Elliptic Curve Primality Proving

Jared Asuncion

PhD Away Days Bordeaux-Luxembourg
19 October 2019

Definition

An elliptic curve over k ($\operatorname{char} k \neq 2, 3$) is a smooth projective curve given by an equation of the form $y^2 = f(x) = x^3 + ax + b$ where $a, b \in k$ and $f(x)$ has no double roots in $\overline{k}$.

Example

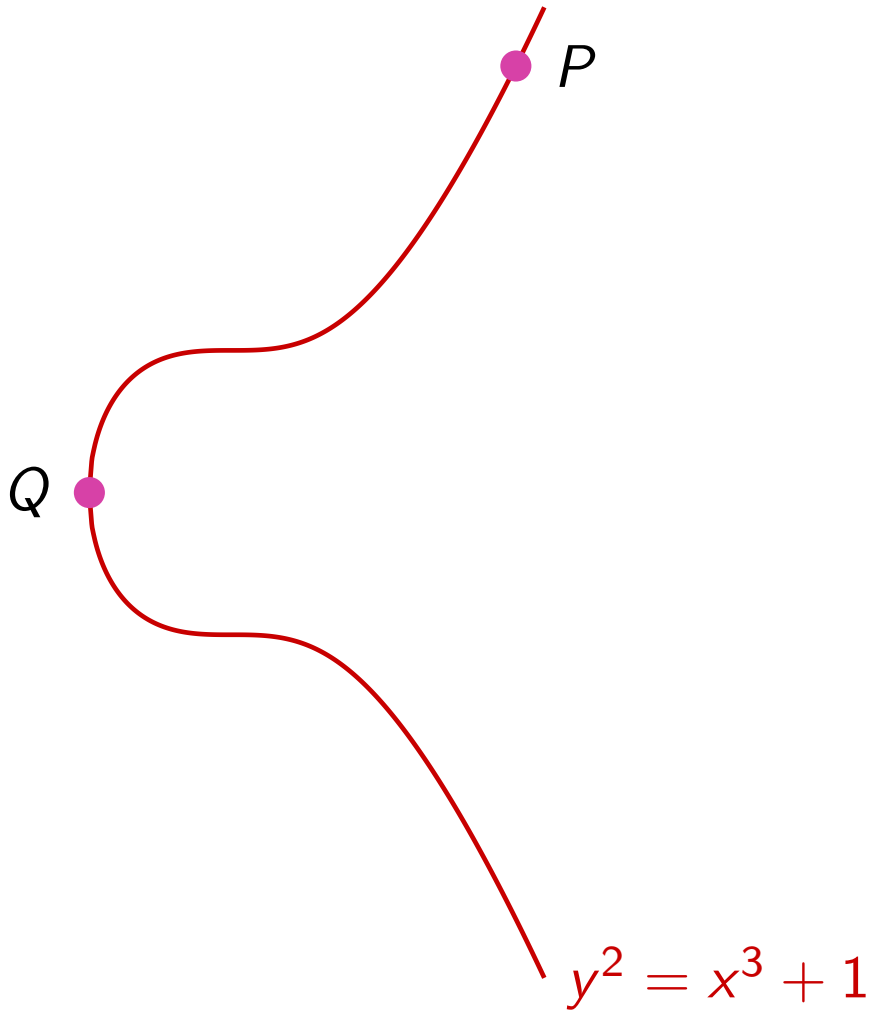
Take $k = \mathbb{R}$. Then $y^2 = x^3 + x + 1$ is an elliptic curve over $\mathbb{R}$ since $\overline{\mathbb{R}} = \mathbb{C}$ and $x^3 + x + 1$ has distinct roots over $\mathbb{C}$.

Example

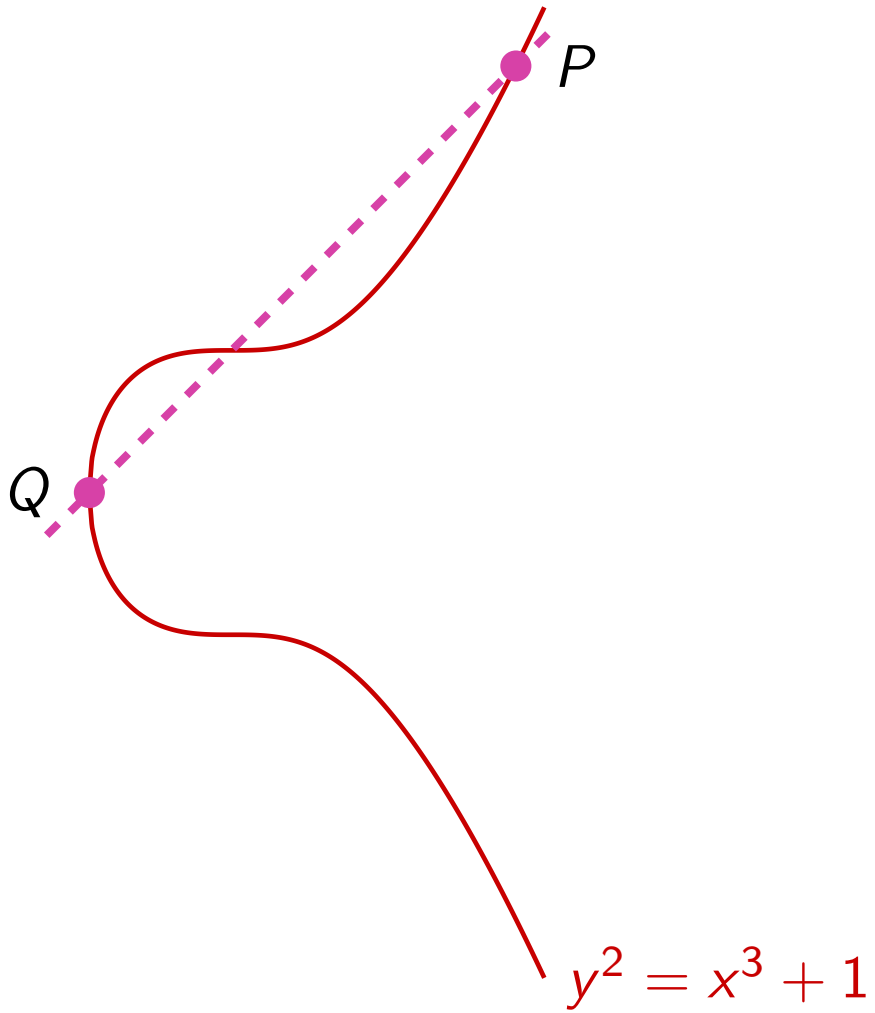
Take $k = \mathbb{F}_{31}$. Then $y^2 = x^3 + x + 1$ is NOT an elliptic curve since

$$\begin{aligned}(x - 14)^2(x - 3) &= x^3 - 31x^2 + 280x - 588 \\ &\equiv x^3 + x + 1 \bmod 31.\end{aligned}$$

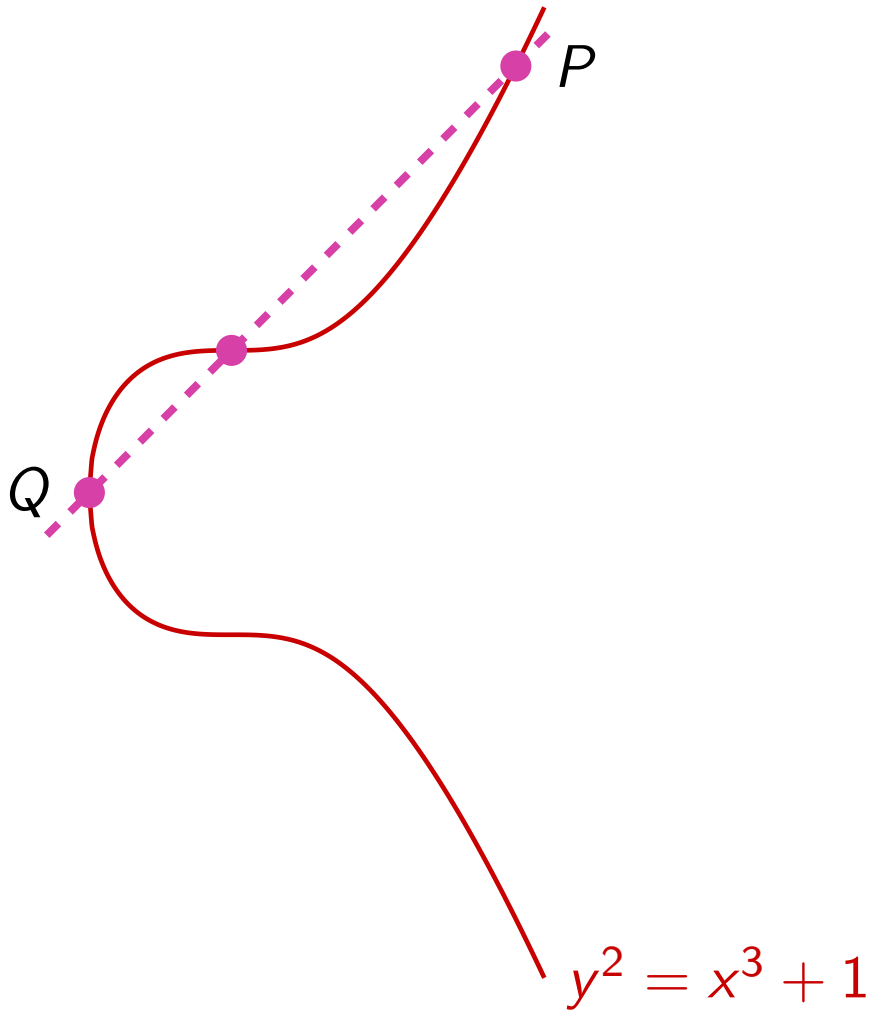
An elliptic curve has a group structure. The group structure is obtained using the 'connect-intersect-reflect' method. The identity of this group is called the point at infinity, denoted by ∞.



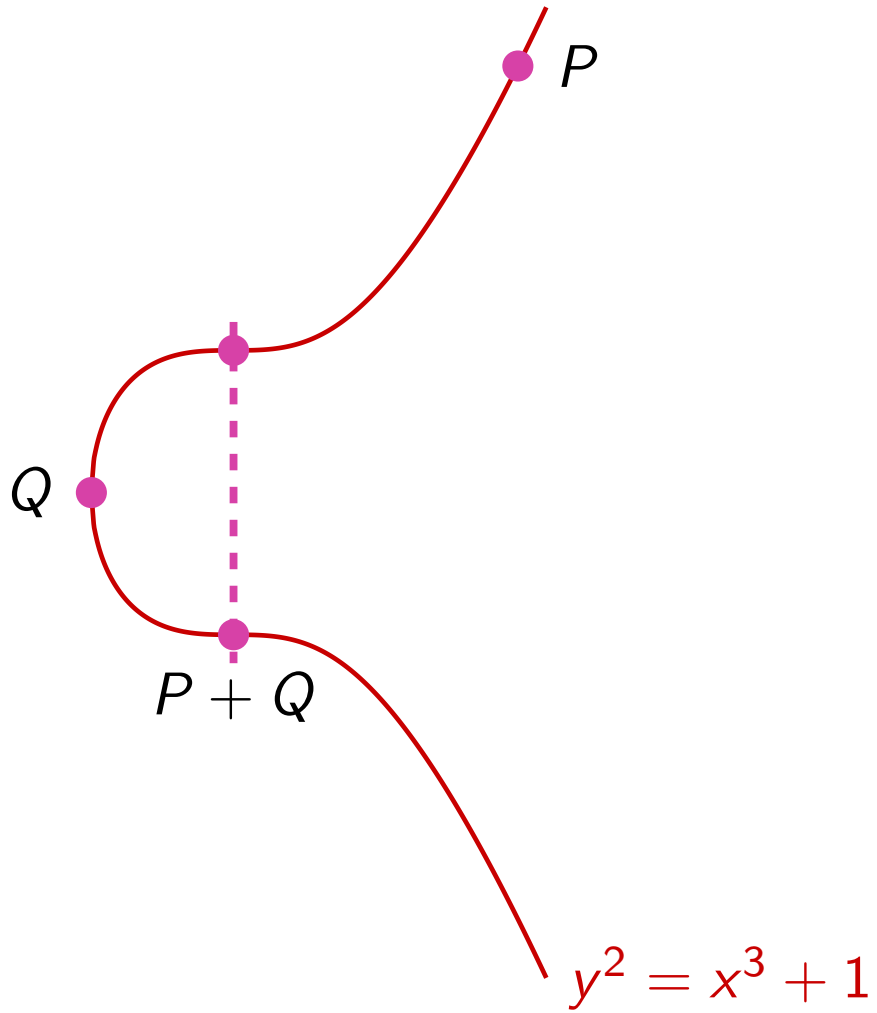
An elliptic curve has a group structure. The group structure is obtained using the 'connect-intersect-reflect' method. The identity of this group is called the point at infinity, denoted by ∞.



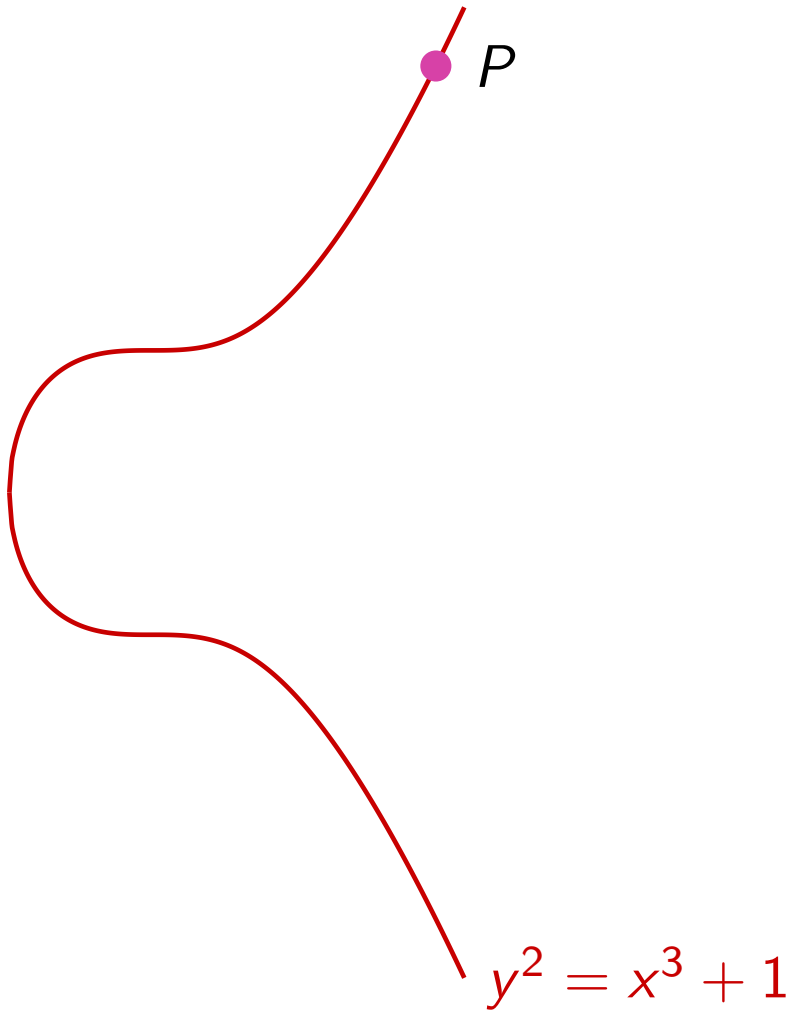
An elliptic curve has a group structure. The group structure is obtained using the 'connect-intersect-reflect' method. The identity of this group is called the point at infinity, denoted by ∞.



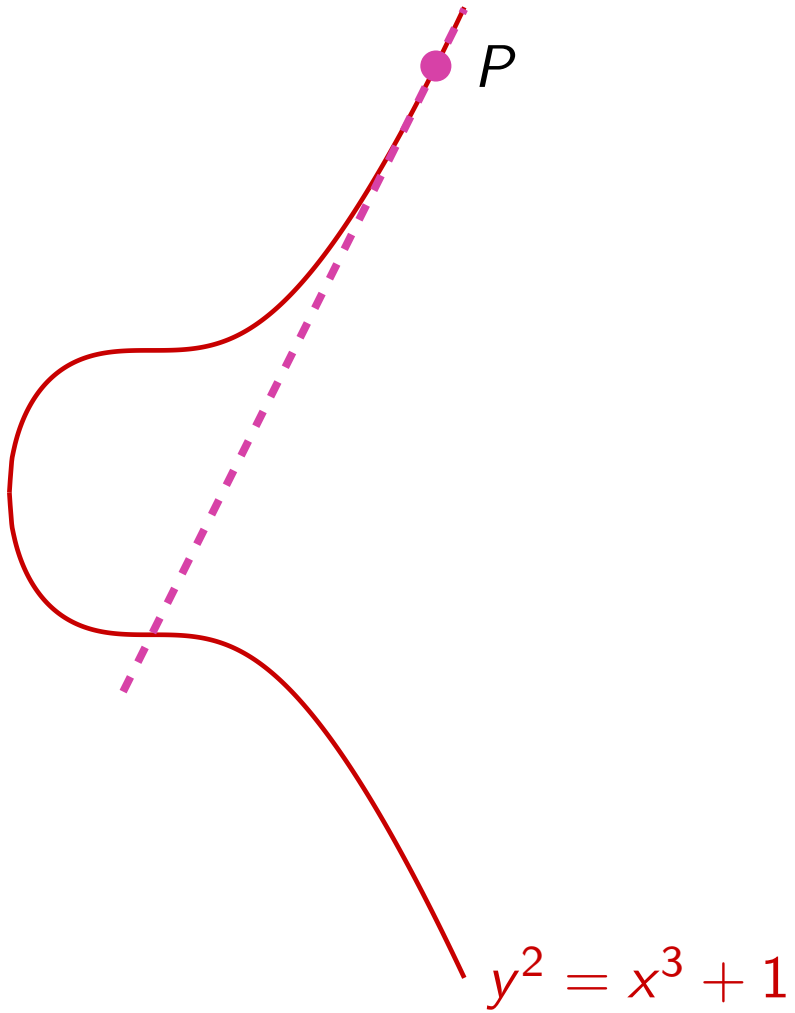
An elliptic curve has a group structure. The group structure is obtained using the 'connect-intersect-reflect' method. The identity of this group is called the point at infinity, denoted by ∞.



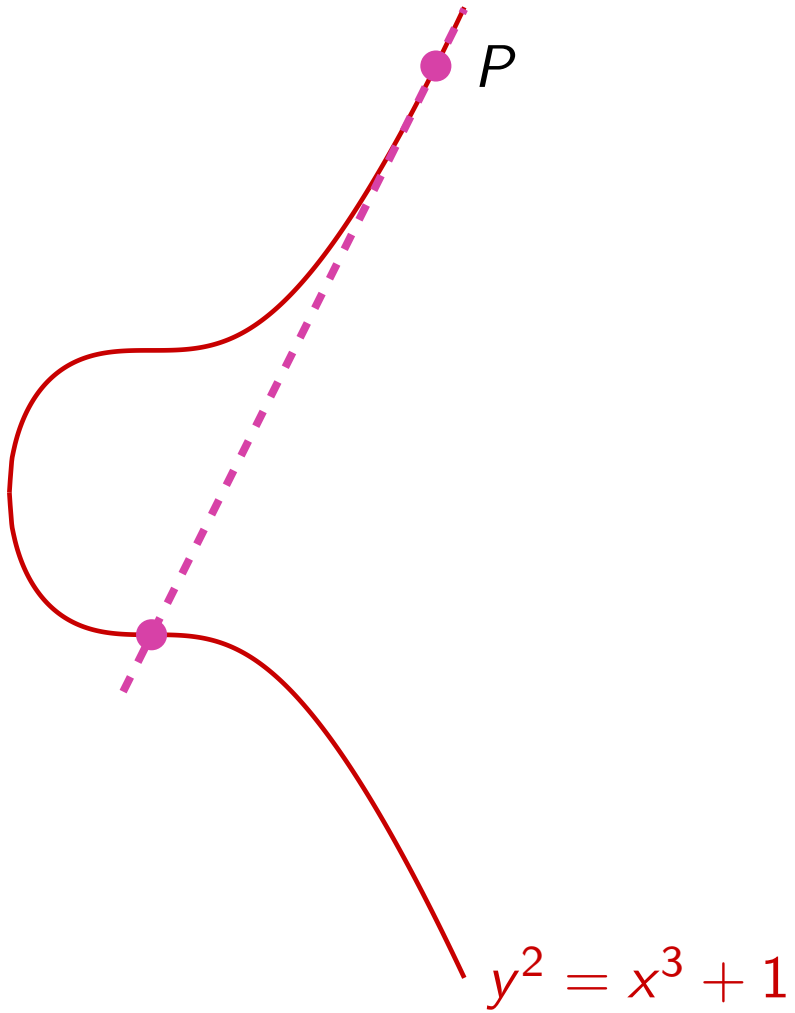
An elliptic curve has a group structure. The group structure is obtained using the 'connect-intersect-reflect' method. The identity of this group is called the point at infinity, denoted by ∞.



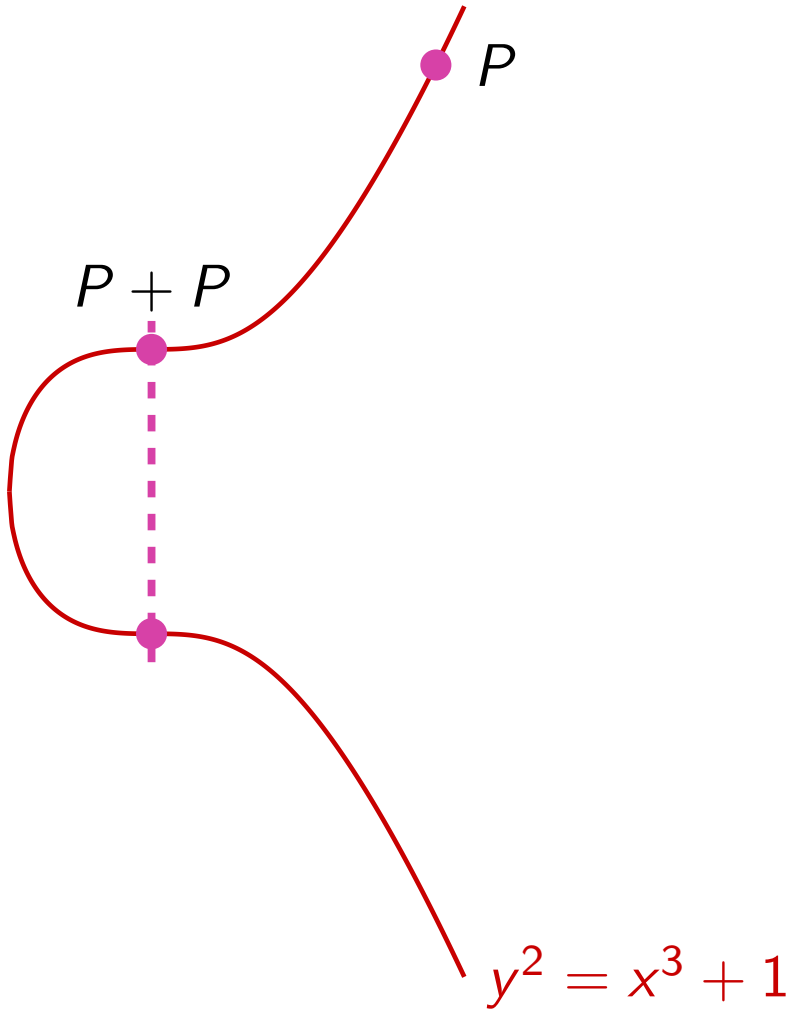
An elliptic curve has a group structure. The group structure is obtained using the 'connect-intersect-reflect' method. The identity of this group is called the point at infinity, denoted by ∞.



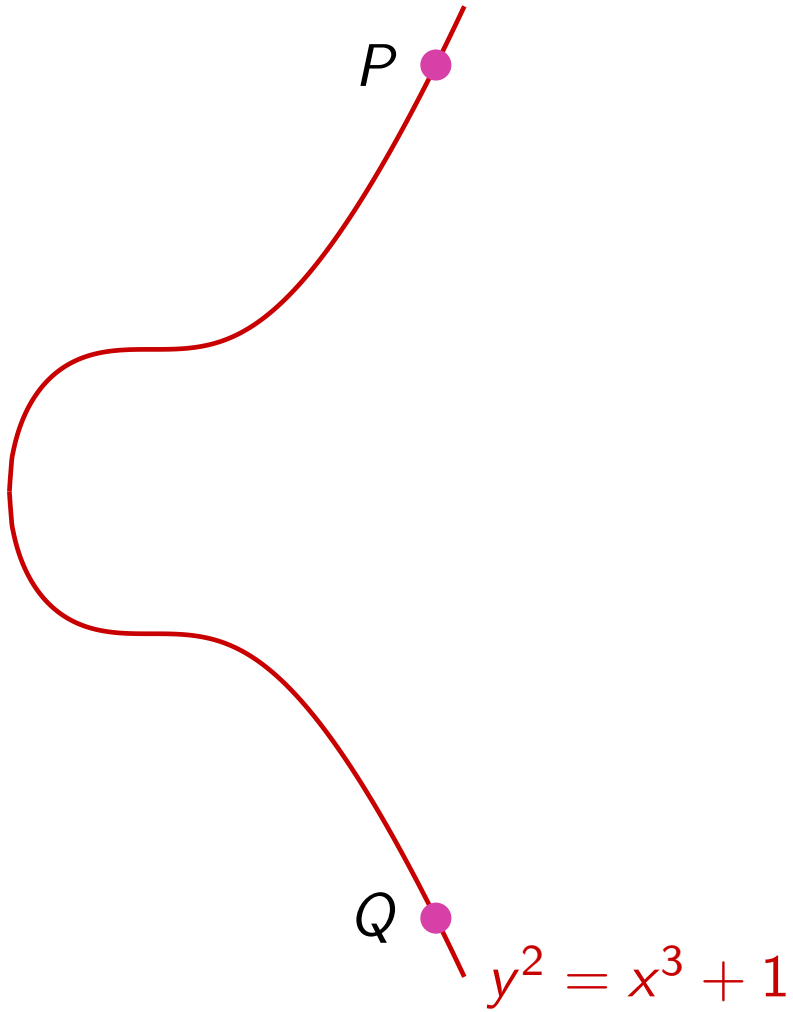
An elliptic curve has a group structure. The group structure is obtained using the 'connect-intersect-reflect' method. The identity of this group is called the point at infinity, denoted by ∞.



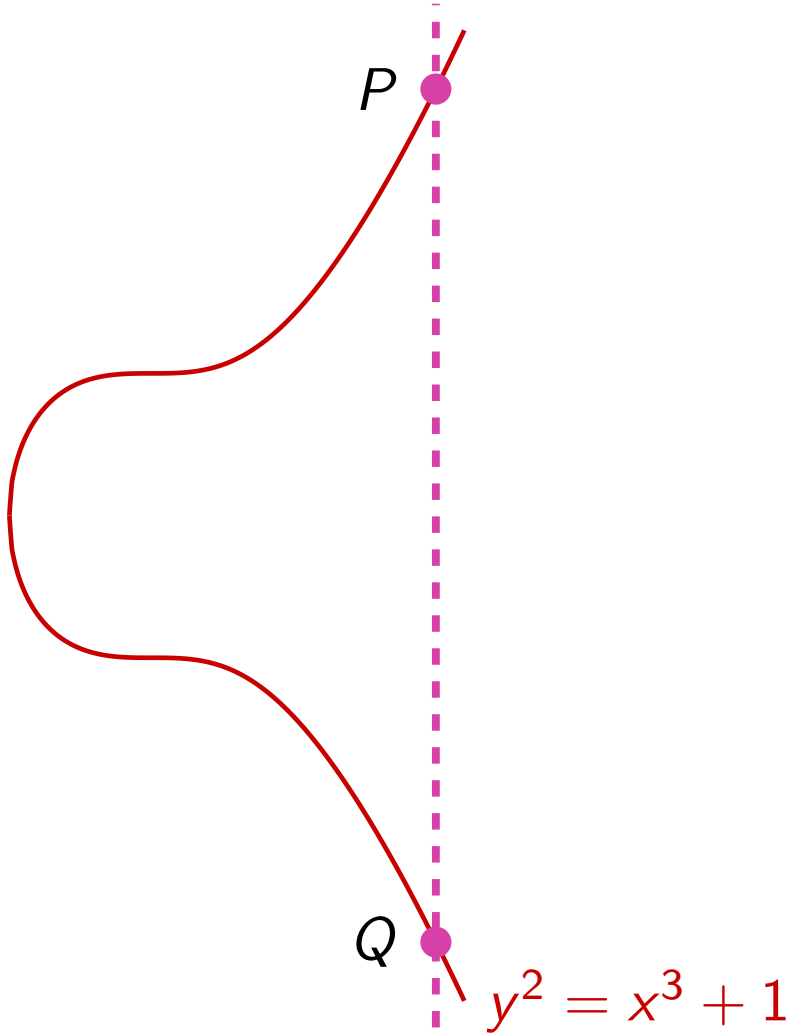
An elliptic curve has a group structure. The group structure is obtained using the 'connect-intersect-reflect' method. The identity of this group is called the point at infinity, denoted by ∞.



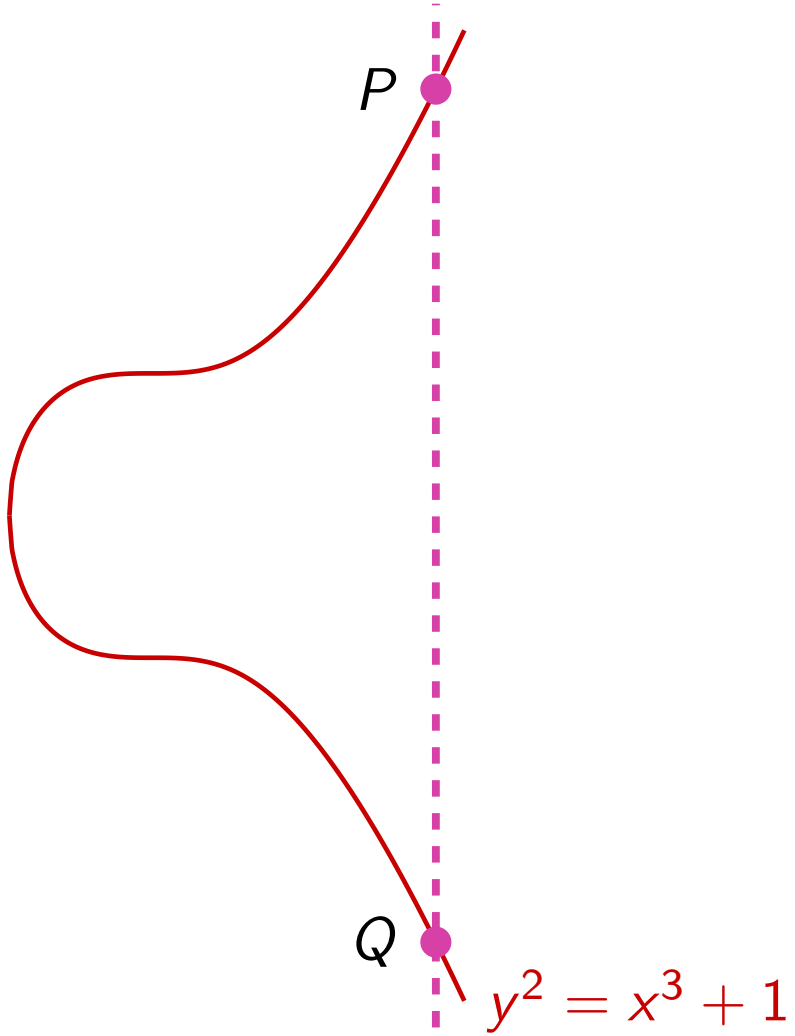
An elliptic curve has a group structure. The group structure is obtained using the 'connect-intersect-reflect' method. The identity of this group is called the point at infinity, denoted by ∞.



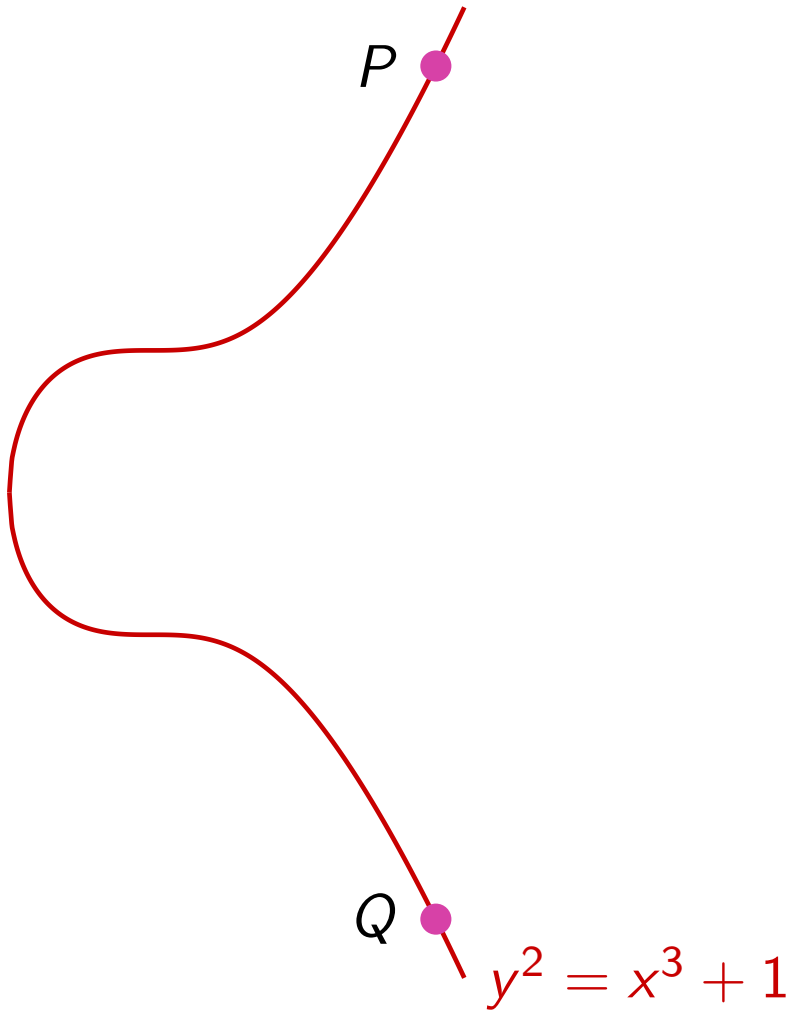
An elliptic curve has a group structure. The group structure is obtained using the 'connect-intersect-reflect' method. The identity of this group is called the point at infinity, denoted by ∞.



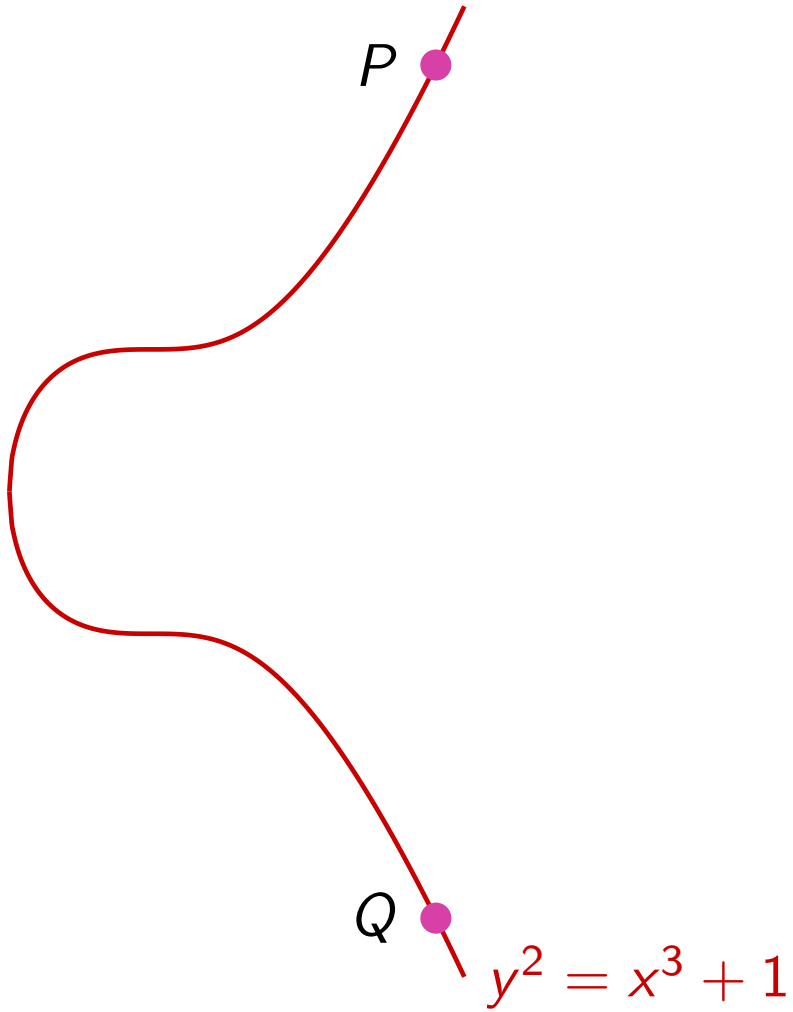
An elliptic curve has a group structure. The group structure is obtained using the 'connect-intersect-reflect' method. The identity of this group is called the point at infinity, denoted by ∞.



An elliptic curve has a group structure. The group structure is obtained using the 'connect-intersect-reflect' method. The identity of this group is called the point at infinity, denoted by ∞.



An elliptic curve has a group structure. The group structure is obtained using the 'connect-intersect-reflect' method. The identity of this group is called the point at infinity, denoted by ∞. So, $P + Q = \infty$.



Using the same equations for the 'connect-intersect-reflect' method, we also find a group law for elliptic curves over finite fields.

Example

The elliptic curve $y^2 = x^3 + x$ *over* $\mathbb{F}_7$ *has eight points with coordinates in* $\mathbb{F}_7$*:*

$$E = \{\infty, (0,0), (1, \pm 3), (3, \pm 4), (5, \pm 2)\}$$

It has other points in extension fields (e.g. in $\mathbb{F}_7(i)$*) such as* $(2, 2i)$*:*

$$\begin{array}{rcccccl} y^2 & = & (2i)^2 & = & -4 & \equiv & 3 \bmod 7 \\ x^3 + x & = & 2^3 + 2 & = & 10 & \equiv & 3 \bmod 7. \end{array}$$

Note that 'multiplication-by-m' is a group homomorphism from E to E (i.e. an endomorphism of E).

$$-1 \cdot (5, 2) = (5, -2) \qquad 2 \cdot (5, 2) = (1, 3)$$
$$-1 \cdot (1, 3) = (1, -3) \qquad 2 \cdot (1, 3) = (0, 0)$$

Note that 'multiplication-by-m' is a group homomorphism from E to E (i.e. an endomorphism of E).

$$-1 \cdot (5, 2) = (5, -2) \qquad 2 \cdot (5, 2) = (1, 3)$$
$$-1 \cdot (1, 3) = (1, -3) \qquad 2 \cdot (1, 3) = (0, 0)$$

Some elliptic curves have extra endomorphisms. For example, the elliptic curve $y^2 = x^3 + x$ has $i : (x, y) \mapsto (-x, iy)$.

$$i \cdot (5, 2) = (-5, 2i) \qquad i^2 \cdot (5, 2) = (5, -2)$$
$$i \cdot (1, 3) = (-1, 3i) \qquad i^2 \cdot (1, 3) = (1, -3)$$
$$i \cdot (-5, 2i) = (5, -2) \qquad i^2 \cdot (-5, 2i) = (-5, -2i)$$
$$i \cdot (-1, 3i) = (1, -3) \qquad i^2 \cdot (-1, 3i) = (1, -3i)$$

Note that 'multiplication-by-m' is a group homomorphism from E to E (i.e. an endomorphism of E).

$$-1 \cdot (5, 2) = (5, -2) \qquad 2 \cdot (5, 2) = (1, 3)$$
$$-1 \cdot (1, 3) = (1, -3) \qquad 2 \cdot (1, 3) = (0, 0)$$

Some elliptic curves have extra endomorphisms. For example, the elliptic curve $y^2 = x^3 + x$ has $i : (x, y) \mapsto (-x, iy)$.

$$i \cdot (5, 2) = (-5, 2i) \qquad i^2 \cdot (5, 2) = (5, -2)$$
$$i \cdot (1, 3) = (-1, 3i) \qquad i^2 \cdot (1, 3) = (1, -3)$$
$$i \cdot (-5, 2i) = (5, -2) \qquad i^2 \cdot (-5, 2i) = (-5, -2i)$$
$$i \cdot (-1, 3i) = (1, -3) \qquad i^2 \cdot (-1, 3i) = (1, -3i)$$

Observe that $i^2 \cdot P = -P$.
It is similar to how $i^2 = -1$ (as complex numbers).

Trial Division

To prove N is prime, it suffices to check if it is divisible by integers greater than 1 whose value is at most $\sqrt{N}$.

We prove that $q = 31$ is prime. Note that $\sqrt{31} \approx 5.5678$.

$$31 \text{ divided by } 2 = 15 \text{ r. } 1$$
$$31 \text{ divided by } 3 = 10 \text{ r. } 1$$
$$31 \text{ divided by } 4 = 7 \text{ r. } 3$$
$$31 \text{ divided by } 5 = 6 \text{ r. } 1$$

Proposition

Let $6 < N$ *be an integer. If there exists:*

- *an integer* m
- *a prime* q
- *an elliptic curve* E *over* $\mathbb{Z}/N\mathbb{Z}$
- *and a point* P *on* E

such that

- $m = qs$ *for some* $s \in \mathbb{Z}$
- $q > \left(N^{1/4} + 1\right)^2$
- $mP = \infty$
- $sP \neq \infty$

then N *is prime.*

Proposition

Let $6 < N = 97$ *be an integer. If there exists:*

- *an integer* m
- *a prime* q
- *an elliptic curve* E *over* $\mathbb{Z}/N\mathbb{Z}$
- *and a point* P *on* E

such that

- $m = qs$ *for some* $s \in \mathbb{Z}$
- $q > \left(N^{1/4} + 1\right)^2$
- $mP = \infty$
- $sP \neq \infty$

then N *is prime.*

Proposition

Let $6 < N = 97$ *be an integer. If there exists:*

- *an integer* $m = 93$
- *a prime* q
- *an elliptic curve* E *over* $\mathbb{Z}/N\mathbb{Z}$
- *and a point* P *on* E

such that

- $m = qs$ *for some* $s \in \mathbb{Z}$
- $q > \left(N^{1/4} + 1\right)^2$
- $mP = \infty$
- $sP \neq \infty$

then N *is prime.*

Proposition

Let $6 < N = 97$ *be an integer. If there exists:*

- *an integer* $m = 93$
- *a prime* $q = 31$
- *an elliptic curve* E *over* $\mathbb{Z}/N\mathbb{Z}$
- *and a point* P *on* E

such that

- $m = qs$ *for some* $s \in \mathbb{Z}$
- $q > \left(N^{1/4} + 1\right)^2$
- $mP = \infty$
- $sP \neq \infty$

then N *is prime.*

Proposition

Let $6 < N = 97$ *be an integer. If there exists:*

- *an integer* $m = 93$
- *a prime* $q = 31$
- *an elliptic curve* E *over* $\mathbb{Z}/N\mathbb{Z}$*, say,* $E : y^2 = x^3 + 69x + 2$
- *and a point* P *on* E

such that

- $m = qs$ *for some* $s \in \mathbb{Z}$
- $q > \left(N^{1/4} + 1\right)^2$
- $mP = \infty$
- $sP \neq \infty$

then N *is prime.*

Proposition

Let $6 < N = 97$ *be an integer. If there exists:*

- *an integer* $m = 93$
- *a prime* $q = 31$
- *an elliptic curve* E *over* $\mathbb{Z}/N\mathbb{Z}$, *say,* $E : y^2 = x^3 + 69x + 2$
- *and a point* P *on* E, *say,* $P = (12, 91)$

such that

- $m = qs$ *for some* $s \in \mathbb{Z}$
- $q > \left(N^{1/4} + 1\right)^2$
- $mP = \infty$
- $sP \neq \infty$

then N *is prime.*

Proposition

Let $6 < N = 97$ *be an integer. If there exists:*

- *an integer* $m = 93$
- *a prime* $q = 31$
- *an elliptic curve* E *over* $\mathbb{Z}/N\mathbb{Z}$*, say,* $E : y^2 = x^3 + 69x + 2$
- *and a point* P *on* E*, say,* $P = (12, 91)$

such that

- $m = qs$ *for some* $s \in \mathbb{Z}$*. We have* $s = 3 \in \mathbb{Z}$ *since* $93 = 31 \cdot 3$*.*
- $q > \left(N^{1/4} + 1\right)^2$
- $mP = \infty$
- $sP \neq \infty$

then N *is prime.*

Proposition

Let $6 < N = 97$ *be an integer. If there exists:*

- *an integer* $m = 93$
- *a prime* $q = 31$
- *an elliptic curve* E *over* $\mathbb{Z}/N\mathbb{Z}$, *say,* $E : y^2 = x^3 + 69x + 2$
- *and a point* P *on* E, *say,* $P = (12, 91)$

such that

- $m = qs$ *for some* $s \in \mathbb{Z}$. *We have* $s = 3 \in \mathbb{Z}$ *since* $93 = 31 \cdot 3$.
- $q > \left(N^{1/4} + 1\right)^2 \approx 17.125$.
- $mP = \infty$
- $sP \neq \infty$

then N *is prime.*

Proposition

Let $6 < N = 97$ *be an integer. If there exists:*

- *an integer* $m = 93$
- *a prime* $q = 31$
- *an elliptic curve* E *over* $\mathbb{Z}/N\mathbb{Z}$*, say,* $E : y^2 = x^3 + 69x + 2$
- *and a point* P *on* E*, say,* $P = (12, 91)$

such that

- $m = qs$ *for some* $s \in \mathbb{Z}$*. We have* $s = 3 \in \mathbb{Z}$ *since* $93 = 31 \cdot 3$*.*
- $q > \left(N^{1/4} + 1\right)^2 \approx 17.125$*.*
- $mP = \infty$*.* E *has exactly* 93 *points so for any* P*, we have* $mP = \infty$*.*
- $sP \neq \infty$

then N *is prime.*

Proposition

Let $6 < N = 97$ *be an integer. If there exists:*

- *an integer* $m = 93$
- *a prime* $q = 31$
- *an elliptic curve* E *over* $\mathbb{Z}/N\mathbb{Z}$*, say,* $E : y^2 = x^3 + 69x + 2$
- *and a point* P *on* E*, say,* $P = (12, 91)$

such that

- $m = qs$ *for some* $s \in \mathbb{Z}$*. We have* $s = 3 \in \mathbb{Z}$ *since* $93 = 31 \cdot 3$*.*
- $q > \left(N^{1/4} + 1\right)^2 \approx 17.125$*.*
- $mP = \infty$*.* E *has exactly* 93 *points so for any* P*, we have* $mP = \infty$*.*
- $sP \neq \infty$*.* $3P = (23, 46) \neq \infty$*.*

then N *is prime.*

Proposition

Let $6 < N = 97$ *be an integer. If there exists:*

- *an integer* $m = 93$
- *a prime* $q = 31$
- *an elliptic curve* E *over* $\mathbb{Z}/N\mathbb{Z}$*, say,* $E : y^2 = x^3 + 69x + 2$
- *and a point* P *on* E*, say,* $P = (12, 91)$

such that

- $m = qs$ *for some* $s \in \mathbb{Z}$*. We have* $s = 3 \in \mathbb{Z}$ *since* $93 = 31 \cdot 3$*.*
- $q > \left(N^{1/4} + 1\right)^2 \approx 17.125$*.*
- $mP = \infty$*.* E *has exactly* 93 *points so for any* P*, we have* $mP = \infty$*.*
- $sP \neq \infty$*.* $3P = (23, 46) \neq \infty$*.*

then N *is prime.*

It remains to prove that $q = 31$ is prime.

To find the above data:

- Let $D < 0$ be a fundamental discriminant.
  That is, either $D = 4m$ for some $m \in \mathbb{Z}$ which is square-free or $D \equiv 1 \bmod 4$ and D is square-free.
- Find integers U, V such that $U^2 + |D|V^2 = 4N$.
  Take $m = N + 1 - U$.
  This requires solving a diophantine equation.
- Can you write m as $m = qs$? If not, go back to step 1.
  This involves removing small prime factors of m.
- Find an elliptic curve E with **complex multiplication** by the imaginary quadratic number field $K = \mathbb{Q}(\sqrt{-|D|})$.
  A twist of this elliptic curve E will have exactly m points modulo N.
- Find a point P that satisfies the conditions.
  Guess a point. The odds are in your favor.

- Download PARI on your smartphone.
  Google Play Store: `https://shorturl.at/krtxD`

- Download PARI on your smartphone.
  Google Play Store: `https://shorturl.at/krtxD`
- Enter the following commands:

PariDroid

```
?
```

- Download PARI on your smartphone.
  Google Play Store: `https://shorturl.at/krtxD`
- Enter the following commands:

PariDroid

```
? N = 10^35 + 69
?
```

- Download PARI on your smartphone.
  Google Play Store: `https://shorturl.at/krtxD`
- Enter the following commands:

PariDroid

```
? N = 10^35 + 69
? cert = primecert(N)
?
```

- Download PARI on your smartphone.
  Google Play Store: `https://shorturl.at/krtxD`
- Enter the following commands:

PariDroid

```
? N = 10^35 + 69
? cert = primecert(N)
? print(primecertexport(cert))
```

- Download PARI on your smartphone.
  Google Play Store: `https://shorturl.at/krtxD`
- Enter the following commands:

PariDroid

```
? N = 10^35 + 69
? cert = primecert(N)
? print(primecertexport(cert))
```

- You can choose a different **prime** N as long as $N > 2^{64}$.
  Otherwise, you can just check if N divides any prime less than 2^{32}.