Counting creatively: curves and cryptography

Sunil Chetty

Department of Mathematics

College of Saint Benedict Saint John's University

February 13, 2014

First examples

Curves are often the first (algebro-geometric) objects one studies in school:

Familiar name	Defining equation
Lines	$ax + by = c$
Quadratics	$y = ax^2 + bx + c$
Circles	$x^2 + y^2 = c$

Question

What seems to be common amongst these examples? In other words, why might each of these fall under one class called "curves"?

Generalities

There are two objects which could be used to define a curve:

1. A geometric set of (e.g. rational) points $C(\mathbb{Q}) = \{(a,b) \in \mathbb{Q}^2 \ : \ f(a,b) = 0\}$.
2. An algebraic equation in two variables defines a curve, i.e. $C : \ f(x,y) = 0$, for some polynomial $f(x,y)$ with coefficients in $\mathbb{Z}$.

   Algebraic geometry makes very deep connections between algebraic structure corresponding to the polynomial and the geometry of a (algebraic) set of points, far beyond curves.

Linear curves: $\mathbb{Q}$-points

Consider a degree 1 curve
$L: \ ax + by + c = 0$, with $a \neq 0$ or $b \neq 0$.

The points on the curve will depend on what values are allowed for x and y.

First consider $L(\mathbb{Q})$, i.e. $(x, y) \in \mathbb{Q}^2$.

- If $b = 0$, then $L(\mathbb{Q}) = \left\{ \left(-\frac{c}{a}, y \right) \ : \ y \in \mathbb{Q} \right\}$
- If $b \neq 0$, solve for $y = f(x)$, get $L(\mathbb{Q}) = \{ (x, f(x)) \ : \ x \in \mathbb{Q} \}$

Linear curves: $\mathbb{Z}$-points

$L: \ ax + by + c = 0$, with $a \neq 0$ or $b \neq 0$.

Now we restrict to $L(\mathbb{Z})$.

- If $\gcd(a, b)$ divides c, the Euclidean algorithm can determine one $(x_0, y_0) \in L(\mathbb{Z})$, and this can generate all the other solutions.
  Example: $6x + 8y = 10$ has point $(-1, 2)$. The two adjacent points are $(-5, 5)$ and $(3, -1)$.

- If $\gcd(a, b)$ does not divide c, then $L(\mathbb{Z}) = \emptyset$.
  Example: $6x + 8y = 15$ has no integral points.

Quadratic curves: first form

Consider a degree 2 curve $Q_1 : \ y + ax^2 + bx + c = 0$

$Q_1(\mathbb{Q})$: as before, there are always infinitely many.

- For any fixed $x \in \mathbb{Q}$, there is a corresponding $y \in \mathbb{Q}$.
- In contrast, for any fixed $y \in \mathbb{Q}$ there may not be any corresponding $x \in \mathbb{Q}$.

  The discriminant $\sqrt{b^2 - 4a(c+y)}$ gives us sufficient information.

$Q_1(\mathbb{Z})$: not significantly different.
What if y were changed to ky?

Quadratic curves: general form

A general degree 2 curve is defined by

$$q(x,y) = ax^2 + bxy + cy^2 + dx + ey + f$$

Consider the case $C: \ x^2 + y^2 = 1$.

- No non-trivial $\mathbb{Z}$-points, i.e. $C(\mathbb{Z}) = \{(\pm 1, 0), (0, \pm 1)\}$.
- Geometry helps to see $C(\mathbb{Q})$ is infinite.
  - Draw the line through $(-1, 0)$ and $(0, t)$, i.e. $y = t(1 + x)$
  - The other point of intersection (x, y) with C satisfies

$$1 - x^2 = t^2(1 + x)^2$$

  - Get $(x, y) = \left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2}\right)$

Quadratic curves: general form

For $Q: \ ax^2 + bxy + cy^2 + dx + ey + f = 0$ there is a general procedure:

- Decide if some point $(x, y) \in Q(\mathbb{Q})$ exists.
- If not, $Q(\mathbb{Q}) = \emptyset$.
- If $(x_0, y_0) \in Q(\mathbb{Q})$ then $Q(\mathbb{Q})$ is infinite, in the same way as with C above.

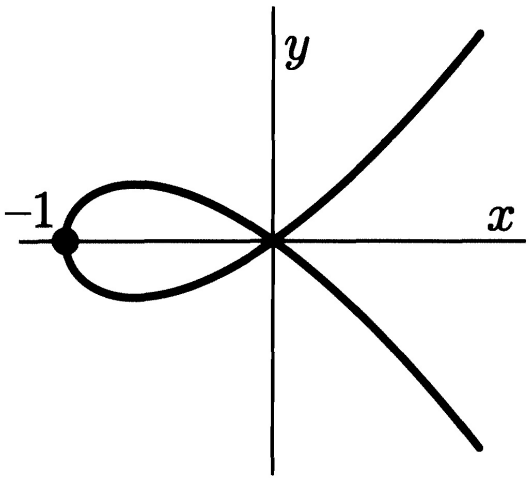
Question

How does one decide if any $(x, y) \in Q(\mathbb{Q})$ exist?

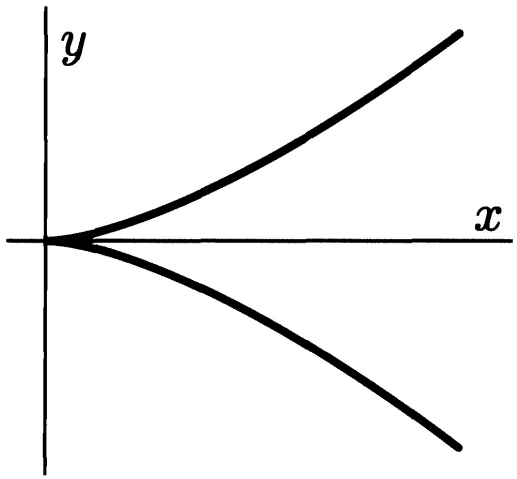
Cubic curves: singular

Consider $E: \ y^2 = x^3 + ax + b$, discriminant $\Delta = 4a^3 + 27b^2$.

Singular cases: $\Delta = 0$, $x^3 + ax + b$ has repeated roots.
$E(\mathbb{Q})$ is determined as quadratics were.



A Singular Cubic with Distinct Tangent Directions

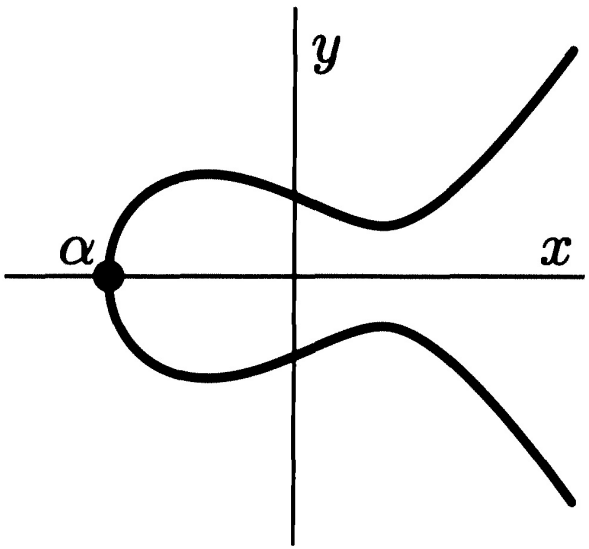


A Singular Cubic with A Cusp

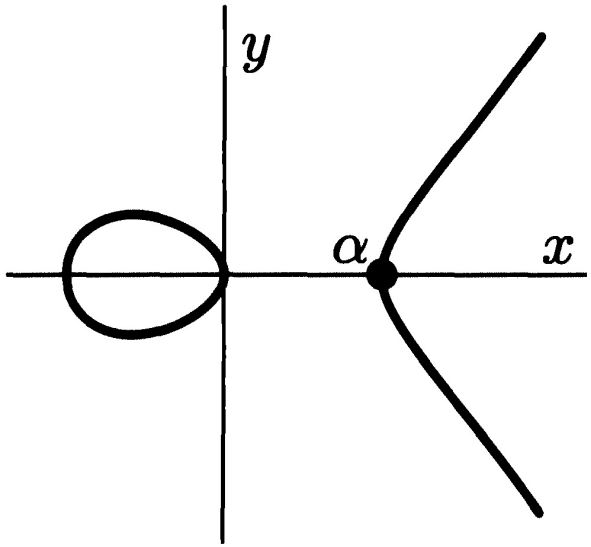
Cubic curves: non-singular

$E: \ y^2 = x^3 + ax + b$, discriminant $\Delta = 4a^3 + 27b^2$.

Non-singular cases: $\Delta \neq 0$, $x^3 + ax + b$ has no repeated roots.
$E(\mathbb{Q})$ is more interesting.



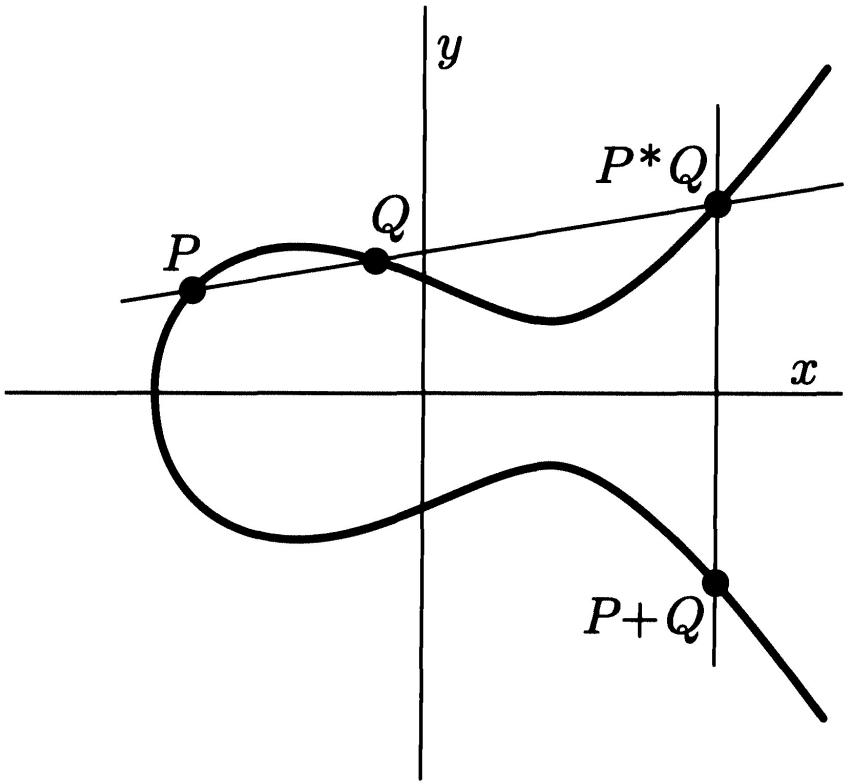
One Real Component



Two Real Components

Structure: geometrically

The set of points $E(\mathbb{Q})$ admits a commutative addition operation



Adding Points on a Weierstrass Cubic

Structure: algebraically

The addition operation makes $E(\mathbb{Q})$ into an Abelian group.

Addition formula: Let $P = (x_1, y_1)$, $Q = (x_2, y_2)$. Then

$$P + Q = (\alpha^2 - x_1 - x_2, \alpha x_3 + \beta)$$

where $y = \alpha x + \beta$ is the line connecting P and Q.

Theorem (Mordell 1922)

The group $E(\mathbb{Q})$ is finitely generated. Thus, $E(\mathbb{Q})$ decomposes

$$E(\mathbb{Q}) \cong E_{tors}(\mathbb{Q}) \times \mathbb{Z}^{r(E,\mathbb{Q})}.$$

The quantity $r(E, \mathbb{Q})$ is known as the (algebraic) *rank* of $E(\mathbb{Q})$.

Mordell's proof

The main steps:

1. Show that $E(\mathbb{Q})/2E(\mathbb{Q})$ is finite.
   - Let $Q_1, \ldots, Q_n$ represent $E(\mathbb{Q})/2E(\mathbb{Q})$.
   - Every $P := P_0 \in E(\mathbb{Q})$ is related to some $2P_1 \in E(\mathbb{Q})$, ...

$$P_i - Q_{i+1} = 2P_{i+1}.$$

2. $\{R \in E(\mathbb{Q}) \ : \ \mathrm{ht}(R) \leq c\}$ is finite for any $c > 0$.
   - height $\mathrm{ht}(P)$ measures complexity: $\mathrm{ht}\left(\frac{a}{b}\right) = \max(|a|, |b|)$.
   - $\mathrm{ht}(2P) \geq 4\mathrm{ht}(P) -$ (some uniform constant)
   - Sequence $P = P_0, P_1, \ldots, P_n$ is decreasing in height, eventually lands in a finite set.

Complex Structure

One can also consider $E(\mathbb{C})$. The key facts:

- For $L = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ a complex lattice, $\mathbb{C}/L$ is a torus.
- Doubly-periodic $\mathfrak{p}(z+\omega) = \mathfrak{p}(z)$ for any $\omega \in L$

$$\mathfrak{p}(z) := \frac{1}{z^2} + \sum_{0 \neq \omega \in L} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right)$$

- The $\mathfrak{p}$-function satisfies the differential equation

$$\mathfrak{p}'^2 = 4\mathfrak{p}^3 - g_2\mathfrak{p} - g_3$$

- $\mathfrak{p}$ defines an analytic isomorphism

$$F : \mathbb{C}/L \to E(\mathbb{C}) : \; z \mapsto \left(\mathfrak{p}(z), \mathfrak{p}'(z)\right)$$

Endomorphisms

(Algebro-Geometric) From the addition law, there are functions $[n] : E(\mathbb{C}) \to E(\mathbb{C})$ for each $n \in \mathbb{N}$

$$[n] : E \to E : \ P \mapsto n \cdot P$$

(Complex) Since $L = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$, multiplication by n maps L to L and hence preserves $\mathbb{C}/L$.

These *endomorphisms* are usually the only maps on E, not always.

Example: Complex multiplication

Take $E(\mathbb{C})$ corresponding to $L = \mathbb{Z} + \mathbb{Z}i$. Multiplication by i also sends L to L.

Communicating Securely: RSA

Question

How does one communicate securely without prior interaction?

- Bob fixes private information: two (large) primes p and q, then forms $N = pq$, and positive integers e, d such that $ed \equiv 1 \pmod{\Phi(N)}$
- Bob posts e publicly, to communicate message m securely with Bob, transmit m^e
- Security relies on the difficulty in factoring a large integer, e.g. N.
- Broken by quantum computers using Shor's algorithm.

Communicating Securely: Abstract Requirements

Question

What is the necessary structure for this encryption system?

1. Closure under multiplication: to ensure m^e is still meaningful
2. Cyclic structure: to *efficiently* remove the exponent e
3. Solve a linear equation (congruence really): to know *how* to remove the exponent e
4. Difficult problem: complexity of factoring and hence of undoing exponentiation

Curves with structure

Question

How does one emulate RSA encryption with points on E?

1. Closure under addition/multiplication by n on rational points.
2. Cyclic structure (yet to be seen)
3. Essentially the same linear equation to decrypt
4. Difficult problem: undoing addition on points of E is intractable

Torsion

From Mordell's Theorem, one piece of $E(\mathbb{Q})$ is the set of torsion points

$$E_{tors}(\mathbb{Q}) = \{P \in E(\mathbb{Q}) \ : \ nP = \mathcal{O} \text{ for some } n > 0\}.$$

Theorem (Mazur 1977)

$E_{tors}(\mathbb{Q})$ must be (isomorphic to) one of the following:

$$\begin{array}{ll} \mathbb{Z}/N\mathbb{Z} & 1 \leq N \leq 10 \text{ or } N = 12 \\ \mathbb{Z}/N\mathbb{Z} \times \mathbb{Z}/(2N)\mathbb{Z} & 1 \leq N \leq 4 \end{array}$$

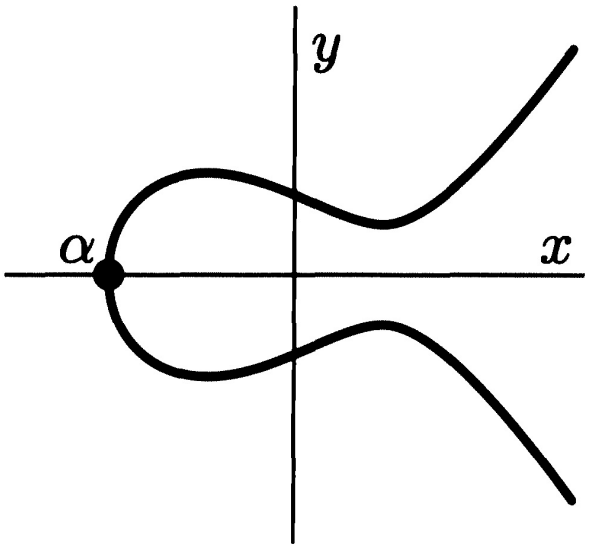
Moreover, all of these possibilities do occur.

$E(\mathbb{Q})[2]$: 2-torsion

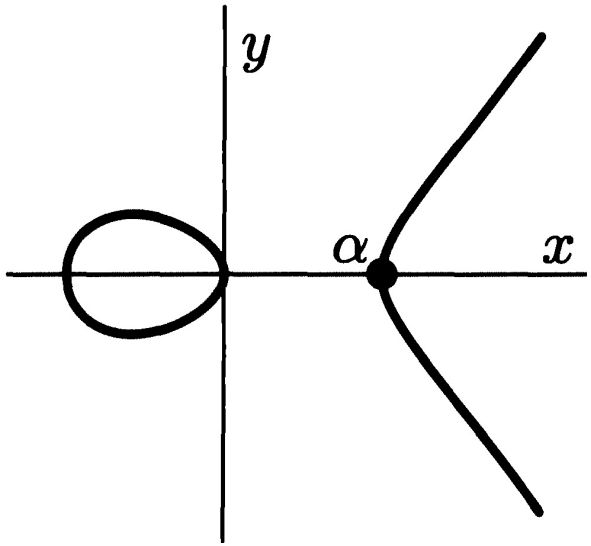
Detecting points $P \in E(\mathbb{Q})$ such that $2P = \mathcal{O}$ is easy.

- If $2P = \mathcal{O}$, the tangent line at P has third intersection at $\mathcal{O}$.
- Such tangent lines are vertical.
- From the graph, these occur at points on the x-axis.

Hence, $E(\mathbb{Q})[2] = \{P \in E(\mathbb{Q}) \ : \ y(P) = \mathcal{O}\}$.



One Real Component



Two Real Components

$E(\mathbb{Q})[3]$: 3-torsion

Detecting points $P \in E(\mathbb{Q})$ such that $3P = \mathcal{O}$ requires use of addition formulas.

- $3P = \mathcal{O}$ iff $2P = -P$ iff $x(2P) = x(-P) = x(P)$.
- From our addition formula $x(2P)$ can be determined explicitly.
- Some algebra yields $x(2P) = x(P)$ iff $x(P)$ satisfies a polynomial $\psi_3(x)$ of degree 4.

Hence, $E(\mathbb{Q})[3]$

- Consists of $(x, y) \in \mathbb{Q}^2$ where $\psi_3(x) = 0$.
- Has at most 9 points

Complex torsion

If we consider $E(\mathbb{C})$ then the connection with $\mathbb{C}/L$, with $L = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$, is very useful.

For $\tilde{z} \in \mathbb{C}/L$:

- $n\tilde{z} = \tilde{0}$ iff $nz \in L$
- $nz \in L$ iff $z = \frac{k_1}{n}\omega_1 + \frac{k_2}{n}\omega_2$

Hence, $E(\mathbb{C})[n] \cong (\mathbb{Z}/n\mathbb{Z})^2$.

Integer points

Unfortunately, $E(\mathbb{Z})$ is not as well-structured as $E(\mathbb{Q})$.

Theorem (Siegel 1928)

The set $E(\mathbb{Z})$ is finite.

Theorem (Nagell 1935, Lutz 1937)

Recall $E: y^2 = x^3 + ax + b$, $a, b \in \mathbb{Z}$. If $P \in E(\mathbb{Q})_{tors}$ then

1. $P \in E(\mathbb{Z})$
2. $y(P) = 0$ and $P \in E(\mathbb{Q})[2]$ or $y(P) \mid \Delta$.

Finite fields

For a prime number p, let $\mathbb{F}_p$ denote $\mathbb{Z}/p\mathbb{Z}$ (a finite field).

Defining the curve E by a polynomial works just as well in this setting. The set $E(\mathbb{F}_p)$ is defined in the same way, and still admits an addition law.

- The geometric definition of addition is no longer meaningful.
- The algebraic formulas for addition still hold.
- $E(\mathbb{F}_p)$ is automatically finite.

Question

How many points can $E(\mathbb{F}_p)$ have?

Hasse bound

There are p choices for $x(P)$ in $\mathbb{F}_p$:

- $x(P) = 0$ yields $(0, 0) \in E(\mathbb{F}_p)$
- $x(P) \neq 0$ and not a square in $E(\mathbb{F}_p)$ yields no points.
- $x(P) \neq 0$ and a square in $E(\mathbb{F}_p)$ yields two points.

One expects half of the values in $\mathbb{F}_p$ to be squares, hence $p + 1$ points in $E(\mathbb{F}_p)$.

Theorem (Hasse 1933)

$|\#E(\mathbb{F}_p) - (p + 1)| < 2\sqrt{p}$.

Reduction $\pmod p$

If $E: \ y^2 = x^3 + ax + b$ has $a, b \in \mathbb{Z}$ then one can reduce the equation $\pmod p$, and define a new curve $\tilde{E}$.

- If $P \in E(\mathbb{Q})_{tors}$ the Nagell-Lutz says $P \in E(\mathbb{Z})$.
- If $P = (x, y)$ then $\tilde{P} = (\tilde{x}, \tilde{y}) \in \tilde{E}(\mathbb{F}_p)$.
- If $P \neq \mathcal{O}$ then $\tilde{P} \neq \tilde{\mathcal{O}}$.

Hence $\pi : E(\mathbb{Q})_{tors} \hookrightarrow \tilde{E}(\mathbb{F}_p)$ is well-defined, one-to-one.

Reduction Lemma

For almost all p, $E(\mathbb{Q})_{tors}$ is a subgroup of $\tilde{E}(\mathbb{F}_p)$.

Example: $E(\mathbb{Q})$ is finite

Consider $E: \ y^2 = x^3 + x$. One can determine $E(\mathbb{Q})$ completely.

- For $p \geq 3$, the Reduction Lemma applies.
- $\tilde{E}(\mathbb{F}_3) = \left\{\tilde{\mathcal{O}}, (0,0), (2,1), (2,2)\right\}$
- $\tilde{E}(\mathbb{F}_5) = \left\{\tilde{\mathcal{O}}, (0,0), (2,0), (3,0)\right\}$
- For this curve, Sage (e.g.) can verify that $E(\mathbb{Q})$ is finite.

From this data, $E(\mathbb{Q}) = E(\mathbb{Q})_{tors} = \{\mathcal{O}, (0,0)\}$.

Example: $E(\mathbb{Q})$ is infinite

Consider $E: \ y^2 = x^3 + 3$. We can prove $E(\mathbb{Q})$ is infinite.

- For $p \geq 5$, the Reduction Lemma applies.
- $\#\tilde{E}(\mathbb{F}_5) = 6$ and $\#\tilde{E}(\mathbb{F}_7) = 13$.
- $\#E(\mathbb{Q})_{tors}$ must divide 6 and 13, so $\#E(\mathbb{Q})_{tors} = 1$.
- By inspection, $(1, 2) \in E(\mathbb{Q})$

From this data, $(1, 2)$ is a point of infinite order, so $E(\mathbb{Q})$ is infinite.

Cryptographic requirements

Recall the requirements for cryptography:

1. Closure under addition/multiplication by n on rational points.
2. Cyclic structure (yet to be seen)
3. Essentially the same linear equation to decrypt
4. Difficult problem: undoing addition on points of E is intractable

Conditions (2) and (4) imply that only $E(\mathbb{F}_p)$ has a chance of being useful.

Sufficient Conditions

Recall: $|\#E(\mathbb{F}_p) - (p+1)| < 2\sqrt{p}$ (Hasse bound)

Plan of attack:

For (4), we ensure that $\#E(\mathbb{F}_p)$ is large

For (2), we ensure that $\#E(\mathbb{F}_p)$ is a prime (ensures cyclic)

Two approaches:

1. Pick a random curve E over $\mathbb{F}_p$, count the points, decide if it is good.
2. Construct a curve E with a prescribed number of points.

Frobenius Φ_p

Fix a prime p.
Over any finite field $\mathbb{F}_q$, $q = p^n$, there is a Frobenius map

$$\Phi_p : E \to E : \ (x, y) \mapsto (x^p, y^p).$$

Two Facts:

- (Fermat's Little Theorem) $\alpha \in \mathbb{F}_p$ implies $\alpha^p = \alpha$.
- $E(\mathbb{F}_p) = \{(x, y) \ : \ x^p = x, \ y^p = y\} = \ker(1 - \Phi_p)$.

Theorem: Characteristic polynomial of Frobenius

Φ_p satisfies $\varphi^2 - a\varphi + p = 0$ where $a = p + 1 - E(\mathbb{F}_p)$.

Schoof's Algorithm

Frobenius Φ_p: $\Phi_p^2 - a\Phi_p + p = 0$

Main idea to obtain a:

- Determine enough small primes ℓ_i such that $\Pi_i \ell_i > 4\sqrt{p}$.
- Use the Chinese Remainder Theorem to find unique $a \pmod{\Pi_i \ell_i}$ in the appropriate range.

Technicalities:

- Compute $R_i = \Phi_p(P_i)$ for $P \in E[\ell_i]$
- Compute $Q_i = \Phi_p^2(R_i) + [p]R_i \in E[\ell]$
- Determine some $a_i \pmod{\ell_i}$ such that $Q_i = [a_i]R_i$.

Generating a curve: CM

Facts:

- If $\tau \in \mathbb{C}$ is quadratic, with $\text{disc}(\tau) = -D$ then the elliptic curve E corresponding $\mathbb{C}/(\mathbb{Z} + \mathbb{Z}\tau)$ has complex multiplication by $\mathbb{Z}[\sqrt{-D}]$.
- There is a complex function j such that the minimal polynomial $H_D(x)$ of $j(\tau)$ has integer coefficients.
- The reduction of $H_D(x)$ has a root $j_0 \in \mathbb{F}_p$ which corresponds to an elliptic curve E

Generating a curve: Algorithm

Procedure:

- Choose an N which you want to be $\#E(\mathbb{F}_p)$ for some p.
- Create a list of primes ℓ_i such that N is a square $\pmod{\ell_i}$, create $D = \Pi_i \ell_i$.
- Find solutions x and y to $x^2 - Dy^2 = 4N$.
- Test whether $p = N + 1 \pm x$ is prime. If so, compute $H_D(x)$ and a root j_0 in $\mathbb{F}_p$.

Thank you for your attention.

Good resources:

- Silverman J., Tate J. *Rational Points on Elliptic Curves*. Springer, 1992.
- Silverman J. *Arithmetic of Elliptic Curves*. 2nd ed. Springer, 2009.
- Washington, L. Elliptic Curves: Number Theory and Cryptography. Chapman and Hall, 2003.