Decrypting Elliptic Curves...

Benjamin Brown

3rd July 2020

THE UNIVERSITY of EDINBURGH

Ellipses

After circles, ellipses are the most familiar curves in mathematics.

Figure: St Patrick's Square.

copy page over

Elliptic Functions

Arc-length of an ellipse?

$$x = a\cos\theta, \quad y = b\sin\theta$$

$$\begin{aligned} L &= \int_0^{2\pi} \sqrt{(\partial_\theta x)^2 + (\partial_\theta y)^2}\, d\theta \\ &= 4a\int_0^1 \sqrt{1 - e^2u^2}\, du \quad (e^2 = (a^2 - b^2)/a^2; \quad u = \sin\theta) \\ &= \frac{1}{2}\int_{1-e^2}^1 \frac{t\, dt}{\sqrt{t(t-1)(t-(1-e^2))}} \quad (t = 1 - e^2u^2) \end{aligned}$$

Something Nicer...

Pendulum motion under gravity (suitable units):

$$\dot{\theta}^2 - \cos\theta = E,$$

with E the energy and θ the amplitude angle.

Thus

$$\dot{\theta} = \frac{d\theta}{dt} = \sqrt{E + \cos\theta},$$

and

$$t = \int dt = \int \frac{d\theta}{\sqrt{E + \cos\theta}} = \int \frac{du}{\sqrt{(E+u)(1-u^2)}}$$

for $u = \cos\theta$.

Integrals of the form

$$w = f(z) = \int_P^z \frac{dt}{\sqrt{c_3 t^3 + c_2 t^2 + c_1 t + c_0}}$$

are called *elliptic integrals*.

Elliptic functions are the inverses to elliptic integrals, $z = f^{-1}(w)$.

Analogous to $\sin^{-1}(x) = \int \frac{1}{\sqrt{1-x^2}}$.

Elliptic integrals have no solution involving only elementary functions.

Denominator is a *square-root* with solution set:

$$E := \left\{(x, y) \in \mathbb{C}^2 : y^2 = x(x-1)(x-\lambda)\right\}.$$

This is called the *Legendre form* of an elliptic curve.

Problem: there is no single-valued function

$$y = \pm\sqrt{f(x)} = \pm\sqrt{x(x-1)(x-\lambda)}$$

on the whole of $\mathbb{C}$!
(two sheet figure)

The two sheets coincide though at $x = 0, 1, \lambda$, and ∞.

Integrating around each of these points sends
$\sqrt{f(x)} \longmapsto -\sqrt{f(x)}$.

We make $\sqrt{f(x)}$ single-valued, we glue the sheets using cuts from 0 to 1, and from λ to ∞.

(Figure)

(Figure)

Integrating $\int \frac{dx}{\sqrt{y}}$ is now well-defined up to cycles around branch cuts,

$$\omega_1 := \int_\alpha \frac{dx}{\sqrt{y}}, \qquad \omega_2 := \int_\beta \frac{dx}{\sqrt{y}}.$$

If we mod out the image of $\int \frac{dx}{\sqrt{y}}$ by $\mathrm{Span}_{\mathbb{Z}}\{\omega_1, \omega_2\}$, get a map

$$E(\mathbb{C}) \longrightarrow \mathbb{C}/(\omega_1 \cdot \mathbb{Z} + \omega_2 \cdot \mathbb{Z}).$$

The Group Law

Property of a cubic curve E: any line L intersects E in at most 3 points.

Pick a marked point $\mathcal{O} \in E$ to serve as the identity (usually ∞ is chosen).

Reminder: an abelian group G is a set with a binary operation $+ : G \times G \to G$ with:

- Identity, $0 \in G$;
- An inverse to each element, for each $g \in G$, there is a $-g \in G$;
- Closure, i.e. the $+$ operation does not leave the group;
- Associativity, i.e. $(a + b) + c = a + (b + c)$;
- $+$ is commutative, i.e. $a + b = b + a$.

Chord and Tangent

For two points $P, Q \in E$, connect them via a line L. This line L intersects E once more at a point we call $P * Q$. Then we define $P + Q = -(P * Q)$.

Point at Infinity

"*Homogenise*" the equation:

$$y^2 = x(x-1)(x-\lambda) \longmapsto y^2 z = x(x-z)(x-\lambda z).$$

i.e., introduce powers of a new coordinate z so every term has degree 3.

Point at infinity obtained by setting $z = 0$, so in the above, $\infty = (0, y, 0)$.

Finite Fields

Elliptic curve addition can be defined over any field.

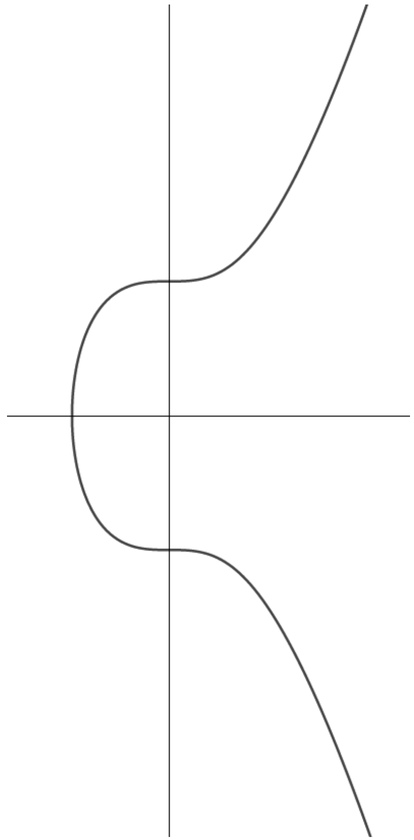
A field is a "nice" ring, *e.g.* $\mathbb{Q}, \mathbb{R}, \mathbb{C}$. These are *infinite fields*.

There are also *finite fields*, say $\mathbb{Z}_2, \mathbb{Z}_3, \ldots$.

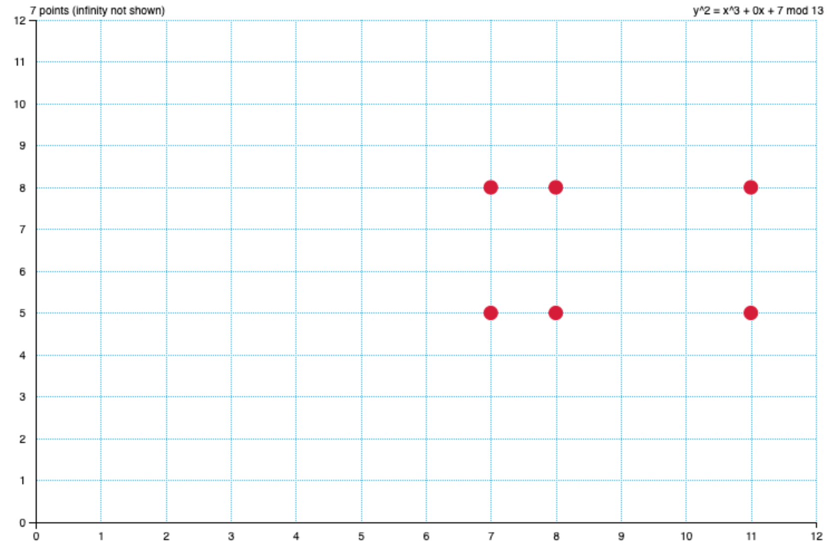
In general $\mathbb{Z}_{p^k}$, with p a prime number and $k \geq 1$, are all fields.

In $\mathbb{Z}_p$ arithmetic is done modulo p.

Elliptic curves look very different over a finite field $\mathbb{F}_p$!



(a) $y^2 = x^3 + 7$ over $\mathbb{R}$



(b) $y^2 = x^3 + 7$ over $\mathbb{F}_{13}$

Figure: Secp256k1 elliptic curve.

Point $(7, 5)$, we have
$7^3 + 7 = 343 + 7 = 13 \cdot 26 + 12 \equiv 12 \mod 13$, and
$5^2 = 25 \equiv 12 \mod 13$.

Cryptography

Cryptography is the process of writing using various methods, ciphers, to keep messages secret.

Example: Caesar Cipher (very insecure!)

- “Decrypting elliptic curves” $\mapsto$ “Ghfubswlqj hoolswlf fxuyhv”.

Usage Cases

- Public-Key Signatures (RSA, ECDSA); signed OS updates, SSL certificates, e-Passports.
- Public-Key Encryption (RSA, ECDH); SSL key exchange.

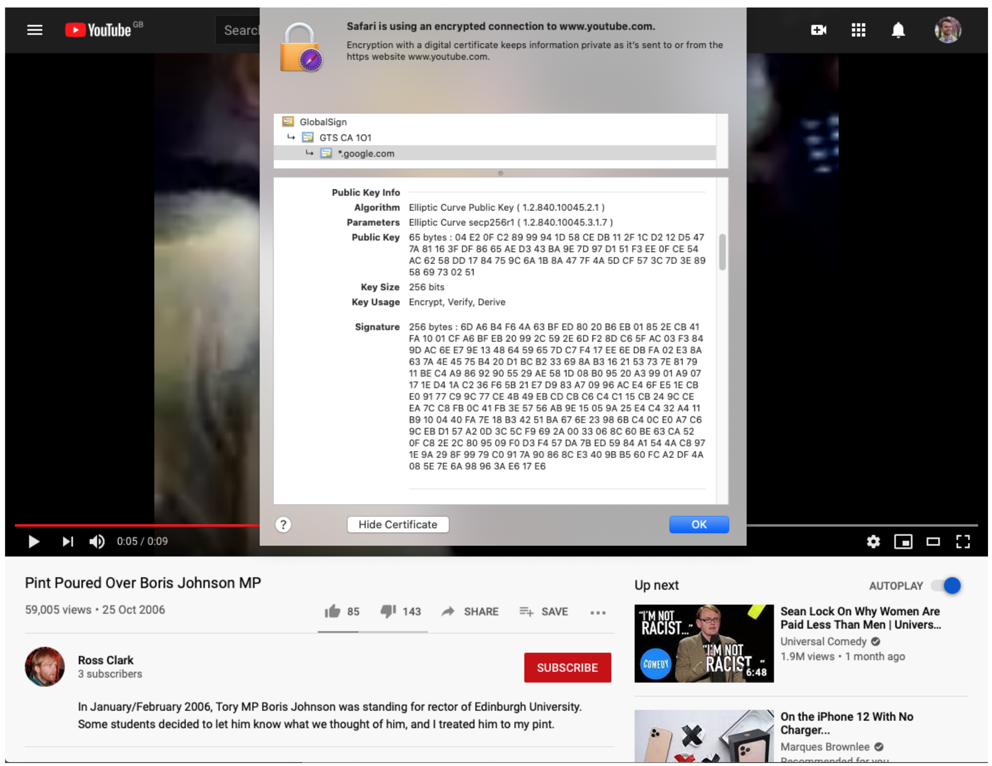


Figure: Elliptic Curve Digital Signature Algorithm.

Diffie-Hellman Key Exchange

Standardise a large prime p and base point $(x, y) \in E(\mathbb{F}_p)$.

Alice chooses a big secret a, and computes her public key $a(x, y)$.

Bob chooses a big secret b, and computes his public key $b(x, y)$.

Alice computes $a \cdot \big(b(x, y)\big)$.

Bob computes $b \cdot \big(a(x, y)\big)$.

They use this shared secret to encrypt via a cipher.

Draw figure.

Discrete Logarithm Problem

Someone observing this exchange would only know what $E(\mathbb{F}_p), a(x, y), b(x, y)$ and $ab(x, y)$ are.

If we set $g = (x, y)$, Alice's public key is $g^a = k$.

To find her private key a, need to solve for

$$\log_g k = a \mod p.$$

This is the *discrete logarithm problem*, and solving it is as difficult as trying a brute-force approach, i.e. trying all possible values of a.

How Long?

The private key *a* can be any number in $[0, 2^{256}]$, where $2^{256} \sim 1.1576 \times 10^{77}$.

That is, the size of the private key space has 10^{77} decimals following it.

On the other hand, the number of atoms in the visible Universe is $\sim 10^{80}$.

Elliptic curve multiplication provides a *trap-door function*; easy to calculate in only one direction.