Pairing Friendly Elliptic Curves and Finite Fields

Igor E. Shparlinski

Macquarie University

Introduction

Weierstraß equation

$\mathbb{F}_q$ = 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 $\gcd(q, 6) = 1$).

Basic 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 and which is
  - either cyclic
  - or isomorphic to a product of two cyclic groups $\mathbf{Z}/M \times \mathbf{Z}/L$ with $L|M$.

Weil Pairing

Bilinear Map:

$$e : \mathcal{G} \times \mathcal{G} \to \mathbb{F}_{q^k}^*$$

where $\mathcal{G}$ is a subgroup $\mathbb{E}(\mathbb{F}_q)$

$$e(P, Q) \in \mathbb{F}_{q^k}^*$$

and

$$\begin{aligned} e(P + R, Q) &= e(P, Q)e(R, Q), \\ e(P, Q + R) &= e(P, Q)e(P, R) \end{aligned}$$

Necessary Condition $\#\mathcal{G} \mid q^k - 1$

Special Case: $\mathcal{G} = \mathbb{E}(\mathbb{F}_q)$

The smallest k with

$$\#\mathbb{E}(\mathbb{F}_q) \mid q^k - 1$$

is called the **embedding degree** of $\mathbb{E}(\mathbb{F}_q)$.

Applications of Weil Pairing

- **MOV Attack on EC-Dlog** *A. Menezes, T. Okamoto and S. Vanstone,* **1993**:
  Instead of solving EC-Dlog over $\mathbb{E}(\mathbb{F}_q)$ one can solve Dlog over $\mathbb{F}_{q^k}$.

- **Tripartie DH Protocol** *A. Joux,* **2001**:
  To create a common secret key, A, B and C choose secret numbers a, b, c and publish pairs

  $$(aP, aQ), \qquad (bP, bQ), \qquad (cP, cQ).$$

  Now each of them is able to compute the common key

  $$K = e(P, Q)^{abc}.$$

- **Identity Based Cryptography** *D. Boneh and M. Franklin,* **2003**:

Problem

For the above applications to be practical and efficient the embedding degree must be small.

Quick Answer: Take any supersingular curve $\mathbb{E}(\mathbb{F}_q)$. It has

$$\#\mathbb{E}(\mathbb{F}_q) = q + 1 \mid q^2 - 1,$$

thus the embedding degree $k = 2$.

However,

Supersingular curves are not to be trusted!

Question (reformulated): How can we construct an **ordinary** elliptic curve with a small embedding degree?

More Questions

- What is the embedding degree of a random curve? One can randomise:
  - Curve (fix $\mathbb{F}_q$ and take random A and B in the Wierstrass equation).
  - Field (fix $\mathbb{E}$ over $\mathbb{Q}$ and take its reduction modulo a random prime p).
  - Both
- How can we construct elliptic curves with a small embedding degree?
- In what fields do elliptic curves with a small embedding degree exist?

Random Curves and **MOV** Attack

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

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

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

If the embedding degree k of $\mathbb{E}(\mathbb{F}_q)$ is

$$k = o\left(\frac{(\log q)^2}{(\log\log q)^2}\right)$$

then the **discrete logarithm** on $\mathbb{E}(\mathbb{F}_q)$ can be solved in subexponential time:

$$\begin{aligned}
&\mathcal{L}_{q^k}\left(1/3, (64/9)^{1/3}\right) \\
&\quad = \exp\left(\left(\left(\frac{64}{9}\right)^{1/3} + o(1)\right)(\log q^k)^{1/3}(\log\log q^k)^{2/3}\right) \\
&\quad = \exp\left(\left(\left(\frac{64}{9}\right)^{1/3} + o(1)\right)(k\log q)^{1/3}(\log(k\log q))^{2/3}\right) \\
&\quad = \exp\left(o(\log q)\right) = q^{o(1)}
\end{aligned}$$

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**,

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

What is p is given?

What if the cardinality is not prime?

Florian Luca and I.S., **2004**:
For *all* primes p and *almost all elliptic curves* over $\mathbb{F}_p$ of *any 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 $k \le K$;

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

Another Bad Idea

Take an ordinary elliptic curve $\mathbb{E}$ over $\mathbb{F}_q$ and the consider it over $\mathbb{F}_{q^n}$.

Florian Luca and I.S., **2006**:

Subspace Theorem

$\Downarrow$

Theorem 1 *For any $\delta > 0$, there exists a constant $c > 0$, such that for any sufficiently large X the bound*

$$k(q^n) \geq c(\log n)^{1/6}$$

holds for all positive integers $n \leq X$ except at most X^δ of them.

Scarcity of Pairing Friendly Fields

Requirements

Let

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

be the kth *cyclotomic polynomial*.

$$\Phi_k(X) \mid X^k - 1$$

$$\ell \mid q^k - 1 \text{ and } \ell \nmid q^m - 1,\ 1 \leq m < k, \implies \ell \mid \Phi_k(q)$$

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

$$\ell \mid q + 1 - t \mid q^k - 1 \quad \text{and} \quad \ell \nmid q^m - 1,\ 1 \leq m < k$$

$$\Downarrow$$

$$\ell | \Phi_k(q) \quad \text{and} \quad q \equiv t - 1 \pmod{\ell}$$

$$\Downarrow$$

$$\ell \mid \Phi_k(t - 1)$$

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

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

(based on black magic or luck).

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

We want:

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

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

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

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 $\mathbb{E}$.

So we also need

$t^2 - 4q = -r^2 s$ with small square-free s

Counting Function:

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

$$|t| \le 2q^{1/2}, \qquad t \ne 0, 1, 2,$$
$$\ell \mid q + 1 - t, \qquad \ell \mid \Phi_k(q),$$
$$t^2 - 4q = -r^2 s.$$

with a square-free $s \le z$.

Florian Luca and I.S., **2006**:

Theorem 2 *For any fixed k and real x, y and z the following bound holds*

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

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.

Moral

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 $\log \ell / \log q \geq 1/2$), the suitable fields are very **rare**.

Notation

$$A \ll B \quad \text{(I. M. Vinogradov)}$$

$$\Updownarrow$$

$$A = O(B) \quad \text{(E. Landau)}$$

$\ll$ is more compact and easier to use (admits more informative chains like $A \ll B = C$).

Proof

Since $\ell \mid q+1-t$ and $\ell \mid \Phi_k(q)$, we also have

$$\ell \mid \Phi_k(t-1). \tag{3}$$

and

$$\ell m = q+1-t$$

for some m which together with $t^2-4q = -r^2 s$ implies that

$$(t-2)^2 + r^2 s = 4\ell m.$$

Therefore

$$\ell \mid (t-2)^2 + r^2 s. \tag{4}$$

Comparing (3) and (4), we conclude that ℓ divides the resultant $R_k(r^2 s)$ of the polynomials $\Phi_k(X)$ and $(X-1)^2 + r^2 s$, that is

$$\ell \mid R_k(r^2 s) = \mathrm{Res}\left(\Phi_k(X), (X-1)^2 + r^2 s\right).$$

$\Phi_k(X)$ is an irreducible and $\deg \Phi_k = \varphi(k)$,

$$\Downarrow$$

$R_k(r^2 s)$ does not vanish

- if $k \neq 1, 2, 3, 4, 6$ (since $\varphi(k) \geq 3$ for $k \neq 1, 2, 3, 4, 6$).

- if $k = 2$, since $\Phi_2(X) = X + 1$ and it is obvious that -1 is not a root of $(X-1)^2 + r^2 s$ for $s \geq 1$.

- if $k = 3, 4, 6$, since $\varphi(k) = 2$ and $R_k(r^2 s) = 0$ implies that $\Phi_k(X) = (X-1)^2 + r^2 s$ which is impossible (substitute $X = 0$).

$\omega(n) =$ the number of prime divisors of n.

If $r^2 s$ is fixed, then by

$$\ell \mid R_k(r^2 s) = \mathrm{Res}\left(\Phi_k(X), (X-1)^2 + r^2 s\right).$$

we see that ℓ can take at most

$$\omega(|R_k(r^2 s)|) \ll \log |R_k(r^2 s)| \ll \log(r^2 s) \leq \log x \tag{5}$$

possible values.

$t^2 - 4q = -r^2 s \implies r^2 s \leq 4x$ if $q \leq x$. Thus the total number of products $r^2 s$ can be estimated as

$$\sum_{s \leq z} \sum_{r \leq \sqrt{4x/s}} 1 \leq \sum_{s \leq z} \left\lfloor \sqrt{4x/s} \right\rfloor \ll \sqrt{xz}. \tag{6}$$

When $r^2 s$ and ℓ are fixed, we see that m in

$$\ell m = q + 1 - t$$

can take at most

$$\left\lfloor \frac{x + 1 + 2x^{1/2}}{\ell} \right\rfloor \leq \left\lfloor \frac{x + 1 + 2x^{1/2}}{y} \right\rfloor \ll \frac{x}{y} \tag{7}$$

possible values.

By

$$\ell m = q + 1 - t \quad \text{and} \quad (t-2)^2 + r^2 s = 4\ell m,$$

if r, s and m are fixed then q and t are fixed too. Combining (5), (6) and (7), we conclude the proof.

Heuristic Bounds

Galbraith, McKee and Valenca, **2005**:
there are about $x^{1/2+o(1)}$ prime powers $q \leq x$ for which there is an ordinary elliptic curve $\mathbb{E}$ satisfying $\#\mathbb{E}(\mathbb{F}_q) \mid \Phi_k(q)$.

This applies to all curves without any restriction on the arithmetic structure of $\#\mathbb{E}(\mathbb{F}_q)$, or on the size of the discriminant of the field of complex multiplication.

It seems that giving a rigorous proof of this result is out of reach nowadays due to our poor knowledge of the distribution of roots of polynomial congruences.

All arguments in our derivation of the upper bound can be reverted except that we ignored that

1. ℓ in

   $$\ell \mid R_k(r^2 s) = \mathrm{Res}\left(\Phi_k(X), (X-1)^2 + r^2 s\right).$$

   must satisfy

   $$y \le \ell \le x.$$

2. $\Phi_k(X)$ and $(X-1)^2 + r^2 s$ must have a common root t with $|t| \le 2x^{1/2}$.

Lemma 3 *For $0 < \alpha < \beta < 1$, there is a positive proportion of integers $n \le U$ which have a prime divisor ℓ with $U^\alpha \le \ell \le U^\beta$.*

1. $\Longrightarrow$ affects only the density.
2. $\Longrightarrow$ correction factor $x^{1/2}/y$.

Florian Luca and I.S., **2006**:

These arguments can be made more precise

Putting everything together we obtain that the bound

$$Q_k(x,y,z) \gg \frac{x^{1/2}}{y} \cdot \text{ Bound of Theorem 2}$$

$$= x^{2+o(1)}y^{-2}z^{1/2}$$

should hold, provided that $y \ge x^{1/2}$.

Is it more precise than Theorem 2?

We believe so. . .

Regular Constructions

As we have seen trying to find a pairing friendly curve/field by the blind random search is hopeless.

So several regular constructions have been invented:

Miyaji, Nakabayashi and Takano, **2001**:

Barreto and Scott, **2004**:

Barreto, Lynn and Scott, **2003,2004**:

Barreto and Naehrig, **2006**:

Dupont, Enge and Morain, **2005**:

Freeman, **2006**:

Some generalisations in

Galbraith, McKee and Valenca, **2005**:

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).

MNT Construction For $k = 6$

The MNT algorithm produces positive integers q and t of the form

$$q = 4m^2 + 1, \qquad t = \pm 2m + 1$$

for some positive integer m.

Divisibility

We have

$$q + 1 - t = 4m^2 \pm 2m + 1.$$

Since $\Phi_6(X) = X^2 - X + 1$ we obtain

$$\begin{aligned} \Phi_6(4m^2 + 1) &= (4m^2 + 1)^2 - (4m^2 + 1) + 1 \\ &= (4m^2 + 1)^2 - 4m^2 \\ &= (4m^2 - 2m + 1)(4m^2 + 2m + 1) \end{aligned}$$

CM Discriminant $= s$

We have

$$\begin{aligned} 4q - t^2 &= 16m^2 + 4 - (\pm 2m + 1)^2 \\ &= 4m^2 + 4 - 4m^2 \mp 4m - 1 \\ &= 12m^2 \mp 4m + 3 \\ &= \frac{(\pm 6m + 1)^2 + 8}{3} = r^2 s \end{aligned}$$

So we choose $m = \pm(u-1)/6$ where $u = 6m + 1$ is a solution to the following *Pell equation*

$$u^2 - 3sv^2 = -8, \qquad u, v \in \mathbb{N}. \tag{8}$$

Cryptographic Suitability

We need to check that

$$\ell = q + 1 - t$$

is prime.

Our Arguments

We combine the following observations:

- **MNT** gives a parametric family of curves whose parameter runs through a solution of a Pell equation (8) (i.e., $u^2 - 3sv^2 = -8$).

- 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).

$\Longrightarrow$ the expected number of **MNT** curves for every s is, by the order of magnitude,

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

or even by

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

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.

Bad News:

Apparently the number of all **MNT** curves of prime cardinalities with CM discriminant up to z, is is bounded, by the order of magnitude,

$$\sum_{s \leq z} \frac{1}{s} \asymp \log z.$$

Good News:

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