, where r is prime.

How do we proceed?

Combine the following facts:

- *Weil Pairing:* If $\mathbb{E}(\mathbb{F}_q) \cong \mathbf{Z}/M \times \mathbf{Z}/L$ with $L|M$, then $L|q-1$.

- *Hendrik Lenstra,* **1987**: For any N, the probability that $\#\mathbb{E}(\mathbb{F}_q) = N$ for a random curve $\mathbb{E}$ is $O\left(q^{-1/2}\log q(\log\log q)^2\right)$.

  Thus all values of $N \in [q-2q^{1/2}, q+2q^{1/2}]$ are taken about the same number of times.

The question about $e_q(\mathbb{E})$ is now reduced to studying how often $N \in [q-2q^{1/2}+1, q+2q^{1/2}+1]$ has a large common divisor with $q-1$.

Is Cyclicity Typical?

- Fix the field — Vary the curve:

  Sergei Vlăduţ, **1999**:
  At least 75% of elliptic curves over $\mathbb{F}_q$ are cyclic, but **not** 100%.

- Fix the curve over $\mathbb{F}_q$: — Vary the extension:
  Sergei Vlăduţ, **1999**:
  Over every finite there is a curve $\mathbb{E}$ such that $\mathbb{E}(\mathbb{F}_{q^n})$ is cyclic for a positive proportion of n.

- Fix the curve over $\mathbb{Q}$: — Vary the prime:

  Related to the **Lang–Trotter Conjecture!**

  Alina Cojocaru, Ram Murty, Bill Duke, **2001-2006**: (a series of results)

  - under the **ERH** the set of primes for which $\mathbb{E}(\mathbb{F}_p)$ is cyclic is of positive density (depending on $\mathbb{E}$);

  - the smallest prime for which $\mathbb{E}(\mathbb{F}_p)$ is cyclic is not too large.

Finding the Group Structure

Victor Miller, **1984-2004**:
There is a probabilistic algorithm which runs in time $(\log q)^{O(1)}$ + time to factor

$$d(q) = \gcd(\#\mathbb{E}(\mathbb{F}_q), q-1)$$

John Friedlander, Carl Pomerance and I.S., **2005**:
Typically $d(q)$ is easy to factor: the expected time is $(\log q)^{1+o(1)}$.

David Kohel and I.S., **2001**:
Deterministic algorithm which runs in time $q^{1/2+o(1)}$ (in fact it produces a set of generators).

The result is based on the extension of *Bombieri's bound* of exponential sums

$$\sum_{P \in \mathcal{H}} \exp\left(2\pi\sqrt{-1}\mathrm{Tr}\left(f(P)\right)/p\right) = O(q^{1/2})$$

for any subgroup $\mathcal{H} \in \mathbb{E}(\mathbb{F}_q)$ and any function f which is not constant on $\mathbb{E}$.

Arithmetic Structure of $\#\mathbb{E}(\mathbb{F}_q)$

Primality

The Holy Grail is to prove at least one out of the following claims (also very important for elliptic curve cryptography):

- For every q, there are sufficiently many curves $\mathbb{E}$ over $\mathbb{F}_q$, such that $\#\mathbb{E}(\mathbb{F}_q)$ is prime;
- for a curve $\mathbb{E}$ over $\mathbb{F}_q$, $\#\mathbb{E}(\mathbb{F}_{q^n})/\#\mathbb{E}(\mathbb{F}_q)$ is prime for infinitely many integers n;
- for a curve $\mathbb{E}$ over $\mathbb{Q}$ without torsion points, $\#\mathbb{E}(\mathbb{F}_p)$ is prime for infinitely many primes p.

Out of reach!

One of the obstacles is the lack of the results about primes in short intervals.

Large and Small Prime Divisors of $\#\mathbb{E}(\mathbb{F}_q)$

Question: What if we ask for curves such that $\#\mathbb{E}(\mathbb{F}_q)$ does not have a large prime divisor?

Hendrik Lenstra, **1987**: For the rigorous analysis of the *elliptic curve factorisation* we need to show that there are sufficiently many curves over $\mathbb{F}_p$ for which $\#\mathbb{E}(\mathbb{F}_p)$ is smooth. — Still unknown!

Hendrik Lenstra, Jonathan Pila and Carl Pomerance, **1993**:
The current knowledge is enough to analyze rigorously the hyperelliptic smoothness test (larger intervals ...).

Question: What if we only ask for curves such that $\#\mathbb{E}(\mathbb{F}_q)$ has a large prime divisor?

Glyn Harman, **2005**:
There is a positive proportion of integers n in the middle part of the Hasse–Weil interval $n \in [q + 1 - q^{1/2}, q + 1 + q^{1/2}]$ with the largest prime divisor $P(n) \geq n^{0.74}$

Number of Prime Divisors

S. A. Miri and V. K. Murty, **2001**:
Alina Cojocaru, **2005**:
Under the **ERH**, for any non-CM elliptic curve $\mathbb{E}$ over $\mathbb{Q}$, one has an analogue of the *Turán–Kubilius* inequality:

$$\sum_{p \leq x} \left(\omega\left(\#\mathbb{E}(\mathbb{F}_p)\right) - \log\log p\right)^2 = O(\pi(x)\log\log x)$$

where, as usual, $\pi(x) = \#\{p \leq x\}$.

Yu-Ru Liu, **2004**:
For CM curves, a similar result is obtained unconditionally.

S. A. Miri and V. K. Murty, **2001**: *Alina Cojocaru,* **2005**:
Jörn Steuding & Annegret Weng, **2005**:
Jorge Jimnez & Henryk Iwaniec, **2006**:
There are at least $C(\mathbb{E})x/(\log x)^2$ primes $p \leq x$ such that

- $\Omega(\#\mathbb{E}(\mathbb{F}_p)) \leq 9$, if $\mathbb{E}$ is a non-CM curve,
- $\omega(\#\mathbb{E}(\mathbb{F}_p)) \leq 6$, if $\mathbb{E}$ is a non-CM curve,
- $\omega(\#\mathbb{E}(\mathbb{F}_p)) \leq 2$, if $\mathbb{E}$ is a CM curve.

CM Discriminants

For a curve $\mathbb{E}$ defined over $\mathbb{F}_p$ we put $t = \#E(\mathbb{F}_p) - p - 1$ and write

$$t^2 - 4p = -r^2 s$$

where s is squarefree. Then either $-s$ or $-4s$ is the discriminant of the endomorphism ring of $\mathbb{E}$, or CM discriminant.

Florian Luca and I.S., **2004**:

- The discriminant is usually large for a "random" curve;
- All curves modulo p define $2p^{1/2} + O(p^{1/3})$ distinct discriminants.

In particular, the last bound is based on an improvement of a result of Cutter–Granville–Tucker.

Cryptographic Applications

Embedding Degree and **MOV** Attack

Alfred Menezes, Tatsuaki Okamoto and Scott Vanstone, **1993**:
MOV constructs an embedding of a fixed cyclic subgroup of order L of $\mathbb{E}(\mathbb{F}_p)$ into the multiplicative group $\mathbb{F}^*_{p^k}$ provided $L|p^k-1$.

Number Field Sieve: **discrete logarithm** in $\mathbb{F}^*_{p^k}$ can be found in time $\mathcal{L}_{p^k}\left(1/3,(64/9)^{1/3}\right)$ where, as usual,

$$\mathcal{L}_m(\alpha,\beta)=\exp\left((\beta+o(1))(\log m)^{\alpha}(\log\log m)^{1-\alpha}\right).$$

The smallest k with

$$\#\mathbb{E}(\mathbb{F}_p)|p^k-1$$

is called the **embedding degree**.

If the embedding degree of $\mathbb{E}(\mathbb{F}_p)=o\left((\log p)^2\right)$ then the **discrete logarithm** on $\mathbb{E}(\mathbb{F}_p)$ can be solved in subexponential time $p^{o(1)}$.

R. Balasubramanian and N. Koblitz, **1998**:
For *almost all primes* p and almost all elliptic curves over $\mathbb{F}_p$ of *prime cardinality* the embedding degree is large.

E.g. for a "random" prime $p \in [x/2, x]$ and a random curve modulo p of *prime cardinality*,

$$\Pr\{\text{embedding degree} \le (\log p)^2\} \le x^{-1+o(1)}.$$

Florian Luca and I.S., **2004**:
For *all* primes p and almost all elliptic curves over $\mathbb{F}_p$ of *arbitrary cardinality* the embedding degree is large:

Let $K = (\log p)^{O(1)}$. For a randomly chosen curve

$$\Pr\{\text{embedding degree} \le K\} \le p^{-1/(4\kappa+6)+o(1)},$$

where

$$\kappa = \frac{\log K}{\log_2 p}.$$

For $K = (\log p)^2$ the RHS is $p^{-1/14+o(1)}$.

The proof is based on

- studying $N \in [p+1-2p^{1/2}, p+1+2p^{1/2}]$ with $N | p^k - 1$, for some $k \le K$;

- Lenstra's bound on the number of curves with $\mathbb{E}(\mathbb{F}_p) = N$.

For $H \ge h \ge 1$ and $K \ge 1$, we let $N(p, K, H, h)$ be the number of integers $N \in [H-h, H+h]$ with $N \mid (p^k - 1)$ for some $k \le K$.

For $\log H \asymp \log h \asymp \log p$ and $\log K = O(\log_2 p)$,

$$N(p, K, H, h) \le h^{1-1/(2\kappa+3)+o(1)},$$

where

$$\kappa = \frac{\log K}{\log_2 p}.$$

Also, similar results about the probability that

- $P(\#\mathbb{E}(\mathbb{F}_p)) | p^k - 1$ for $k \le K$;

- $\#\mathbb{E}(\mathbb{F}_p) | \prod_{k=1}^{K} (p^k - 1)$.

Scarcity of Pairing Friendly Fields

For several other cryptographic applications of the *Tate or Weil pairing* on elliptic one need elliptic curves $\mathbb{E}$ with **small** embedding degree.

Supersingular curves give $\mathbb{E}(\mathbb{F}_q) = q + 1$ thus are natural candidates. However, one can also suspect that supersingular curves have some cryptographic weaknesses and thus ask for constructions generating *ordinary curves*.

Let

$$\Phi_k(X) = \prod_{\substack{j=0 \\ \gcd(j,k)=1}}^{k} (X - \exp(2\pi\sqrt{-1}j/k))$$

be the kth *cyclotomic polynomial*.

$\mathbb{E}$ with $\#\mathbb{E}(\mathbb{F}_q) = q + 1 - t$ is of embedding degree k

$$\Updownarrow$$

$$q + 1 - t | \Phi_k(q)$$

$$\Updownarrow$$

$$q + 1 - t | \Phi_k(t - 1)$$

Typically, such constructions work into two steps:

Step 1 Choose a prime ℓ, integers $k \geq 2$ and t, and a prime power q such that

$$\begin{aligned} |t| &\leq 2q^{1/2}, \qquad & t &\neq 0, 1, 2, \\ \ell &\mid q + 1 - t, & \ell &\mid \Phi_k(q). \end{aligned} \tag{1}$$

(based on black magic or luck).

Step 2 Construct an elliptic curve $\mathbb{E}$ over $\mathbb{F}_q$ with $\#\mathbb{E}(\mathbb{F}_q) = q + 1 - t$.

k should be reasonable small (e.g., $k = 2, 3, 4, 6$), while the ratio $\log \ell / \log q$ should be as large as possible, preferably close to 1.

Unfortunately, there is no efficient algorithm for Step 2, except for the case when the $t^2 - 4q$ has a very small square-free part; that is, when

$$t^2 - 4q = -r^2 s \tag{2}$$

with some integers r and s, where s is a small square-free positive integer. In this case either $-s$ or $-4s$ is the fundamental discriminant of the CM field of $\mathbb{E}$.

Let $Q_k(x, y, z)$ be the number of prime powers $q \le x$ for which there exist prime $\ell \ge y$ and t satisfying (1) and (2) with a square-free $s \le z$.

Florian Luca and I.S., **2006**:
For any fixed k and real x, y and z the following bound holds

$$Q_k(x, y, z) \le x^{3/2+o(1)} y^{-1} z^{1/2}$$

as $x \to \infty$.

In particular, if $z = x^{o(1)}$, which is the only practically interesting case anyway, we see that unless $y \le x^{1/2}$ there are very few finite fields suitable for pairing based cryptography.

In other words, unless the common request of the primality of the cardinality of the curve is relaxed to the request for this cardinality to have a large prime divisor (e.g., a prime divisor ℓ with $\log \ell / \log q \ge 1/2$), the suitable fields are very rare.

Heuristic on MNT curves

Atsuko Miyaji, Masaki Nakabayashi and Shunzou Takano, **2001**:
MNT algorithm to produce elliptic curves satisfying the condition (1) with $k = 3, 4, 6$, and the condition (2) for a given value of s.

Florian Luca and I.S., **2005**:
Heuristic estimates on the number of elliptic curves which can be produced by **MNT**.

It seems that they produce only finitely many suitable curves (still this can be enough for practical needs of elliptic curve cryptography).

Our arguments are based on a combination of the following observations:

- **MNT** gives a parametric family of curves whose parameter runs through a solution of a *Pell equation* $u^2 - 3sv^2 = -8$ (for $k = 6$, and similar for $k = 3, 4$).

- Consecutive solutions (u_j, v_j) of a Pell equation grow exponentially, as at least s^{cj} and most probably as $e^{cs^{1/2}j}$ for some constant $c > 0$.

- The probability of a random integer n to be prime is $1/\log n$.

- MNT curves should satisfy two independent primality conditions (on the field size and on the cardinality of the curve).

Therefore, the expected total number of **MNT** curves for every s is bounded, by the order of magnitude, by

$$\sum_{j=1}^{\infty} \frac{1}{(\log s^{cj})^2} \ll \frac{1}{\log s} \sum_{j=1}^{\infty} \frac{1}{j^2} \ll \frac{1}{\log s}.$$

or even by

$$\sum_{j=1}^{\infty} \frac{1}{(\log e^{cs^{1/2}j})^2} \ll \frac{1}{s} \sum_{j=1}^{\infty} \frac{1}{j^2} \ll \frac{1}{s}.$$

Probably the total number of all **MNT** curves of prime cardinalities (over all finite fields) and of bounded CM discriminant, is bounded by an absolute constant.

Apparently the number of all **MNT** curves of prime cardinalities with CM discriminant up to z, is at most $z^{o(1)}$.

Similar heuristic shows that **MNT** produces sufficiently many curves whose cardinality has a large prime divisor.

Generating Pseudorandom Points on Elliptic Curves

Fix a point $G \in \mathbb{E}(\mathbb{F}_p)$ of order t

- EC Linear Congruential Generator, **EC-LCG**:

  For the "initial value" $U_0 \in \mathbb{E}(\mathbb{F}_q)$, consider the sequence:

  $$U_k = G \oplus U_{k-1} = kG \oplus U_0, \qquad k = 1, 2, \ldots .$$

  Introduced and studied by:

  Sean Hallgren, **1994**: **EC-LCG**

  Also by
  Gong, Berson, Stinson, **2001**:
  Beelen, Doumen, **2002**:
  El Mahassni, Hess, I.S., **2001-2003**:

- EC Power Generator, **EC-PG**:

  For an integer $e \geq 2$, consider the sequence (with $W_0 = G$),

  $$W_k = eW_{k-1} = e^k G, \qquad k = 1, 2, \ldots ,$$

  Introduced and studied by:

  Tanja Lange, I.S., **2003**:

- EC Naor-Reingold Generator, **EC-NRG**:

  Given an integer vector $\mathbf{a} = (a_1, \ldots a_k)$, consider the sequence:

  $$F_{\mathbf{a}}(n) = a_1^{\nu_1} \ldots a_k^{\nu_k} G, \qquad n = 1, 2, \ldots ,$$

  where $n = \nu_1 \ldots \nu_k$ is the bit representation of n, $0 \leq n \leq 2^k - 1$.

  Introduced and studied by:

  Bill Banks, Frances Griffin, Daniel Lieman, Joe Silverman, I.S., **1999-2001**:

  Example: Let $G \in \mathbb{E}(\mathbb{F}_p)$ be of order $t = 19$, $k = 4$ and $\mathbf{a} = (2, 5, 3, 4)$. Then,

  $$\begin{aligned}
  F_{\mathbf{a}}(0) &= 2^0 5^0 3^0 4^0 G = G, \\
  F_{\mathbf{a}}(1) &= 2^0 5^0 3^0 4^1 G = 4G, \\
  F_{\mathbf{a}}(2) &= 2^0 5^0 3^1 4^0 G = 3G, \\
  F_{\mathbf{a}}(3) &= 2^0 5^0 3^1 4^1 G = 12G, \\
  \ldots &\quad \ldots \\
  F_{\mathbf{a}}(11) &= 2^1 5^0 3^1 4^1 G = 24G = 5G, \\
  \ldots &\quad \ldots \\
  F_{\mathbf{a}}(15) &= 2^1 5^1 3^1 4^1 G = 120G = 6G,
  \end{aligned}$$

They all have analogues in the group $\mathbb{F}_q^*$

Florian Hess, Tanja Lange, I.S., **2001–2004**:

Theorem:
If G is of order $t \geq p^{1/2+\varepsilon}$ then

EC-LCG, **EC-PG**, **EC-NRG**

are reasonably well distributed

Conjecture:
The above sequences are very well distributed

Proof ingredients:

- Bounds of exponential sums

  David Kohel, I.S., **2000**:

  $$\sum_{P \in \mathcal{H}} \exp\left(2\pi i f(P)/p\right) = O(p^{1/2})$$

  for any subgroup $\mathcal{H} \in \mathbb{E}(\mathbb{F}_p)$ and any function f which is not constant on $\mathbb{E}$.

- Results about not vanishing some functions over $\mathbb{E}$