p-adic attacks on elliptic curves

Overdrive Hacking Conference 2019

Enric Florit

Who am I?

Enric Florit

- Maths + CS student at University of Barcelona
- I do number theory and cryptography
- Member of Hacking Lliure

HACKING
LLIURE

Introduction

What are Elliptic Curves?

Elliptic Curve Cryptography

Attacking ECC

The p-adic attack

Public-key cryptography

We want to

- Exchange keys (for symmetric crypto)
- Sign data
- Encrypt things?

RSA

RSA is easier to understand, it's basic modular arithmetic:

- Take two **large** primes $\check{E}$ and $\hat{G}$, set $\wedge = \check{E} \times \hat{G}$ and $\varphi(\wedge) = (\check{E} - 1)(\hat{G} - 1)$.
- Choose $\hat{U}$ between 1 and $\varphi(\check{E}\hat{G})$ such that $\gcd(\hat{U}, \varphi(\check{E}\hat{G})) = 1$.
- Compute $\times \equiv \hat{U}^{-1} \mod \varphi(\check{E}\hat{G})$.
- $\check{E}\check{\imath}Đ = (\wedge, \hat{U})$, $\check{E}\hat{g}\hat{\imath}\kappa = (\check{E}, \hat{G}, \times)$.

The equation of an elliptic curve

An elliptic curve is the set of points (l', L) in the plane that satisfy the equation

$$L^2 = l'^3 + \quad l' + *,$$

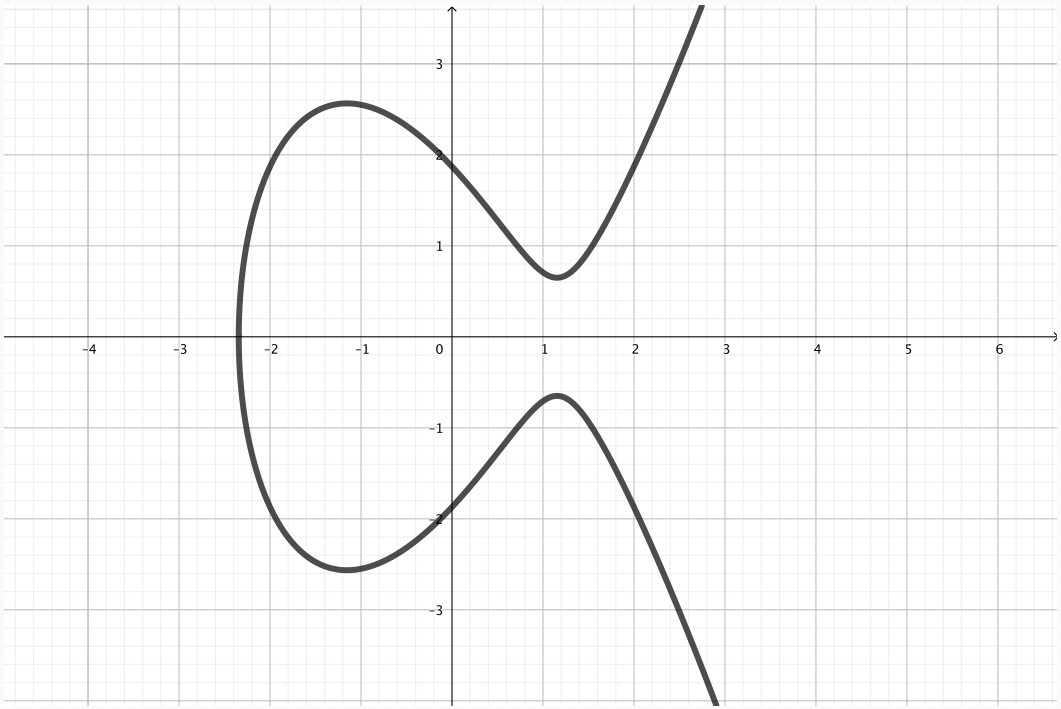
where , * are constants[1] (integer, rational, real, complex...).

[1] With $4 \ ^3 + 27*^2 \neq 0$

The graph of an elliptic curve

$$L^2 = l'^3 - 4l' + \frac{7}{2}$$

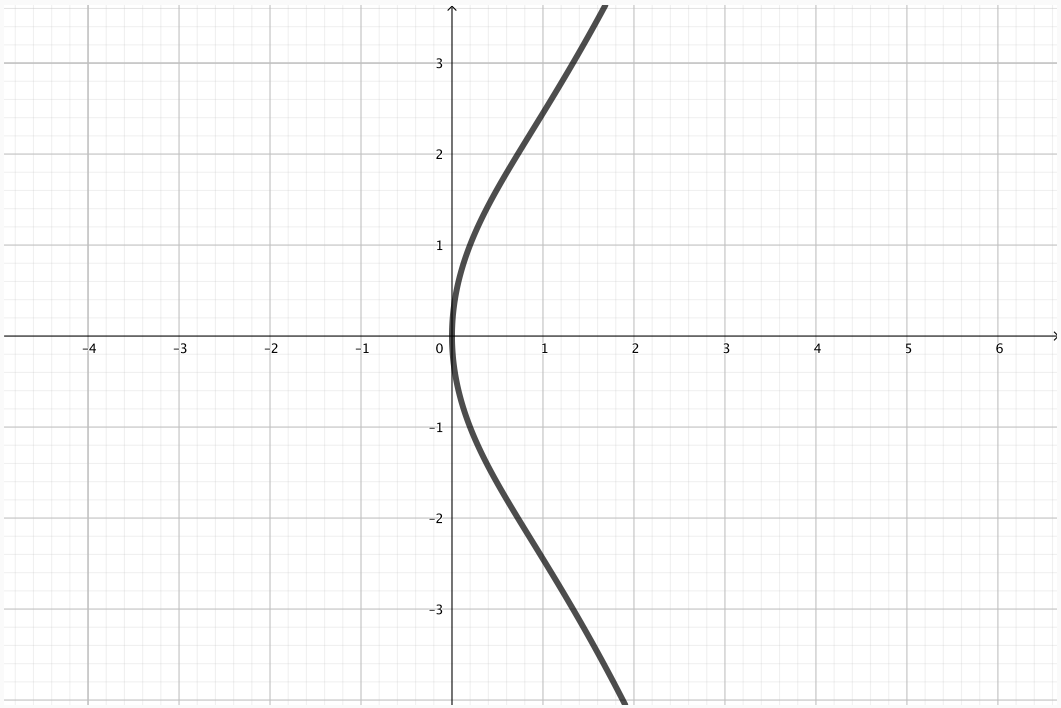
If we plot this curve, we have a picture like this:



The graph of an elliptic curve

$$L^2 = l^3 + 5l$$

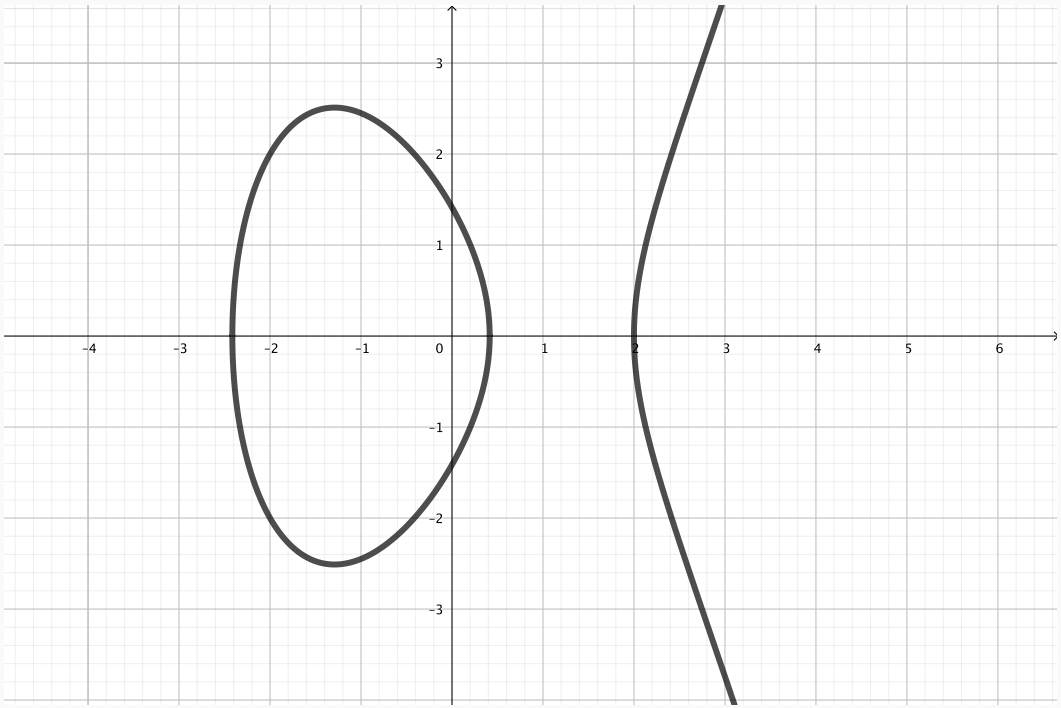
If we plot this curve, we have a picture like this:



The graph of an elliptic curve

$$L^2 = l^3 - 5l + 2$$

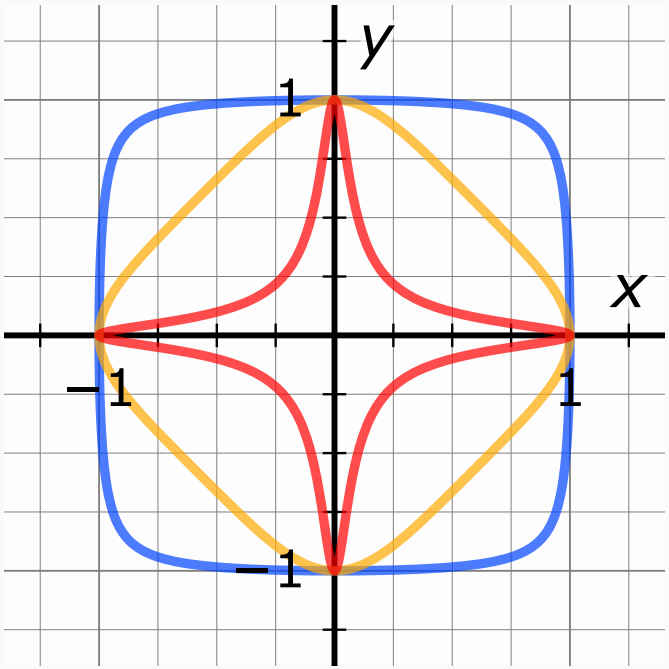
If we plot this curve, we have a picture like this:



There exist other equations

We could also work with other **equivalent** curves

$$l'^2 + L'^2 = 1 - \times l'^2 L'^2$$

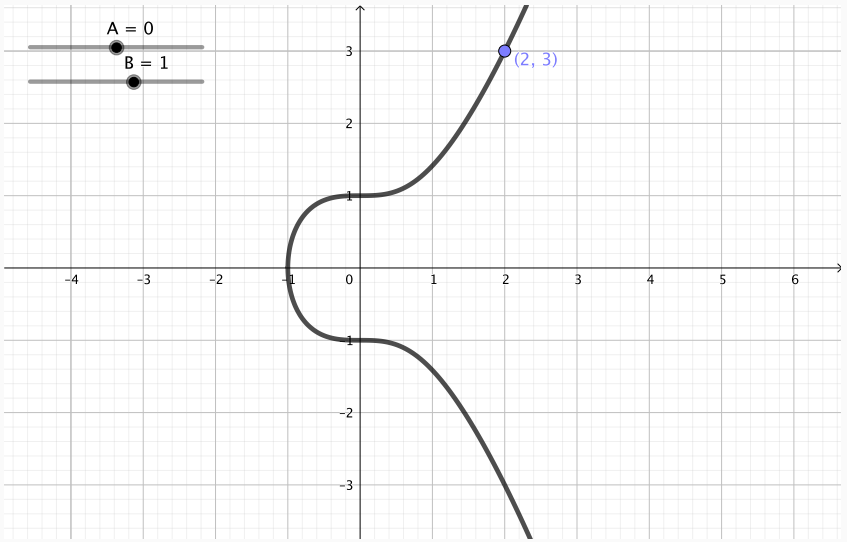


Edwards curves with $\times = 300$ (red), $\times = \sqrt{8}$ (yellow) and $\times = -0.9$ (blue)[2]

[2] https://commons.wikimedia.org/wiki/File:Edward-curves.svg

The graph of an elliptic curve

We say a point (l', L) is on the curve if it satisfies the equation $L^2 = l'^3 + \quad l' + *$.



For example $(2, 3)$ satisfies

$$\begin{cases} l'^3 + 1 = 2^3 + 1 & = 9 \\ L^2 = 3^2 & = 9 \end{cases} \implies y^2 = x^3 + 1.$$

Sum of points

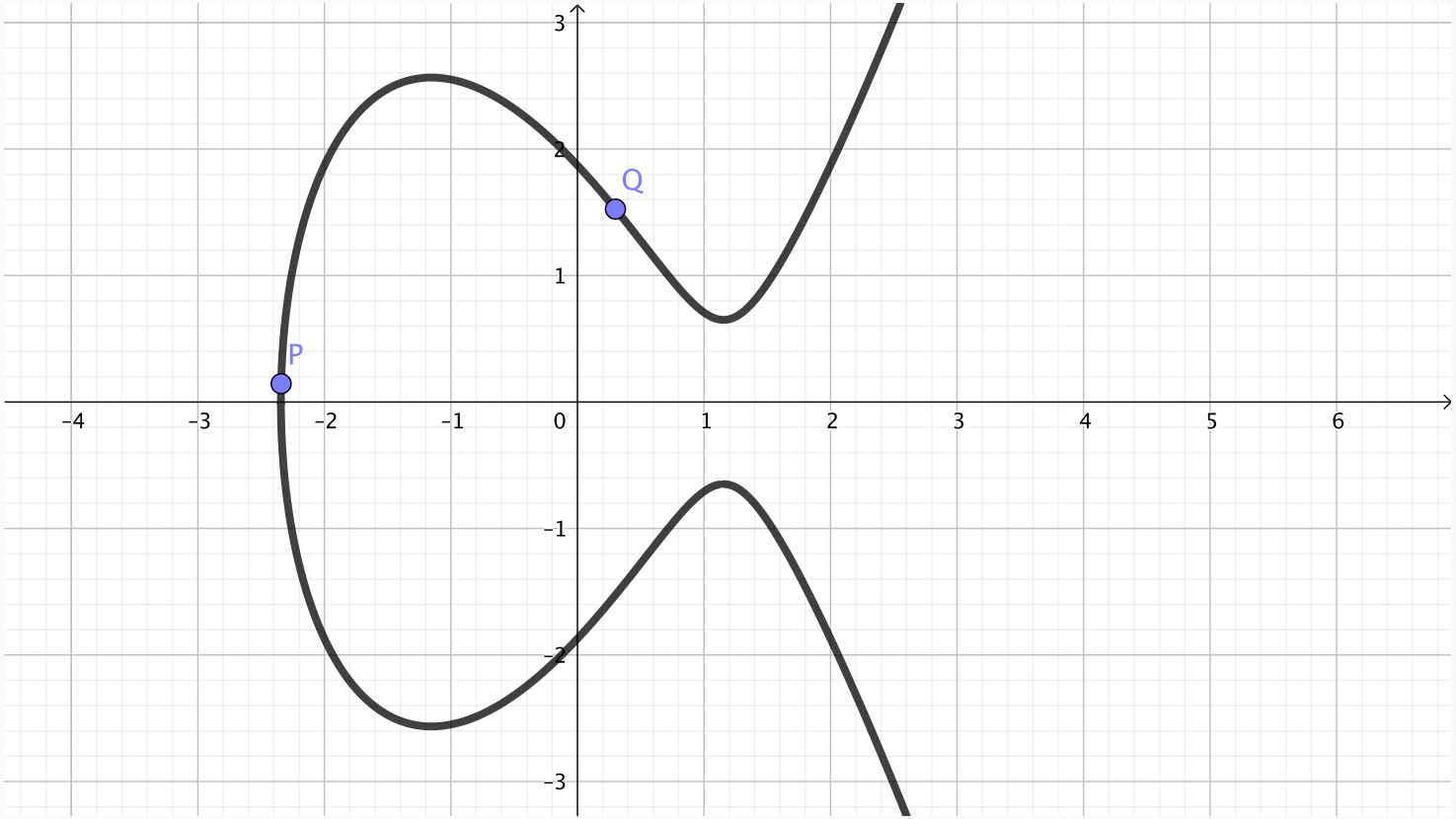
We care about elliptic curves because we can **add points**.

$$E\check{\imath}\ddot{e}\Bbbk 0\ +\check{D}\check{D}\hat{g}\times\hat{\imath}\acute{c}\ddot{A}\tilde{I}\hat{U}\hbar\acute{L}\hat{\imath}\dot{g}\hat{U}\ \dot{g}\check{\imath}\ \acute{C}\Bbbk 0\ \wedge\check{D}\flat$$

We are going to add pairs of points **geometrically**.

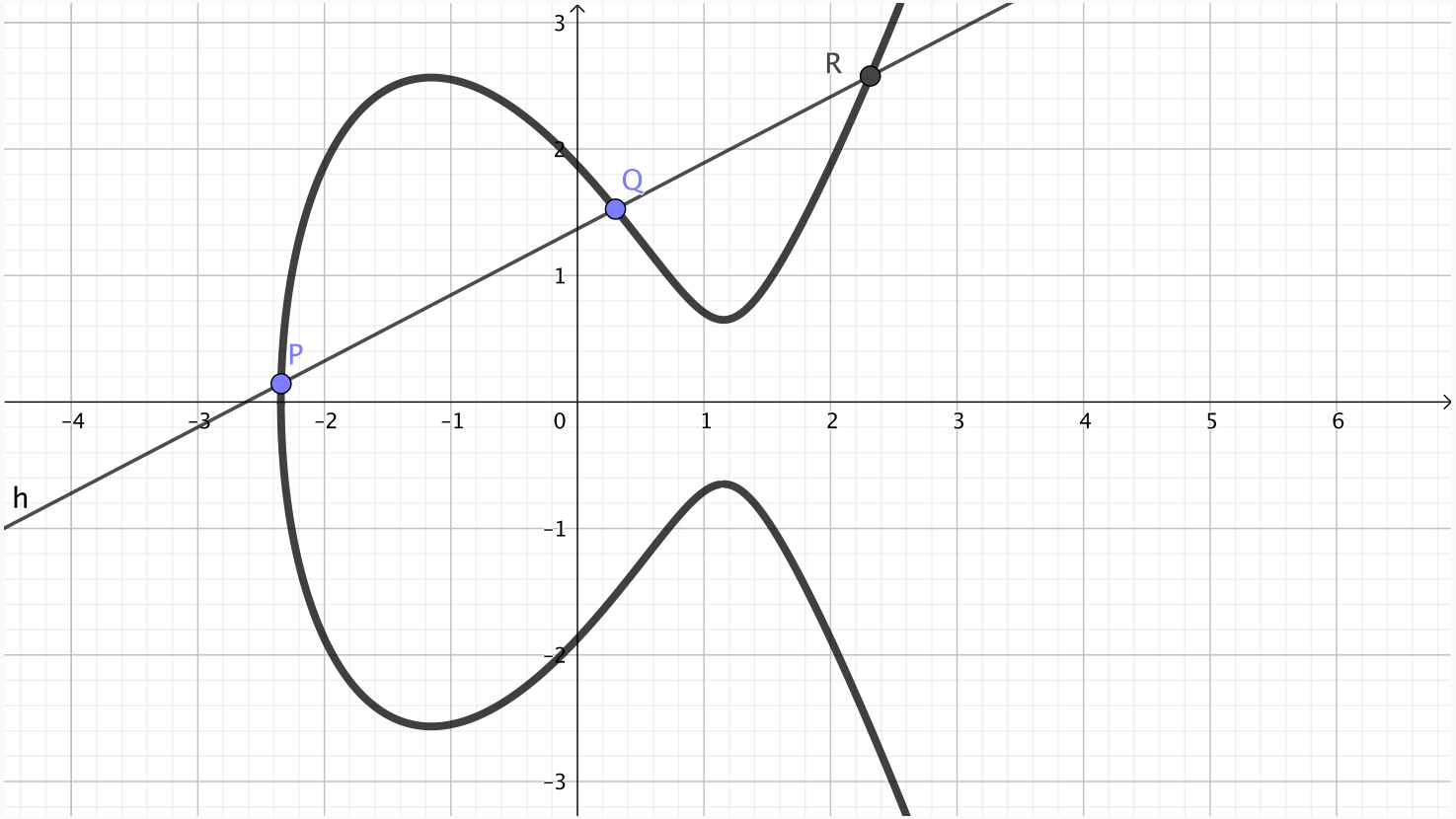
Sum of points

1. Pick a pair of points



Sum of points

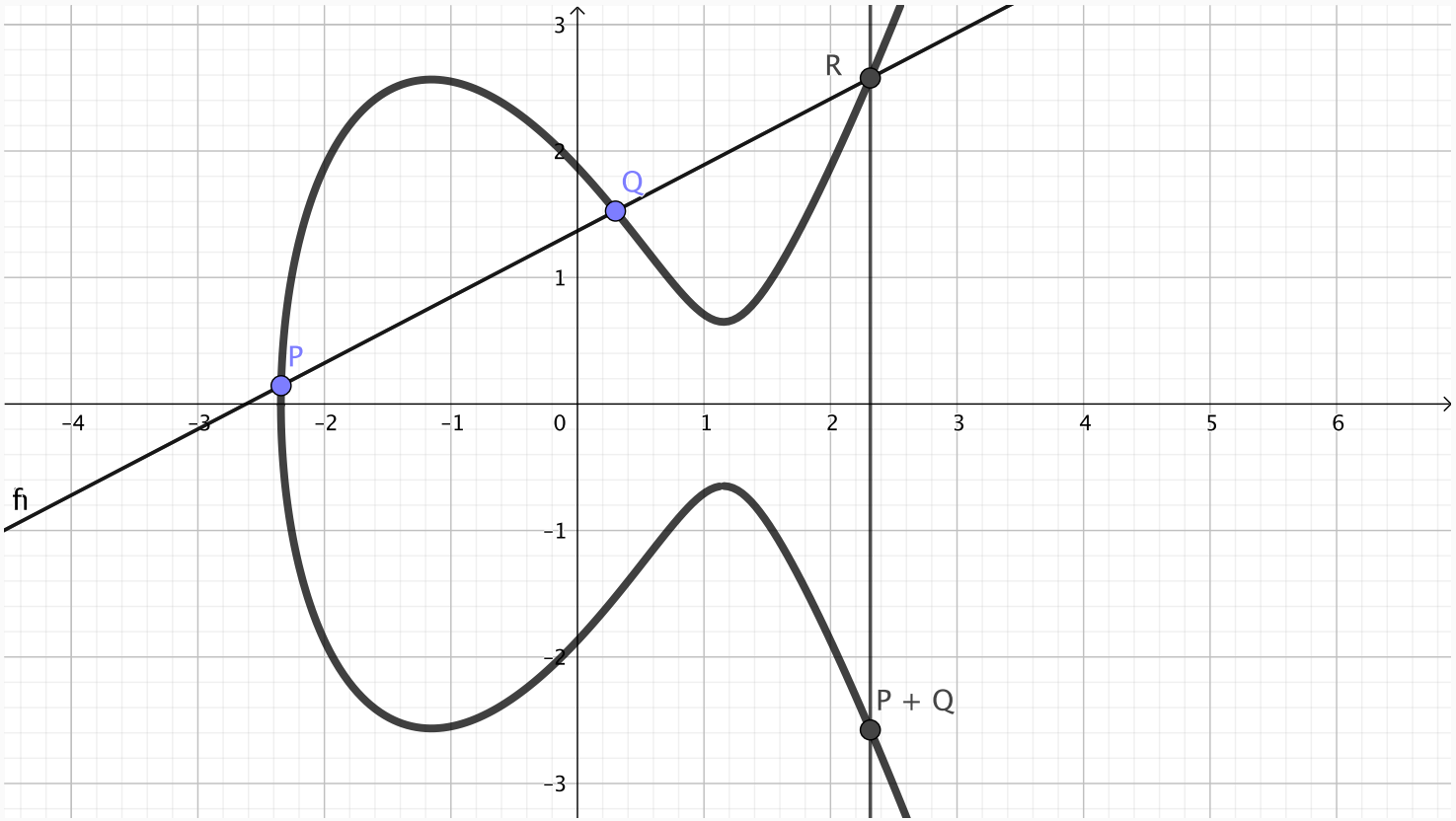
2. Draw a straight line through them



(it intersects the curve again!)

Sum of points

3. Reflect the third point s vertically to get $p + r$

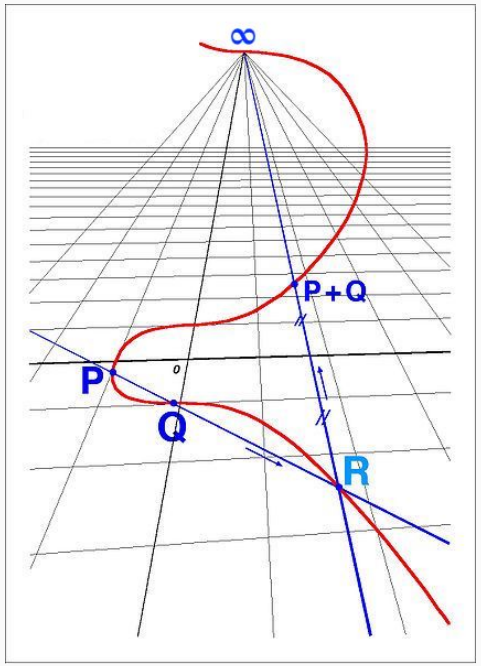


The Point Infinity

We also consider a point at infinity, under the rule

$$p + \infty = p$$

It is visualized like so

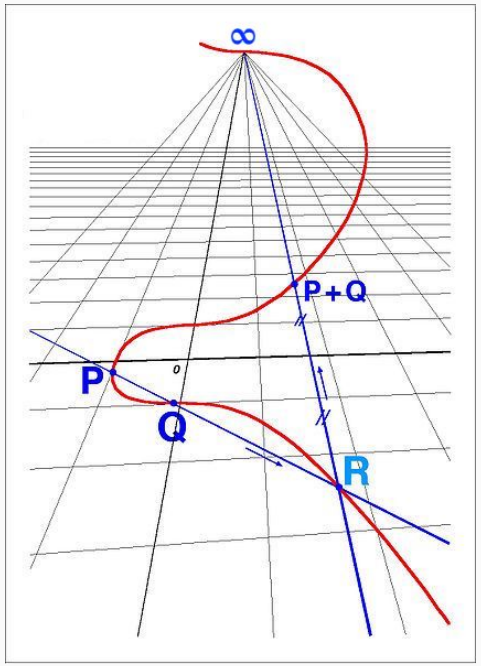


The Point Infinity

We also consider a point at infinity, under the rule

$$p + \infty = p$$

It is visualized like so



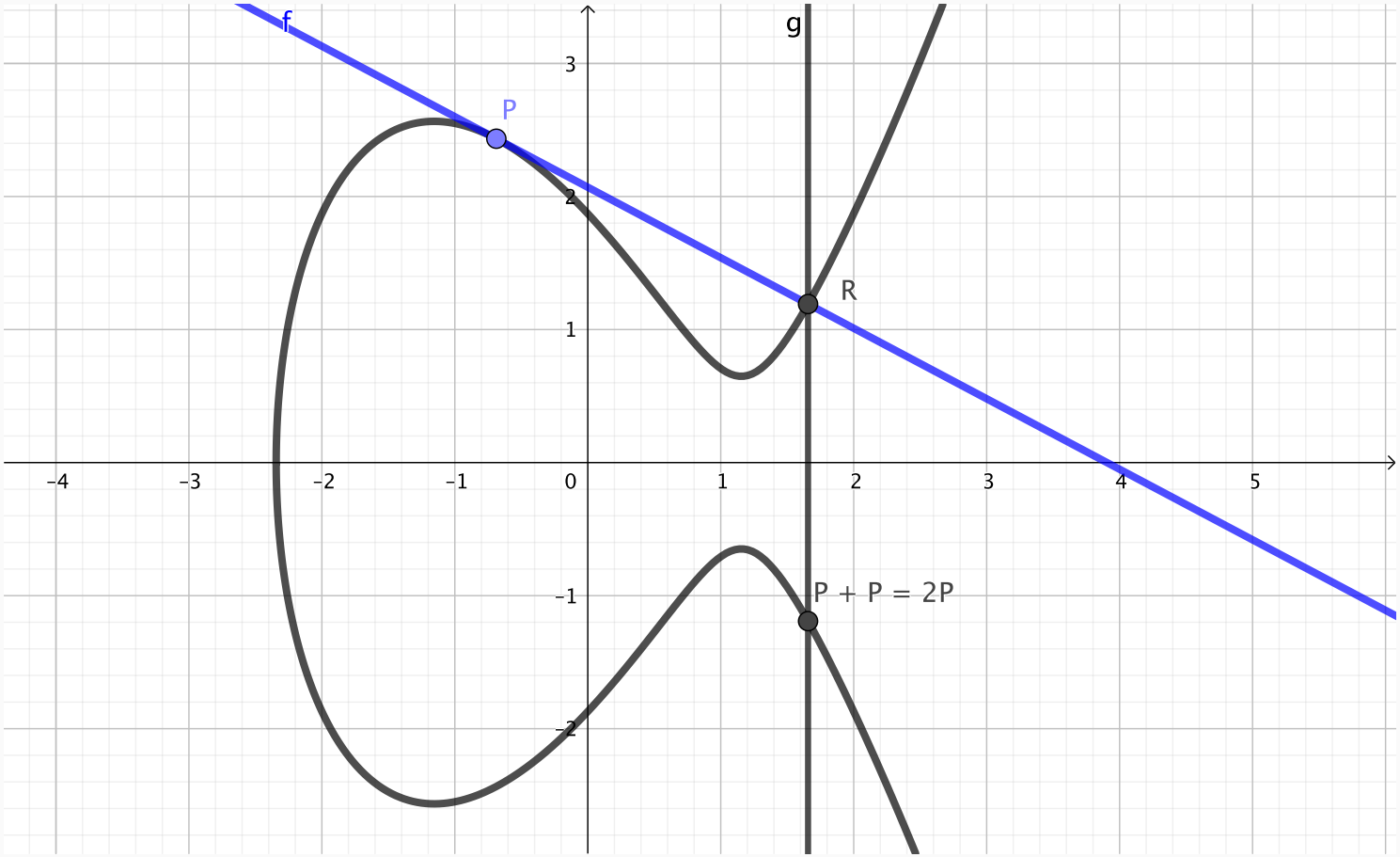
This means we can subtract points! $(p + r) + s = \infty$, and so $s = -(p + r)$.

Sum of points

What about adding $P + P$?

Sum of points

What about adding P + P? Draw the tangent!



Addition formulas (not that important!)

To add $p = (l'_1, L_1)$ and $r = (l'_2, L_2)$,

- If $l'_1 \neq l'_2$, then

$$l'_3 = \acute{C}^2 - l'_1 - l'_2,\ L_3 = \acute{C}(l'_1 - l'_3) - L_1,$$

$$\text{where } \acute{C} = \frac{L_2 - L_1}{l'_2 - l'_1}.$$

- If $l'_1 = l'_2$ and $L_1 \neq L_2$, then $p + r = \infty$.
- If $l'_1 = l'_2$ and $L_1 \neq 0$, then

$$l'_3 = \acute{C}^2 - 2l'_1,\ L_3 = \acute{C}(l'_1 - l'_3) - L_1$$

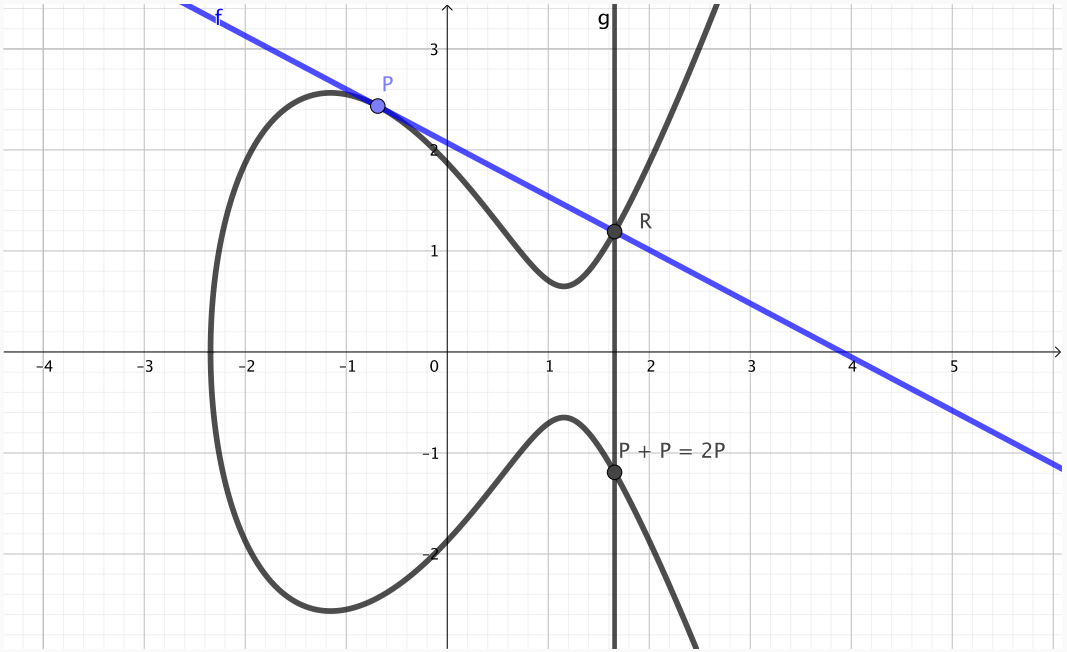
$$\text{where } \acute{C} = \frac{3l'^2_1 +}{2L_1}.$$

- If $l'_1 = l'_2$ and $L_1 = L_2 = 0$, then $p + r = \infty$.
- $p + \infty = p$.

Multiplication of points

If $\acute{c}$ is an integer and p is a point, we may define $\mathsf{n} \times \mathsf{P}$ as adding p to itself $\acute{c}$ times.

(We just saw an example of what $2p$ looks like)



Curves $\acute{C}\check{D}\times\ \check{E}$

Consider a prime number $\check{E}$.

[3] Sometimes called $@?(\check{E})$, the Galois Field of $\check{E}$ elements, and also $\mathrm{Z}=\check{E}\mathrm{Z}$.

Curves $\acute{C}\check{D}\times\ \check{E}$

Consider a prime number $\check{E}$. We can consider our numbers (point coordinates and constants) on $\mathbf{F}_{\check{E}}$, the Finite Field with $\check{E}$ elements.[3] In practice, **we will be working mod p**, or % $\check{E}$.

[3] Sometimes called @?($\check{E}$), the Galois Field of $\check{E}$ elements, and also Z=$\check{E}$Z.

Curves $\acute{C}\check{D}\times\ \check{E}$

Consider a prime number $\check{E}$. We can consider our numbers (point coordinates and constants) on $\mathbf{F}_{\check{E}}$, the Finite Field with $\check{E}$ elements.[3] In practice, **we will be working mod p**, or % $\check{E}$. For instance, if our curve is

$$L^2 = l'^3 + 1242617l' + 21985,$$

then $\acute{C}\check{D}\times$ 7 it becomes

$$L^2 = l'^3 + 5l' + 5,$$

[3] Sometimes called @?($\check{E}$), the Galois Field of $\check{E}$ elements, and also Z=$\check{E}$Z.

Curves $\acute{C}\check{D}\times\ \check{E}$

Consider a prime number $\check{E}$. We can consider our numbers (point coordinates and constants) on $\mathbf{F}_{\check{E}}$, the Finite Field with $\check{E}$ elements.[3] In practice, **we will be working mod p**, or % $\check{E}$. For instance, if our curve is

$$L^2 = l'^3 + 1242617l' + 21985,$$

then $\acute{C}\check{D}\times$ 7 it becomes

$$L^2 = l'^3 + 5l' + 5,$$

and now the **only** points on the curve are

$$\{(1,2),(1,5),(2,3),(2,4),(5,1),(5,6)\}$$

[3] Sometimes called @?($\check{E}$), the Galois Field of $\check{E}$ elements, and also Z=$\check{E}$Z.

Curves mod $\check{E}$

How do you find all points?

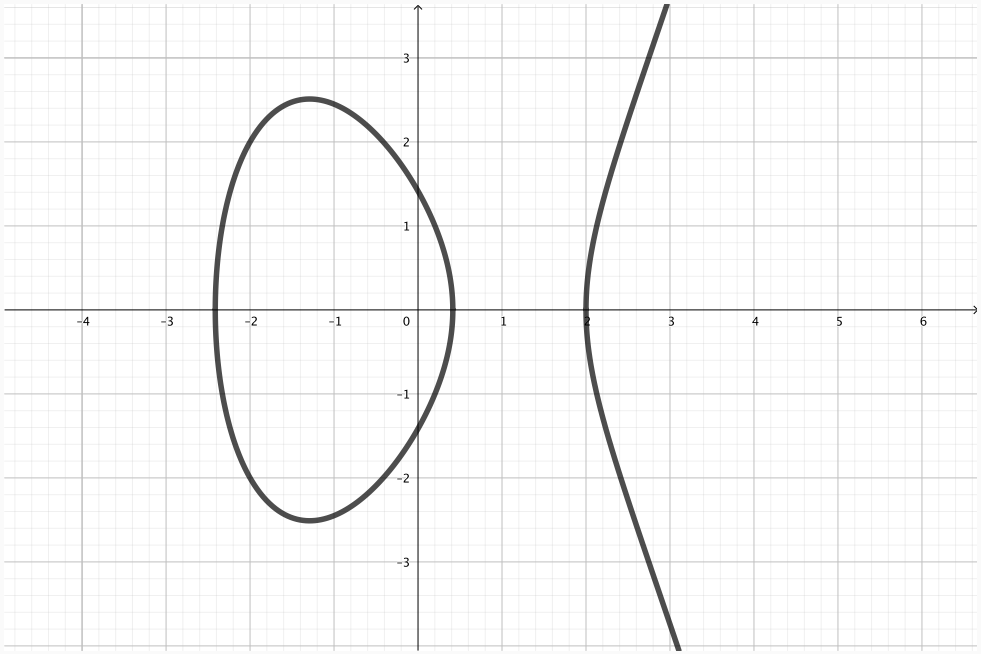
In [1]:
```
print(
    [(x,y)
         for x in range(0,7)
         for y in range(0,7)

     if (y**2 - x**3 - 5*x - 5) % 7 == 0]
)
```

```
[(1, 2), (1, 5), (2, 3), (2, 4), (5, 1), (5, 6)]
```

Curves mod $\check{E}$

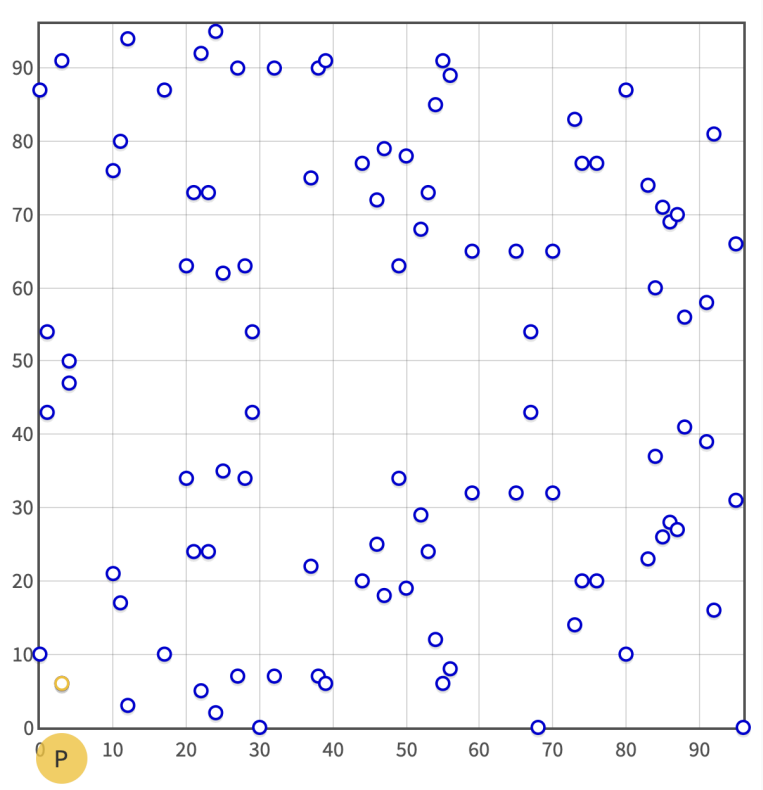
There's a catch!

If the only values are $0, 1, 2, \ldots, \check{E} - 1$, then our curve goes from looking like this...



Curves mod $\check{E}$

...to looking like this:[4]



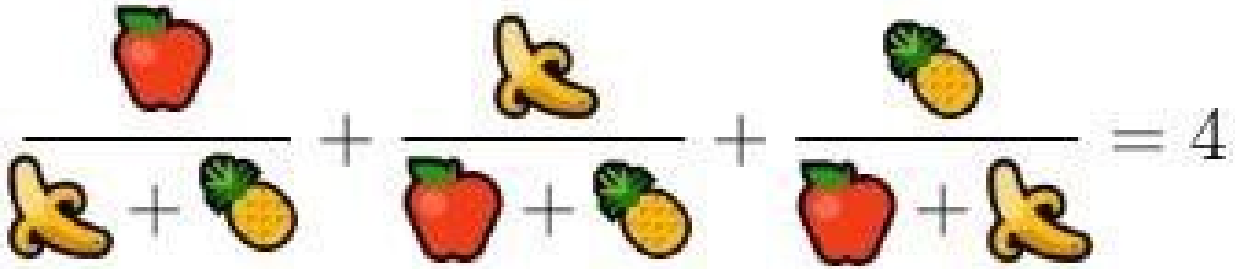
Graph of $L^2 = l'^3 + 2l' + 3 \mod 97$

[4] êħħęĠ-ˣˣÏíħ˝ÿlˈˣ∫@5°čWW

Wow, such big numbers

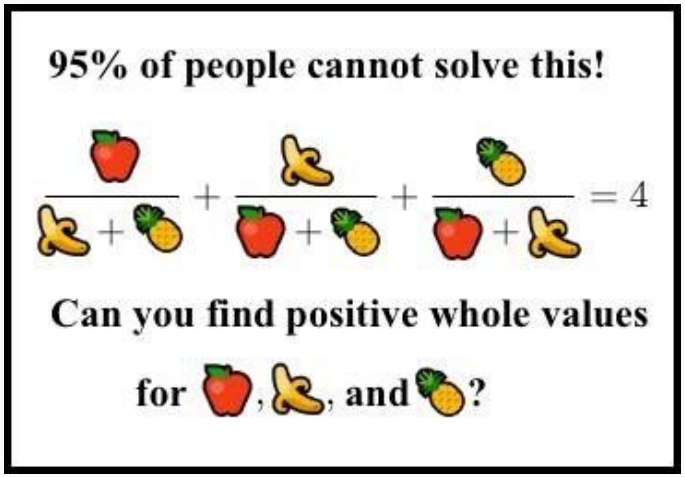
Wow, such big numbers

95% of people cannot solve this!



Can you find positive whole values for , , and ?

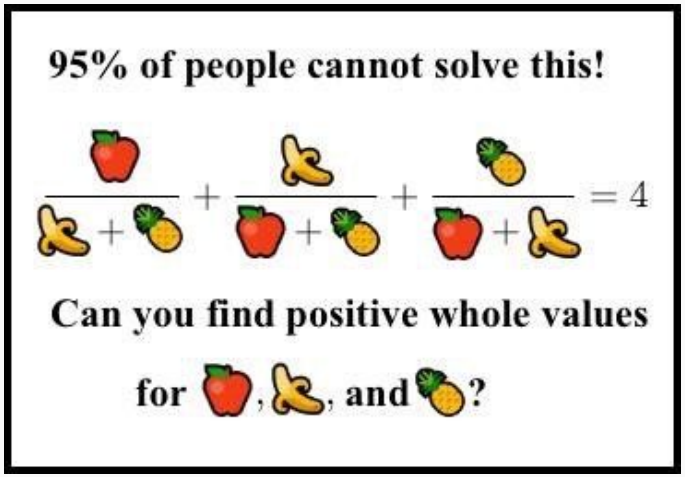
Wow, such big numbers



If you allow for negative values, then you can take:

$$\ddot{A} = 4,\ \eth = -1,\ \tilde{N} = 11$$

Wow, such big numbers



The smallest such values are:[5]

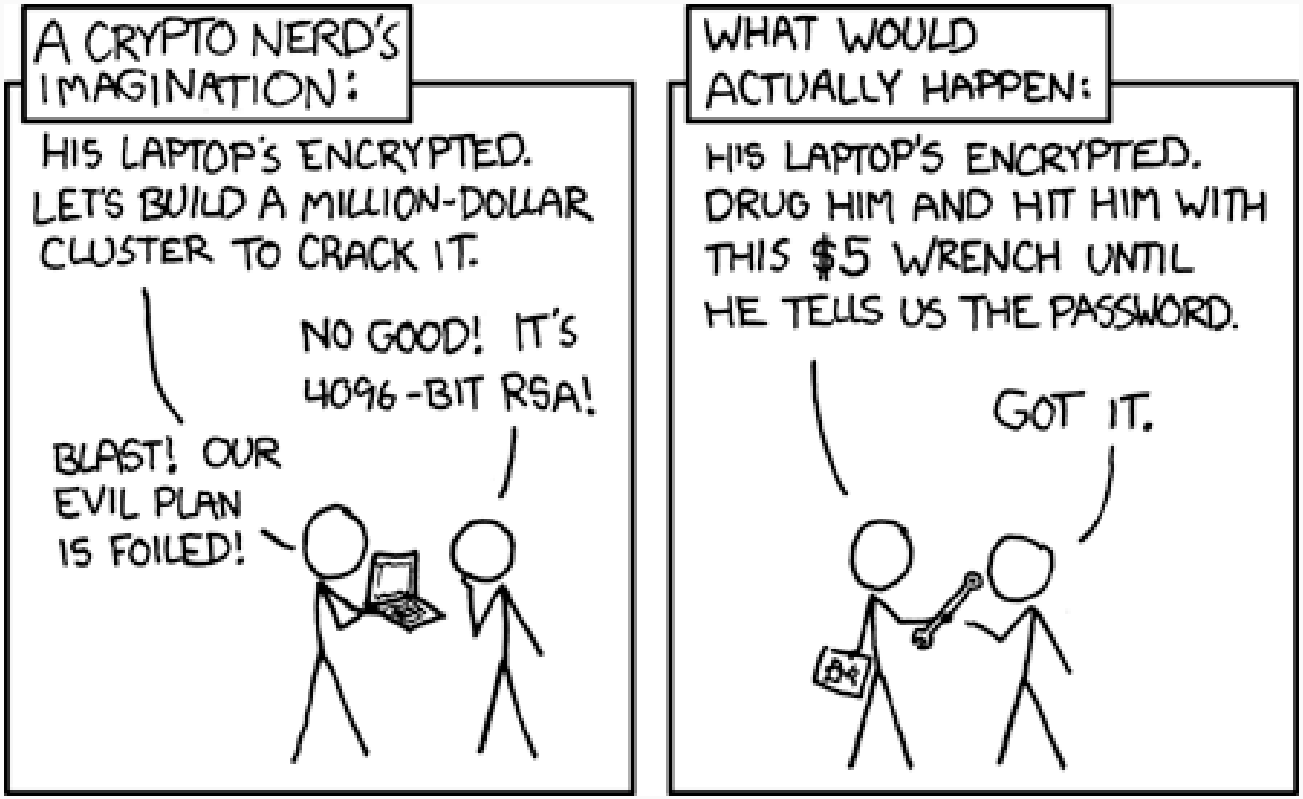
$\ddot{A} = 154476802108746166441951315019919837485664325669565431700026634898253202035277999$

$Đ = 368751317941299998271978115652254748254929799689719709962831374716372246340555 79$

$\tilde{N} = 437361267792869725786125260237139015281653755816161361862143799337842346777 2036$

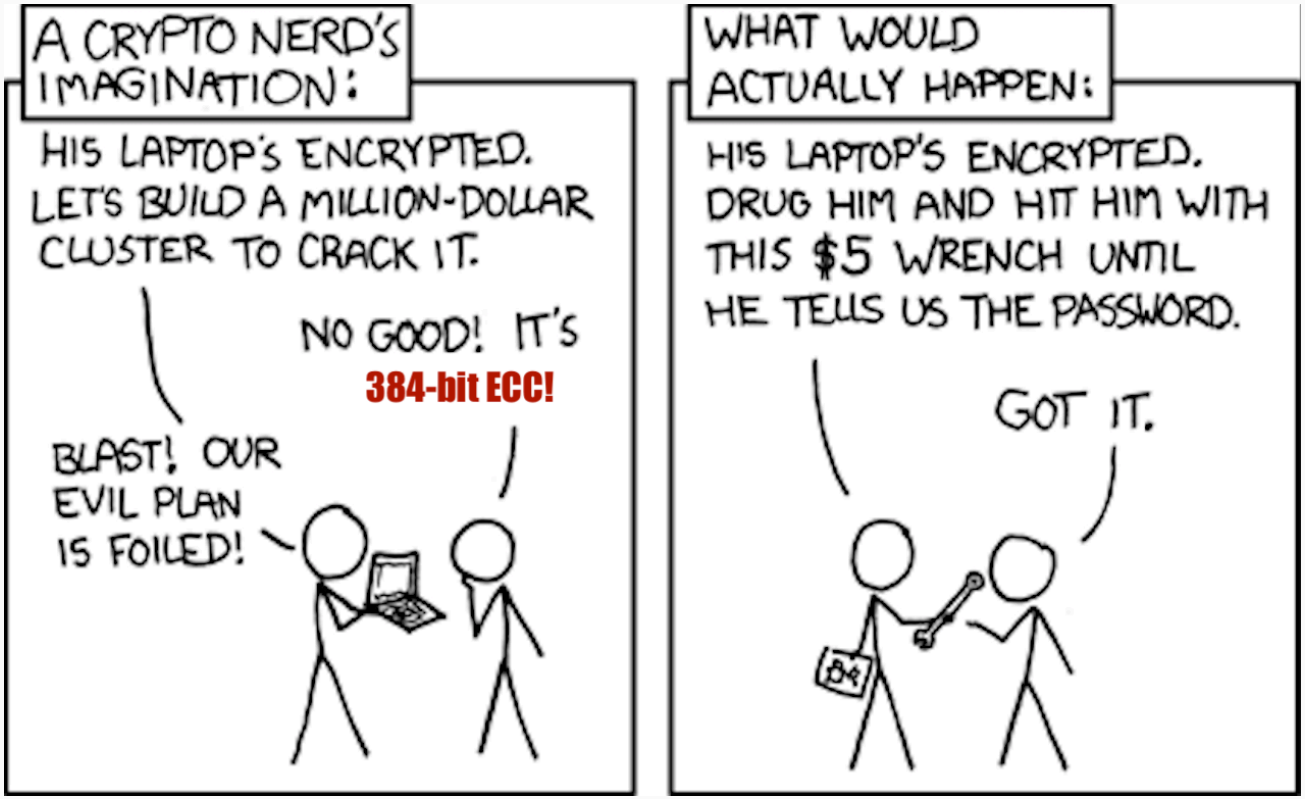
[5] êħħęĠ- x x ěĜ˝ ÃÚ x } ¯ υěw]

Elliptic Curve Cryptography



êħħęĠ₋ˣˣĽüÐÖ˝ Ðčąˣԋ⅁Λˣ

Elliptic Curve Cryptography



êħħęĠ₋ˣˣĽüĐÖ˝ Đčąˣɥ⅁ʌˣ

Elliptic Curve Cryptography Scheme

The typical scheme for ECC consists of:

Elliptic Curve Cryptography Scheme

The typical scheme for ECC consists of:

- The parameters of the curve equation ($L^2 = l'^3 + \mathsf{A}l' + \mathsf{B}$, $l'^2 + L^2 = 1 - \mathsf{d}l'^2L^2$...),
- A prime number $\check{E}$,

Elliptic Curve Cryptography Scheme

The typical scheme for ECC consists of:

- The parameters of the curve equation ($L^2 = l'^3 + \mathsf{A}l' + \mathsf{B}$, $l'^2 + L^2 = 1 - \mathsf{d}l'^2L^2 ...$),
- A prime number $\check{E}$,
- A point $p = (l'_0, L_0)$ on the curve, called a generator,

Elliptic Curve Cryptography Scheme

The typical scheme for ECC consists of:

- The parameters of the curve equation ($L^2 = l'^3 + \mathsf{A}l' + \mathsf{B}$, $l'^2 + L^2 = 1 - \mathsf{d}l'^2L^2$...),
- A prime number $\check{E}$,
- A point $p = (l'_0, L_0)$ on the curve, called a generator,
- A number $\acute{c}$ for which $\acute{c}p = \infty$, and for all $0 < \acute{y} < \acute{c}$, $\acute{y}p \neq \infty$ (the order of p).

Elliptic Curve Cryptography Scheme

The typical scheme for ECC consists of:

- The parameters of the curve equation ($L^2 = l'^3 + \mathsf{A}l' + \mathsf{B}$, $l'^2 + L^2 = 1 - \mathsf{d}l'^2L^2 ...$),
- A prime number $\check{E}$,
- A point $p = (l'_0, L_0)$ on the curve, called a generator,
- A number $\acute{c}$ for which $\acute{c}p = \infty$, and for all $0 < \acute{y} < \acute{c}$, $\acute{y}p \neq \infty$ (the order of p).

We want $\acute{c}$ to be large, and $\gcd(\check{E}, \acute{c}) = 1$.

The first two points are referenced as $+£s®5$, and the scheme as $(+£s®5, \acute{c}, p)$.

Elliptic Curve Diffie Hellman

We now have the curve parameters:

$$\begin{cases} L^2 = l'^3 + \quad l' + * \\ \check{E}, p = (l'_0, L_0), \acute{c} \end{cases}$$

In this scheme, a private key is an integer × between 1 and $\acute{c} - 1$.

The corresponding public key is × p.

Key Exchange // ECDH

ALICE	BOB
$\times\ , \times\ p$	$\times_*, \times_* p$
(Alice gets $\times_* p$)	(Bob gets $\times\ p$)
$\times\ \cdot (\times_* p)$	$\times_* \cdot (\times\ p)$

They both have **the same point $\mathsf{d_A d_B P} = (\mathsf{x}, \mathsf{y})$.**

Take l', or its hash, as the shared symmetric key.

ECDSA

We can also perform **Digital Signature** using a private key and a $\hat{g}\ddot{A}\acute{c}\times\check{D}\acute{C}\ \hat{\imath}\acute{c}\tilde{I}\hat{U}\text{œ}\hat{U}\hat{g}$ (used only once).

ECDSA

We can also perform **Digital Signature** using a private key and a $\hat{g}\ddot{A}\acute{c}\times\check{D}\acute{C}\ \hat{i}\acute{c}\tilde{I}\hat{U}\text{œ}\hat{U}\hat{g}$ (used only once).

Let $\ddot{e}$ be the hashed message, and choose a random integer $\hat{g}$. Then compute

$$\dot{g} = \hat{g}^{-1}(\ddot{e} + \times\ l'),$$

with $l' = l'(\hat{g}p)$. The signature is

$$(\ddot{e}, \dot{g}, \hat{g}p).$$

ECDSA - Verification

The curve is $(+£s®5, ć, p)$ Alice's public key is $r = \times\ p$, and the signature is $(ë, ġ, \hat{g}p)$. To verify it, compute:

$$ǐ_1 = ġ^{-1}ë \mod ć$$

$$ǐ_2 = ġ^{-1}l'(\hat{g}p) \mod ć$$

$$\mathsf{V} := \mathsf{u}_1\mathsf{P} + \mathsf{u}_2\mathsf{Q}.$$

If the message is correct, then the verification holds:

$$® = ǐ_1 p + ǐ_2 r = ġ^{-1}ëp + ġ^{-1}l'\times\ p = ġ^{-1}(ë + l'\times\ )p = \hat{g}p.$$

Discrete Logarithm Problem

Say you encounter a public key r and a curve $(+£s®5, ć, p)$, we want to find $ý$ such that

$$r = ýp$$

$ý$ will be the private key!

Discrete Logarithm Problem

Say you encounter a public key r and a curve $(+£s®5, ć, p)$, we want to find $ý$ such that

$$r = ýp$$

$ý$ will be the private key!

This is a Discrete Logarithm Problem:

$$@îκÛć\ p\ Äć \times ýp \Vdash ŏć \times ý\eth$$

DLP “Attacks”

The are general algorithms to solve a DLP:

- Giant Step-Baby Step (memory intensive)
- Pollard’s Rho and Lambda
- Pohling-Hellman

MOV Attack

Based on pairings, i.e. mapping pairs of points to a finite field $\mathbf{F}_{\check{E}^{\acute{y}}}$ where the discrete logarithm is easier to compute.

Still expensive in most cases.

Anomalous curves

If an elliptic curve has exactly $\check{E}$ points over $\mathbf{F}_{\check{E}}$, we say it is **anomalous**.

We don't use them for cryptography, because they can be attacked in polynomial time.

The $\check{E}$-adic attack

We will attack curves mod $\check{E}$ having exactly $\check{E}$ points ($\check{E}$ a prime, as always).

The $\check{E}$-adic attack

We will attack curves mod $\check{E}$ having exactly $\check{E}$ points ($\check{E}$ a prime, as always).

As always, p is the generator, and r is a public key. We know there is some $\acute{y}$ with

$$r = \acute{y}p$$

The $\check{E}$-adic attack

We will attack curves mod $\check{E}$ having exactly $\check{E}$ points ($\check{E}$ a prime, as always).

As always, p is the generator, and r is a public key. We know there is some $\acute{y}$ with

$$r = \acute{y}p$$

It would be nice to just do $\acute{y} = \frac{r}{p}$ but...

The $\check{E}$-adic attack

We will attack curves $\mod \check{E}$ having exactly $\check{E}$ points ($\check{E}$ a prime, as always).

As always, p is the generator, and r is a public key. We know there is some $\acute{y}$ with

$$r = \acute{y}p$$

It would be nice to just do $\acute{y} = \frac{r}{p}$ but... We can't really divide points!

The $\check{E}$-adic attack (background)

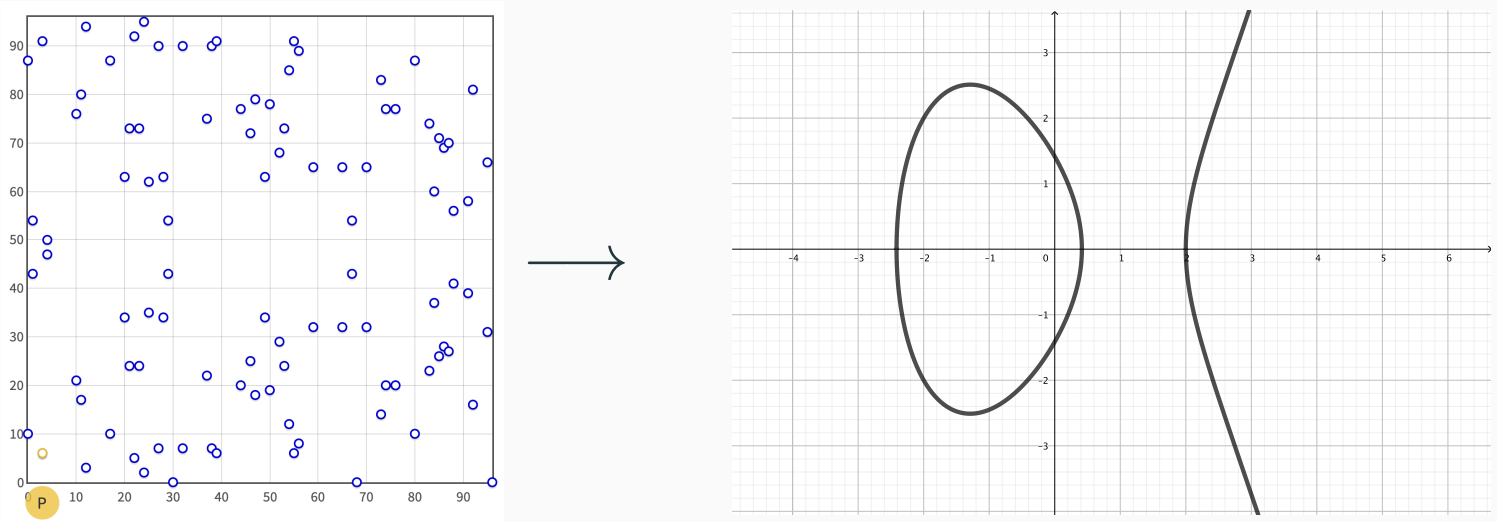
If we have a curve $5: L^2 = l'^3 + \quad l' + *$ in $\mathbf{F}_{\check{E}}$ and two points p and r, we can $\tilde{A}\hat{\imath}\mathring{a}\tilde{I}$ it to a curve $\tilde{5}: L^2 = l'^3 + \tilde{} l' + \tilde{*}$ and two points $\tilde{p}$ and $\tilde{r}$ with

$$\begin{cases} \equiv \tilde{}, * \equiv \tilde{} & \mod \check{E} \\ p \equiv \tilde{p}, \ r \equiv \tilde{r} & \mod \check{E} \end{cases}.$$

The $\check{E}$-adic attack (background)

If we have a curve $5: L^2 = l'^3 + \quad l' + *$ in $\mathbf{F}_{\check{E}}$ and two points p and r, we can $\tilde{A}\hat{i}\mathring{a}\tilde{I}$ it to a curve $\tilde{5}: L^2 = l'^3 + \tilde{} l' + \tilde{*}$ and two points $\tilde{p}$ and $\tilde{r}$ with

$$\begin{cases} \equiv \tilde{}, * \equiv \tilde{} & \mod \check{E} \\ p \equiv \tilde{p}, \ r \equiv \tilde{r} & \mod \check{E} \end{cases}.$$



The $\check{E}$-adic attack (background)

If we have a curve 5 in rationals, we can consider the reduction map modulo $\check{E}$, which takes each coordinate mod $\check{E}$.

The $\check{E}$-adic attack (background)

If we have a curve 5 in rationals, we can consider the reduction map modulo $\check{E}$, which takes each coordinate mod $\check{E}$.

$$\hat{g}\hat{U}\times_{\check{E}} : 5(\mathrm{Q}) \to 5(\mathrm{F}_{\check{E}})$$

$$\left(\frac{\ddot{A}}{\text{Đ}}, \frac{\tilde{N}}{\times}\right) \mapsto (\ddot{A}\text{Đ}^{-1}, \tilde{N}\times^{-1}) \mod \check{E}$$

$$\infty \mapsto \infty$$

The $\check{E}$-adic attack (background)

If we have a curve 5 in rationals, we can consider the reduction map modulo $\check{E}$, which takes each coordinate mod $\check{E}$.

$$\hat{g}\hat{U}\times_{\check{E}} : 5(\mathrm{Q}) \to 5(\mathrm{F}_{\check{E}})$$
$$\left(\frac{\ddot{A}}{\text{Đ}}, \frac{\tilde{N}}{\times}\right) \mapsto (\ddot{A}\text{Đ}^{-1}, \tilde{N}\times^{-1}) \mod \check{E}$$
$$\infty \mapsto \infty$$

If $\check{E}$ divides Đ or $\times$, then the point goes to ∞.

The $\check{E}$-adic attack (background)

If we have a curve 5 in rationals, we can consider the reduction map modulo $\check{E}$, which takes each coordinate mod $\check{E}$.

$$\hat{g}\hat{U}\times_{\check{E}} : 5(\mathrm{Q}) \to 5(\mathrm{F}_{\check{E}})$$
$$\left(\frac{\ddot{A}}{\text{Đ}}, \frac{\tilde{N}}{\times}\right) \mapsto (\ddot{A}\text{Đ}^{-1}, \tilde{N}\times^{-1}) \mod \check{E}$$
$$\infty \mapsto \infty$$

If $\check{E}$ divides Đ or $\times$, then the point goes to ∞.

The map $\hat{g}\hat{U}\times_{\check{E}}$ is linear (as in linear algebra), meaning

$$\hat{g}\hat{U}\times_{\check{E}}(\acute{c}p) = \acute{c} \times \hat{g}\hat{U}\times_{\check{E}}(p)$$
$$\hat{g}\hat{U}\times_{\check{E}}(p + r) = \hat{g}\hat{U}\times_{\check{E}}(p) + \hat{g}\hat{U}\times_{\check{E}}(r).$$

The $\check{E}$-adic attack (background)

If a curve 5 has $\acute{c}$ points in $\mathrm{F}_{\check{E}}$, then all points satisfy:

$$\acute{c}p = \infty.$$

The $\check{E}$-adic attack (background)

Given a curve $5(\mathrm{Q})$, take the set of points with denominator divisible by $\check{E}$:[6]

$$5_{\hat{g}} = \left\{ \left(\frac{\ddot{A}}{\text{Đ}}, \frac{\tilde{N}}{\times} \right) \in 5(\mathrm{Q}) \mid \check{E}^{2\hat{g}} | \text{Đ},\ \check{E}^{3\hat{g}} | \times \right\}.$$

[6] This is the $\check{E}$-adic bit of the talk!

The $\check{E}$-adic attack (background)

Given a curve $5(\mathrm{Q})$, take the set of points with denominator divisible by $\check{E}$:[6]

$$5_{\hat{g}} = \left\{ \left(\frac{\ddot{A}}{\text{Đ}}, \frac{\tilde{N}}{\times} \right) \in 5(\mathrm{Q}) \mid \check{E}^{2\hat{g}} | \text{Đ},\ \check{E}^{3\hat{g}} | \times \right\}.$$

If p is in 5_1, then $\check{E}$ divides the denominators of the point, and so $\hat{g}\hat{U}^{\times}{}_{\check{E}}(p) = \infty$ (and viceversa).

[6] This is the $\check{E}$-adic bit of the talk!

The $\check{E}$-adic attack (background)

Given a curve $5(\mathrm{Q})$, take the set of points with denominator divisible by $\check{E}$:[6]

$$5_{\hat{g}} = \left\{ \left(\frac{\ddot{A}}{\dot{D}}, \frac{\tilde{N}}{\times} \right) \in 5(\mathrm{Q}) \mid \check{E}^{2\hat{g}} | \dot{D},\ \check{E}^{3\hat{g}} | \times \right\}.$$

If p is in 5_1, then $\check{E}$ divides the denominators of the point, and so $\hat{g}\hat{U}^{\times}{}_{\check{E}}(p) = \infty$ (and viceversa).

We can consider the **p-adic logarithm**

$$\lambda_1 \colon 5_1 \to \mathrm{Z}/\check{E}^4\mathrm{Z}$$

$$(l', L) \mapsto \frac{1}{\check{E}} \frac{l'}{L} \mod \check{E}^4$$

[6] This is the $\check{E}$-adic bit of the talk!

The $\check{E}$-adic attack

- Begin with a curve $5(\mathrm{F}_{\check{E}})$ with exactly $\check{E}$ points, p the generator and r a public key.

The $\check{E}$-adic attack

- Begin with a curve $5(\mathrm{F}_{\check{E}})$ with exactly $\check{E}$ points, p the generator and r a public key.
- Lift 5, p and r to $\tilde{5}(\mathrm{Q})$, $\tilde{p}$ and $\tilde{r}$ in rational numbers.

The $\check{E}$-adic attack

- Begin with a curve $5(\mathrm{F}_{\check{E}})$ with exactly $\check{E}$ points, p the generator and r a public key.
- Lift 5, p and r to $\tilde{5}(\mathrm{Q})$, $\tilde{p}$ and $\tilde{r}$ in rational numbers.
- Let $\tilde{p}_1 = \check{E} \cdot \tilde{p}$, $\tilde{r}_1 = \check{E} \cdot \tilde{r}$. Then $\tilde{p}_1 \in \tilde{5}_1$, since $\hat{g}\hat{U}\times_{\check{E}}(\tilde{p}_1) = \hat{g}\hat{U}\times_{\check{E}}(\check{E} \cdot \tilde{p}) = \check{E} \cdot \hat{g}\hat{U}\times_{\check{E}}(\tilde{p}) = \infty$. Same with $\tilde{r}_1$.

The $\check{E}$-adic attack

- Begin with a curve $5(\mathrm{F}_{\check{E}})$ with exactly $\check{E}$ points, p the generator and r a public key.
- Lift 5, p and r to $\tilde{5}(\mathrm{Q})$, $\tilde{p}$ and $\tilde{r}$ in rational numbers.
- Let $\tilde{p}_1 = \check{E} \cdot \tilde{p}$, $\tilde{r}_1 = \check{E} \cdot \tilde{r}$. Then $\tilde{p}_1 \in \tilde{5}_1$, since $\hat{g}\hat{U}\times_{\check{E}}(\tilde{p}_1) = \hat{g}\hat{U}\times_{\check{E}}(\check{E} \cdot \tilde{p}) = \check{E} \cdot \hat{g}\hat{U}\times_{\check{E}}(\tilde{p}) = \infty$. Same with $\tilde{r}_1$.
- If $\tilde{p}_1 \notin \tilde{5}_2$, then

$$\acute{y} \equiv \frac{\lambda_1(\tilde{r}_1)}{\lambda_1(\tilde{p}_1)} \mod \check{E}$$

The $\check{E}$-adic attack (Proof)

We can easily check that $\acute{y}$ is the **private key**, i.e. $\acute{y}p = r$:

$$\acute{y}\lambda_1(\tilde{p}_1) - \lambda_1(\tilde{r}_1) = \lambda_1(\acute{y}\tilde{p}_1 - \tilde{r}_1) = \lambda_1(\acute{y}\check{E}\tilde{p} - \check{E}\tilde{r}) = \check{E}\lambda_1(\acute{y}\tilde{p} - \tilde{r}) \equiv 0$$

and we can do this because

$$\infty = \acute{y}p - r = \hat{g}\hat{U}\times_{\check{E}}(\acute{y}\tilde{p} - \tilde{r}) \implies \acute{y}\tilde{p} - \tilde{r} \in \tilde{5}_1.$$

The $\check{E}$-adic attack (Proof)

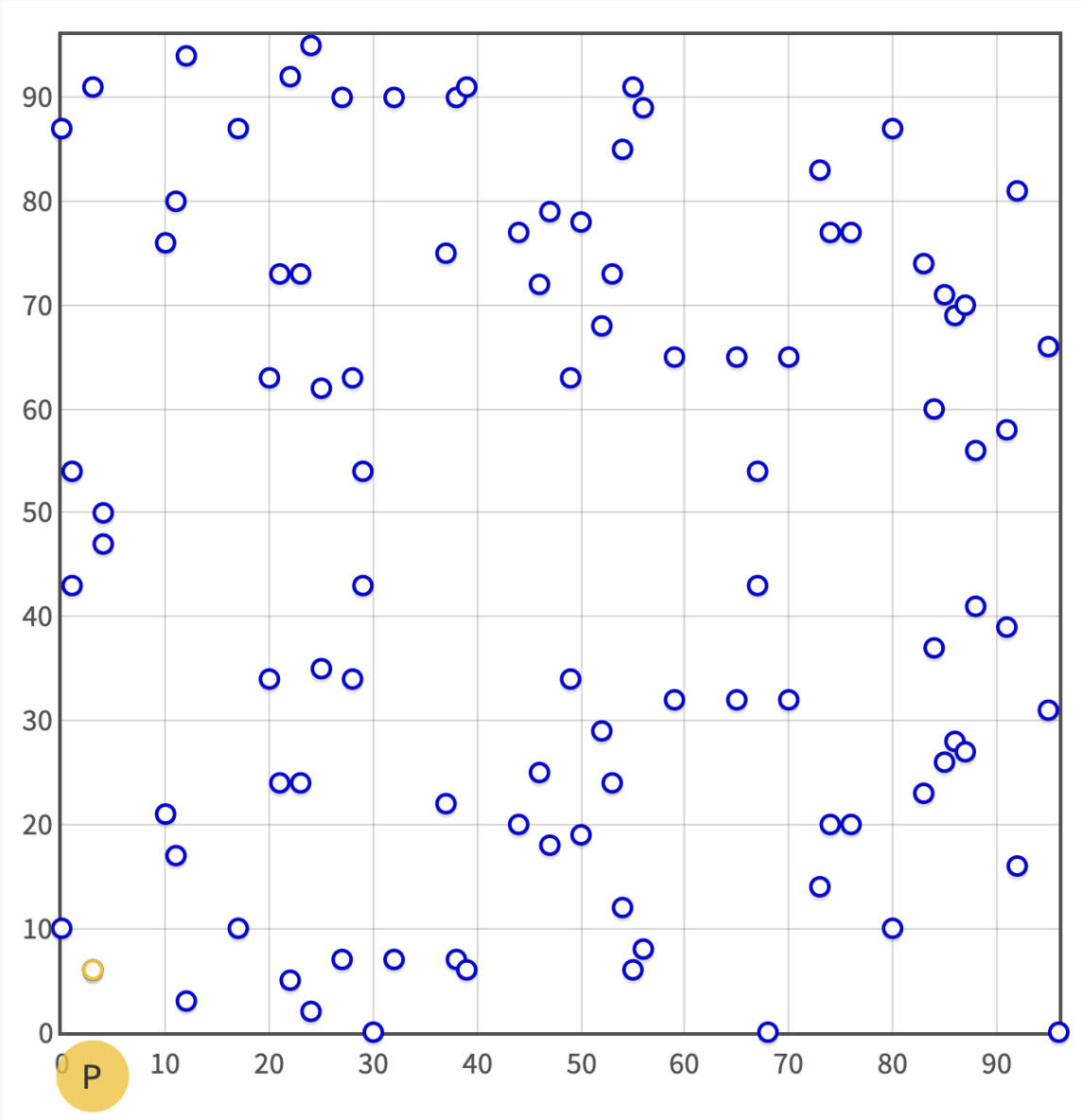
We can easily check that $\acute{y}$ is the **private key**, i.e. $\acute{y}p = r$:

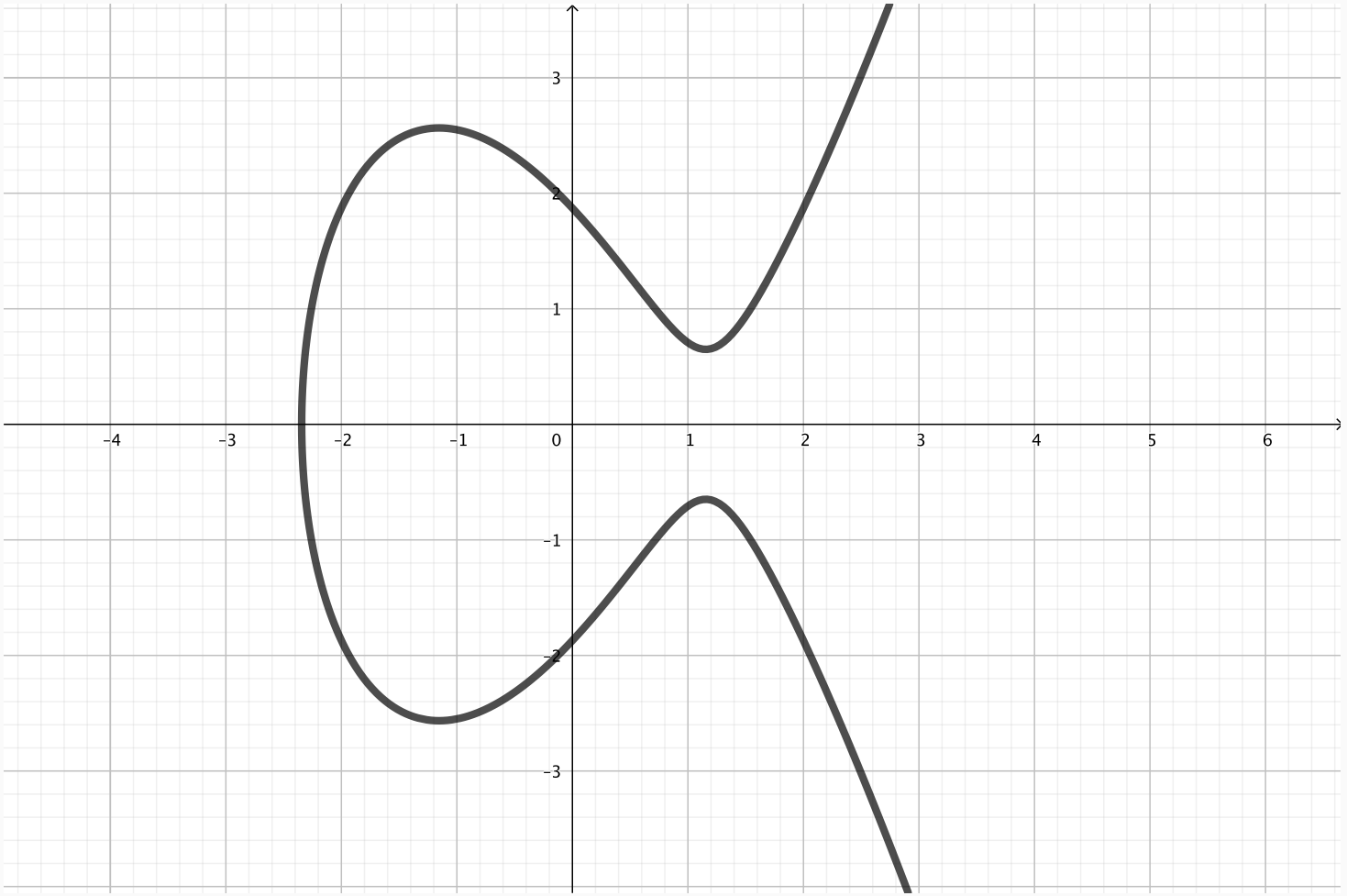
$$\acute{y}\lambda_1(\tilde{p}_1) - \lambda_1(\tilde{r}_1) = \lambda_1(\acute{y}\tilde{p}_1 - \tilde{r}_1) = \lambda_1(\acute{y}\check{E}\tilde{p} - \check{E}\tilde{r}) = \check{E}\lambda_1(\acute{y}\tilde{p} - \tilde{r}) \equiv 0$$

and we can do this because

$$\infty = \acute{y}p - r = \hat{g}\hat{U}^{\times}{}_{\check{E}}(\acute{y}\tilde{p} - \tilde{r}) \implies \acute{y}\tilde{p} - \tilde{r} \in \tilde{5}_1.$$

The numbers involved in the computation of $\acute{y}$ are way too big, but we can work modulo $\check{E}^2$ (see references).


90
80
70
60
50
40
30
20
10
0
0
10
20
30
40
50
60
70
80
90
P


3
2
1
-1
-2
-3
-4
-3
-2
-1
0
1
2
3
4
5
6

Some references

- êħħęĠ-ˣˣκκκ˝ĐĜľęħčɭʃɭ˝íč
- Introduction to ECC êħħęĠ-ˣˣÏíħ˝ÿľˣʃ@®ɭмęs
- Video introduction to ECC at CCC
  êħħęĠ-ˣˣÏíħ˝ÿľˣʃĆ5ą +H
- Smart's attack on anomalous curves
  êħħęĠ-ˣˣκκκ˝êęÿ˝êę˝Đčąˣħ̀ÚĐêĜÚęčĜħĠˣмυˣ
  EpẂ мύ ɭʃʌ˝ęÖä
- êħħęĠ-ˣˣĠÃäÚĐĬĜķÚĠ˝ĐĜ˝ľę˝ħč
- Elliptic Curves: Number theory and cryptography (L. Washington).

To sum up

- Don’t fear elliptic curves! Advanced stuff can look difficult, but the basic theory is attainable.
- They are more lightweight than other public key systems.
- Theoretical attacks can appear based on really strange properties.
- **If you need to implement some ECC, go read:**

  êħħęĠ-ˣˣĠÃäÚÐĬĜķÚĠ˝ĐĜ˝ ľę˝ ħč

  and its references.