Integer factorization and elliptic curves

Sebastiano Tronto

2021-04-14

Fundamental Theorem of Arithmetic

Theorem

Every positive integer can be decomposed as a finite product of prime numbers in a unique way.

Integer factorization

$$n \rightsquigarrow p_1^{e_1} p_2^{e_2} \cdots p_t^{e_t}$$

- Basic arithmetic operations ($+$, $-$, $\times$, integer division, remainder) are fast, factorizing is not.
- Unknown if n can be factorized in "polynomial time" $O((\log n)^k)$.
- Some cryptographic protocols rely on this problem being hard.

Naive algorithm

Key idea: enough to find one (prime) factor.

function `find_one_factor`(n):
  for $i \in \{2, 3, \dots, \lfloor\sqrt{n}\rfloor\}$:
    if $n \bmod i = 0$:
      return i
  return n `# n is prime`

Complexity: $O(\sqrt{n})$

Pollard's $p-1$ method

Assume n not prime (can be tested in polynomial time)

- Pick $x \in (\mathbb{Z}/n\mathbb{Z})^\times$ and $M \in \mathbb{Z}_{>0}$;
- Compute $g = \gcd(x^M - 1, n)$:
  (a) If $1 < g < n$: success!
  (b) If $g = 1$: try larger M
  (c) If $g = n$ (rare): try smaller M or different x

Note: if $p-1$ divides M then $g > 1$ (*Fermat's Little Theorem*)

a^b is fast

function $\texttt{pow}(a, b)$:
    if $b = 0$:
        return 1
    if b is even:
        return $\texttt{pow}(a \cdot a, b/2)$
    return $a \cdot \texttt{pow}(a, b - 1)$

Complexity: $O(\log b)$
(After 2 steps, b is halved)

$\gcd(a, b)$ is fast

Key idea: $\gcd(a, b) = \gcd(b, a \bmod b)$.

function $\texttt{gcd}(a, b)$:
  if $b = 0$:
    return a
  return $\texttt{gcd}(b, a \bmod b)$

Complexity: $O(\log a)$
(After 2 steps, a is halved)

A bird's-eye view

Pollard's method

We take a group $G = (\mathbb{Z}/n\mathbb{Z})^\times$ *and an element* $(x \bmod n) \in G$. *We compute* $(x \bmod n)^M$ *in* G *for some* M, *and from this we find an integer* $z = x^M - 1$, *hoping that* $1 < \gcd(z, n) < n$.

Elliptic curves

- Let K be a field with $\mathrm{char}(K) \neq 2, 3$
- An **elliptic curve** over K is defined by a projective equation

$$E : Y^2Z = X^3 + AXZ^2 + BZ^3 \qquad A, B \in K,\ 4A^3 \neq -27B^2$$

that is

$$E = \{(x : y : 1) \mid x, y \in \overline{K},\ y^2 = x^3 + Ax + B\} \cup \{(0 : 1 : 0)\}$$

- $E(K)$ = points of E with coordinates in K

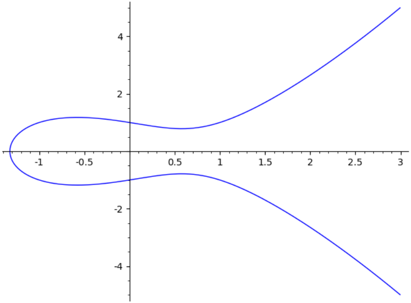


Figure: $y^2 = x^3 - x + 1$

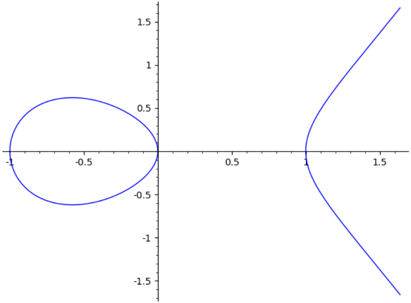
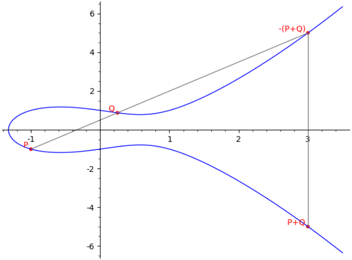


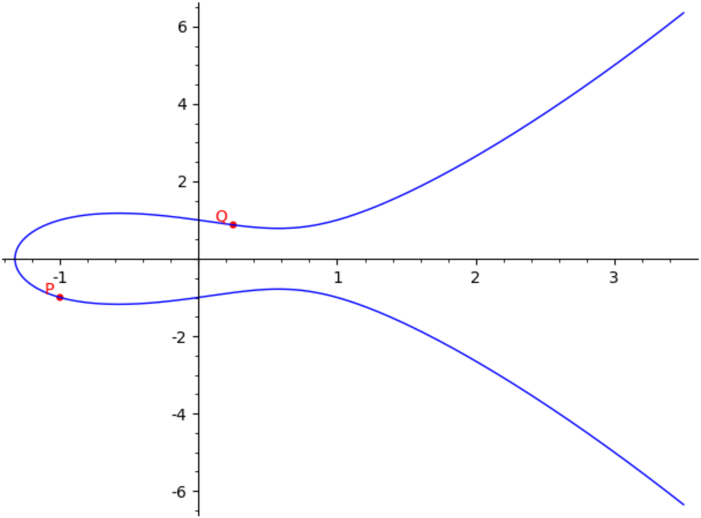
Figure: $y^2 = x^3 - x$

Group law

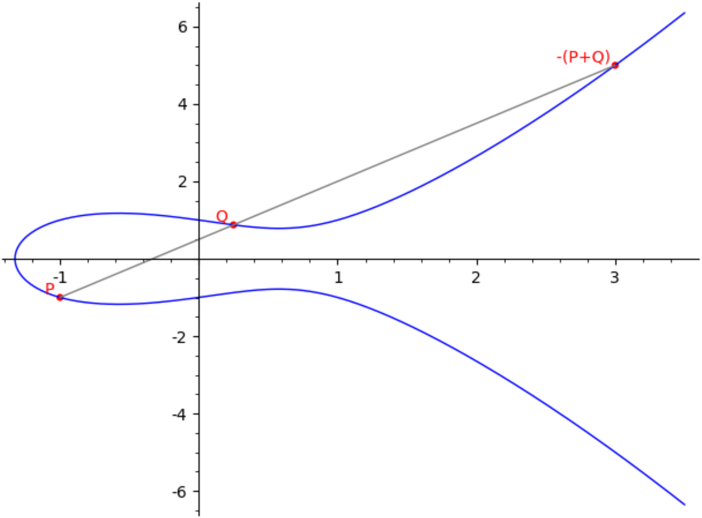
- E is a commutative group
- $P, Q \in E(K) \implies P + Q \in E(K)$
- $(0 : 1 : 0)$ is the neutral element
- $-P$: reflect along x-axis



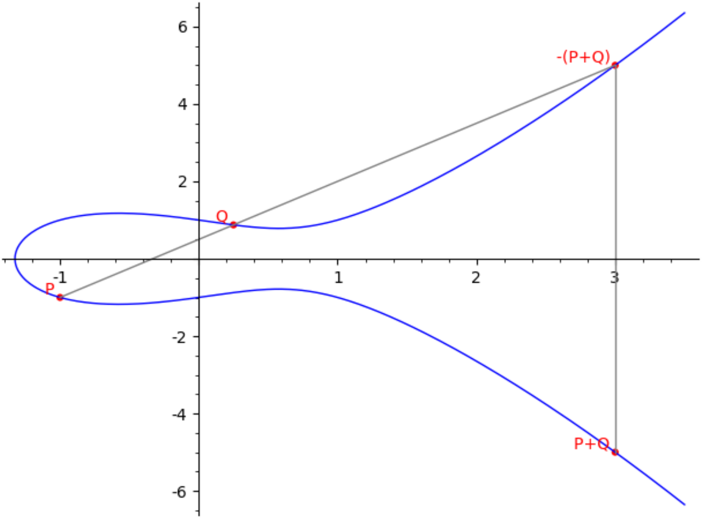
Group law example 1



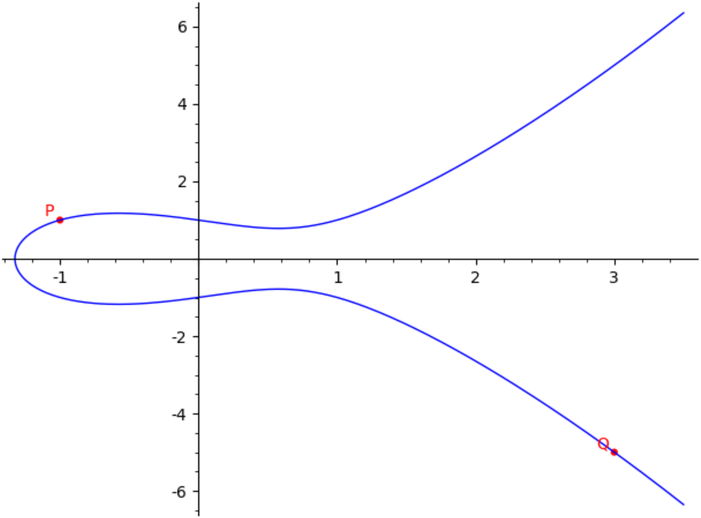
Group law example 1



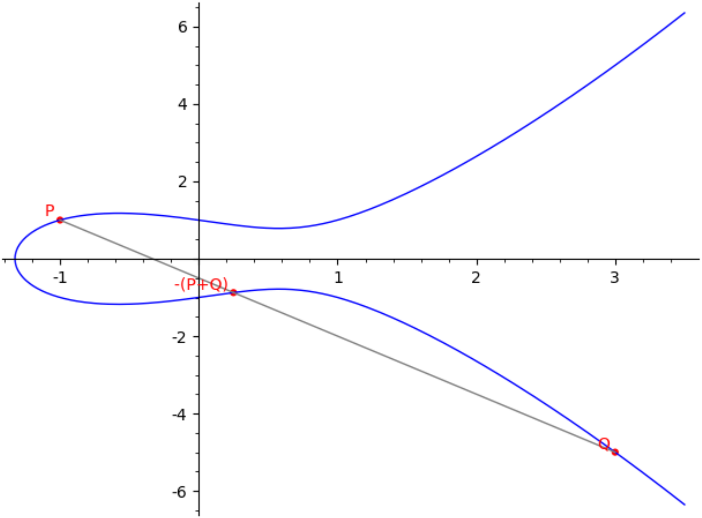
Group law example 1



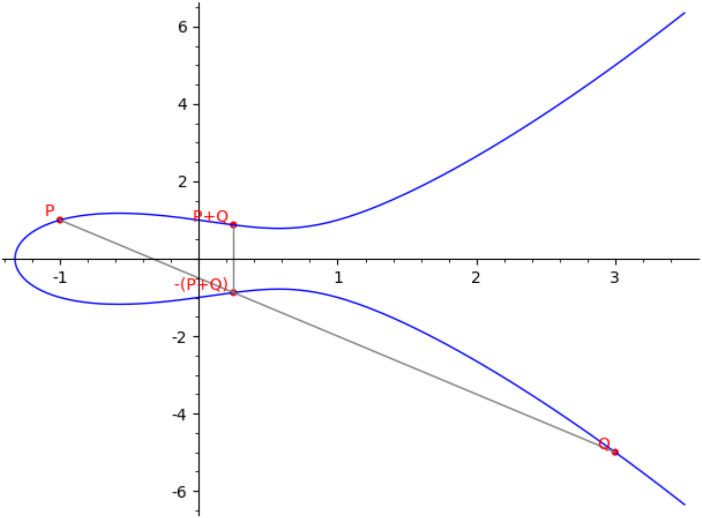
Group law example 2



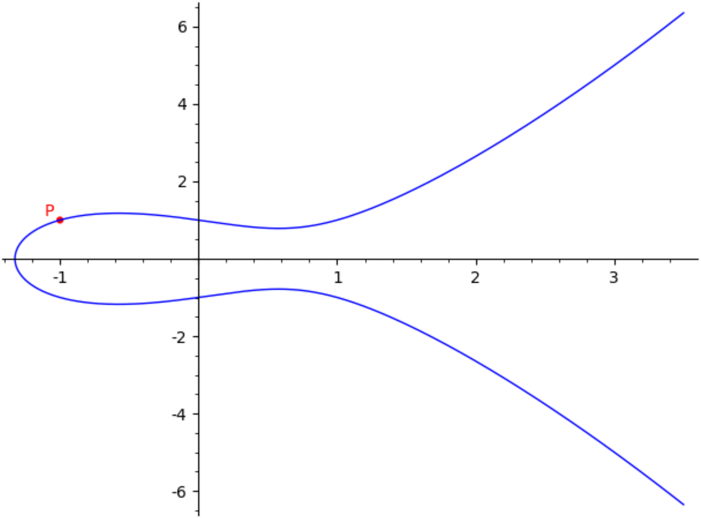
Group law example 2



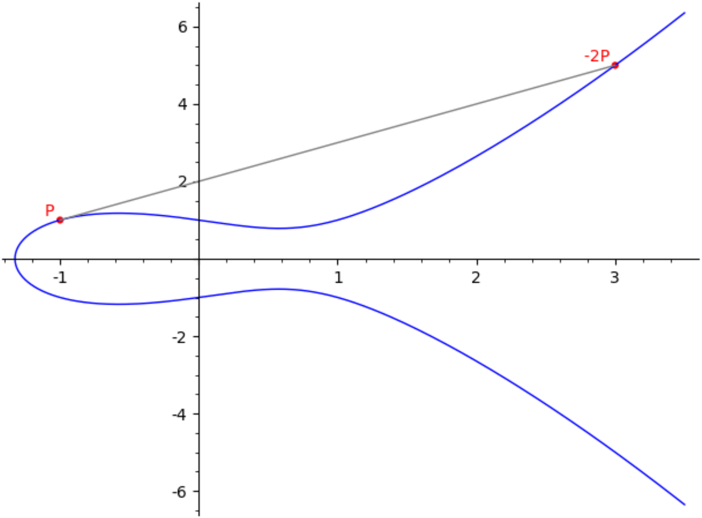
Group law example 2



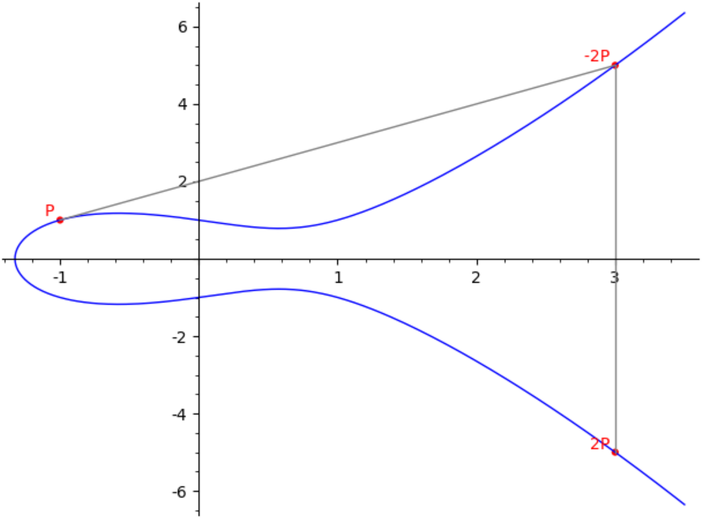
Group law example 3



Group law example 3



Group law example 3



Group law procedure

function sum(A, B, $(x_1 : y_1 : z_1)$, $(x_2 : y_2 : z_2)$):

  if $z_1 = 0$:

    return $(x_2 : y_2 : z_2)$

  if $z_2 = 0$:

    return $(x_1 : y_1 : z_1)$

  x_1 := x_1/z_1; y_1 := y_1/z_1; x_2 := x_2/z_2 y_2 := y_2/z_2

  if $x_1 = x_2$ and $y_1 = -y_2$:

    return $(0 : 1 : 0)$

  if $(x_1, y_1) \neq (x_2, y_2)$:

    λ := $(y_1 - y_2)/(x_1 - x_2)$

  else:

    λ := $(3x_1^2 + A)/2y_1$

  x_3 := $\lambda^2 - x_1 - x_2$; y_3 := $\lambda(x_1 - x_3) - y_1$

  return $(x_3 : y_3 : 1)$

Group of points: examples

- If $K = \mathbb{C}$ then $E(K) \cong \mathbb{R}^2/\mathbb{Z}^2$ as a group (torus)
- If K is a finite extension of $\mathbb{Q}$ then $E(K) \cong \mathbb{Z}^r \oplus T$ with $r \in \mathbb{Z}_{\geq 0}$ and T finite (Mordell-Weil theorem)
- If $K = \mathbb{F}_q$ is finite then $\#E(K) = q + 1 - t$ with $-2\sqrt{q} \leq t \leq 2\sqrt{q}$ (Hasse's Theorem)

Algebraic groups in general

- *Algebraic varieties* with an *algebraic* (*geometric*) group law
- The group law is related to the arithmetic of the base field (intuitively: because points have coordinates)

Elliptic curves over $\mathbb{Z}/n\mathbb{Z}$

- Let $n \in \mathbb{Z}_{>0}$ and $A, B \in \mathbb{Z}$ with $\gcd(6(4A^3 + 27B^2), n) = 1$.
- Consider the set of points of an "elliptic curve" $\bmod n$

$$E(\mathbb{Z}/n\mathbb{Z}) = \\ = \{(x : y : 1) \mid x, y \in \mathbb{Z}/n\mathbb{Z},\ y^2 = x^3 + Ax + B\} \cup \{(0 : 1 : 0)\}$$

- If $p \mid n$ is prime

$$E_p : Y^Z = X^3 + (A \bmod p)XZ^2 + (B \bmod p)Z^3$$

is an elliptic curve over $\mathbb{F}_p$ and

$$E_p(\mathbb{F}_p) = \{(x : y : z) \bmod p \mid (x : y : z) \in E(\mathbb{Z}/n\mathbb{Z})\}$$

Elliptic curve factorization method (ECM)

- Pick P in $E(\mathbb{Z}/n\mathbb{Z})$ and $M \in \mathbb{Z}_{>0}$;
- Compute $g = \gcd(z, n)$, where z is the z-coordinate of

$$M \cdot P = \underbrace{P + P + \cdots + P}_{M \text{ times}}$$

- If $(M \cdot P \bmod p) = (0 : 1 : 0)$ in $E_p(\mathbb{F}_p)$ for some $p \mid n$ then $g > 1$

Elliptic curve factorization method (ECM)

- **Problem:** group law of $E(\mathbb{Z}/n\mathbb{Z})$ is more complicated
- The procedure can fail when dividing by $z \in \mathbb{Z}/n\mathbb{Z}$...
- ...but this means that $\gcd(z, n) > 1$!
- **Workaround:** write a procedure that given two points it returns either "their sum" or a factor of n

Partial group law

Let $n \in \mathbb{Z}_{>0}$ and $V_n = \{(x : y : 1) \mid x, y \in \mathbb{Z}/n\mathbb{Z}\} \cup \{(0 : 1 : 0)\}$.

Definition

If $A \in \mathbb{Z}$ and $P, Q, R \in V_n$ we say that "$P +_A Q = R$" if for every prime p dividing n such that there is $B \in \mathbb{Z}$ such that

$$E : Y^2 Z = X^3 + (A \bmod p) X Z^2 + (B \bmod p) Z^3$$

is an elliptic curve over $\mathbb{F}_p$ with $(P \bmod p), (Q \bmod p) \in E(\mathbb{F}_p)$, then $(P \bmod p) + (Q \bmod p) = (R \bmod p)$ in $E(\mathbb{F}_p)$.

Partial group law procedure

Proposition

There is a finite procedure that, given $n \in \mathbb{Z}_{>1}$, $A \in \mathbb{Z}$ and two points $P, Q \in V_n$, either computes a non-trivial factor of n or a point $R \in V_n$ with "$P +_A Q = R$".

Partial group law procedure

function `sum_or_factor(`A, $(x_1 : y_1 : z_1)$, $(x_2 : y_2 : z_2)$`):`

    if `one of the points is` $(0 : 1 : 0)$`:`

        return `the other`

    if $1 < \gcd(x_1 - x_2, n) < n$ **or** $1 < \gcd(y_1 + y_2, n) < n$`:`

        `we found a factor,` **stop**

    if $\gcd(x_1 - x_2, n) = \gcd(y_1 + y_2, n) = n$

        return $(0 : 1 : 0)$

    if $\gcd(x_1 - x_2, n) = 1$`:`

        λ `:=` $(y_1 - y_2)/(x_1 - x_2)$ `# Operations modulo` n

    if $\gcd(x_1 - x_2, n) = n$`:`

        λ `:=` $(3x_1^2 + A)/(y_1 + y_2)$

    x_3 `:=` $\lambda^2 - x_1 - x_2$`;` y_3 `:=` $\lambda(x_1 - x_3) - y_1$

    return $(x_3 : y_3 : 1)$

Lenstra's ECM

- Pick $A \in \mathbb{Z}$, $P \in V_n$ and $M \in \mathbb{Z}_{>0}$;
- Attempt to compute

$$\underbrace{P +_A P +_A \cdots +_A P}_{M \text{ times}}$$

with the procedure above.

(a) If the procedure fails: success!
(b) If the procedure succeeds, we have failed.

Lenstra's ECM

- Advantage over Pollard's method: we can change the curve (we are actually using all of them at once)
- In practice: used to find small factors ($50 \sim 60$ digits) before applying algorithms that are asymptotically more efficient (number field sieve)

Reference: Lenstra, H. W., "Factoring integers with elliptic curves." *Annals of mathematics* (1987): 649-673.