Part I

Elliptic Curve Cryptography

Elliptic Curves

Elliptic curves are the set of the solutions to a particular equation of the form:

$$y^2 = x^3 + bx + c$$

where x, y, b, c are defined over a field. A special "point at infinity", denoted as ∞ or $\mathcal{O}$ is also part of the curve.

The curves of cryptographic interest are those defined over

$GF(p)$ with p large prime.

$GF(p^n)$ with n large and p small prime (typically $p = 2$)

The Elliptic Curve and the point addition operation (defined later) form an abelian group. Depending on b, c there are several curves with different properties.

1. Elliptic Curve Cryptography

- Square Roots in $\mathbb{Z}_p$
- Elliptic Curves over $\mathbb{R}$
- Addition Law
- Elliptic Curves over $\mathbb{Z}_p$
- Applications to Cryptography

Square Roots in $\mathbb{Z}_p$

Consider the equation

$$x^2 \equiv a \pmod{p} \quad \text{where } p \text{ is an odd prime}$$

If the equation has at least one solution, then a is called a quadratic residue, otherwise a is called a quadratic nonresidue.

The equation has exactly one solution if and only if $a \equiv 0$, then the solution is $x \equiv 0$.

Otherwise there are either 2 or no solutions.

Legendre Symbol

The Legendre symbol is defined as

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is a residue mod } p \text{ and } a \not\equiv 0 \pmod{p} \\ 0 & \text{if } a \equiv 0 \pmod{p} \\ -1 & \text{if } a \text{ is a nonresidue mod } p \end{cases}$$

Theorem

If p is an odd prime, then

$$\left(\frac{a}{p}\right) = a^{(p-1)/2} \bmod p$$

Computation of the Roots

It is easy to check whether a is a residue. Finding the root requires more work.

Theorem

If a is a residue mod p and $p \equiv 3 \pmod 4$, then

$$x \equiv \pm a^{(p+1)/4} \pmod p$$

This is the case most commonly used in cryptography. For $p \equiv 1 \pmod 4$ there are less efficient algorithms, so this case is less interesting. Note that, if a is a non residue, the formula produces garbage.

1. Elliptic Curve Cryptography

- Square Roots in $\mathbb{Z}_p$
- Elliptic Curves over $\mathbb{R}$
- Addition Law
- Elliptic Curves over $\mathbb{Z}_p$
- Applications to Cryptography

Elliptic Curves over the Reals

A curve over the reals has infinite points. The equation $x^3 + bx + c = 0$ can have either 3 or 1 real solutions.

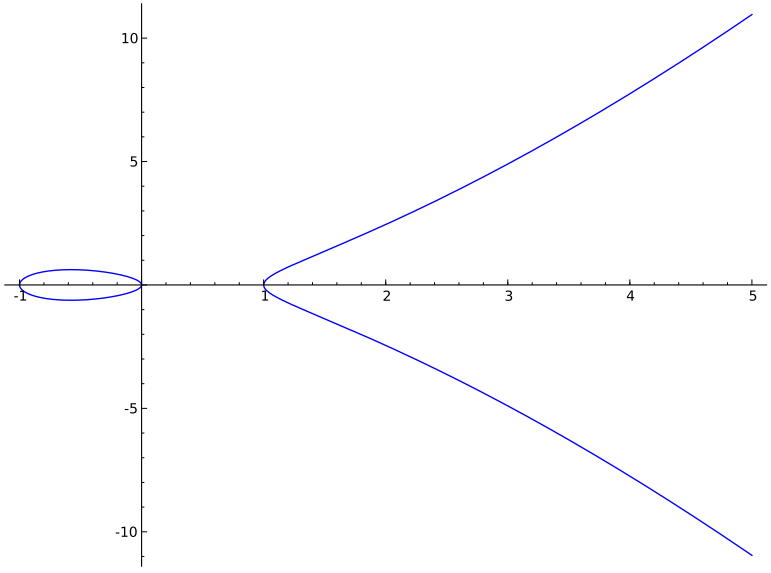


Figure: The Elliptic Curve of equation $y^2 = x(x+1)(x-1) = x^3 - x$

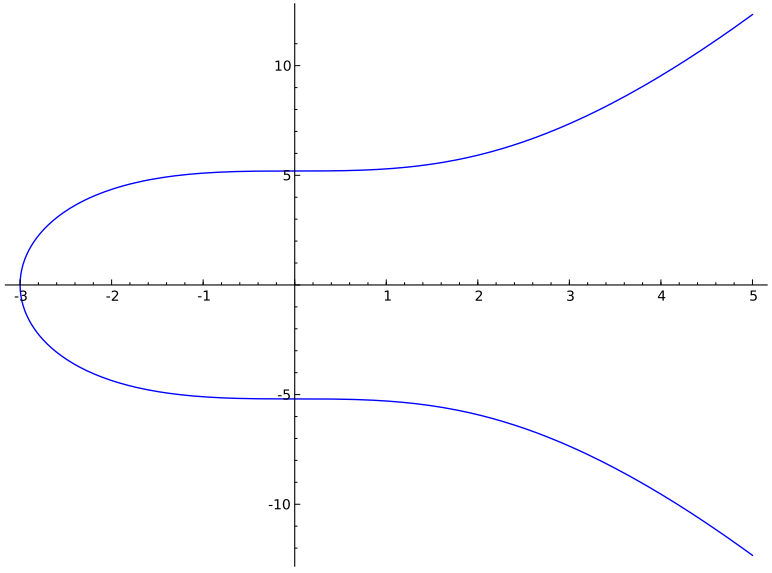


Figure: The Elliptic Curve of equation $y^2 = (x+3)^3 = x^3 + 27$

Singular Curves

If $4b^3 + 27c^2 = 0$ two of the solutions are coincident. These curves are called singular.

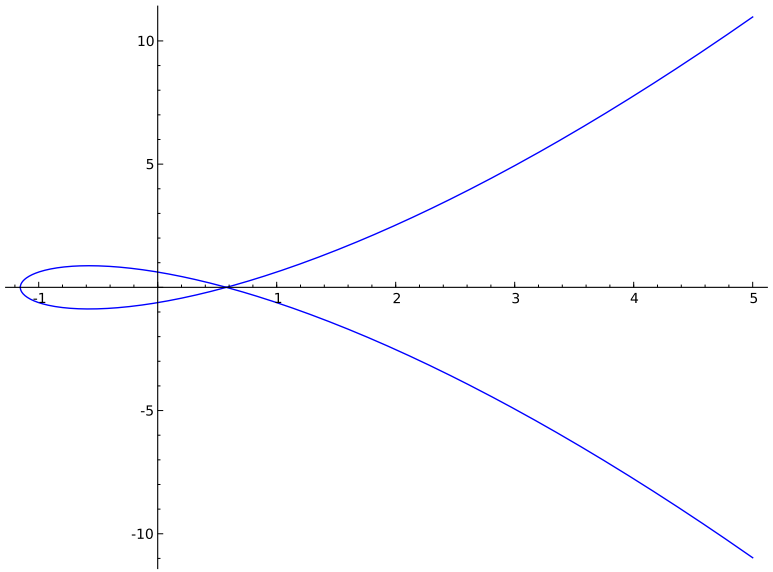


Figure: The Elliptic Curve of equation $y^2 = x^3 - x + \frac{2\sqrt{3}}{9}$

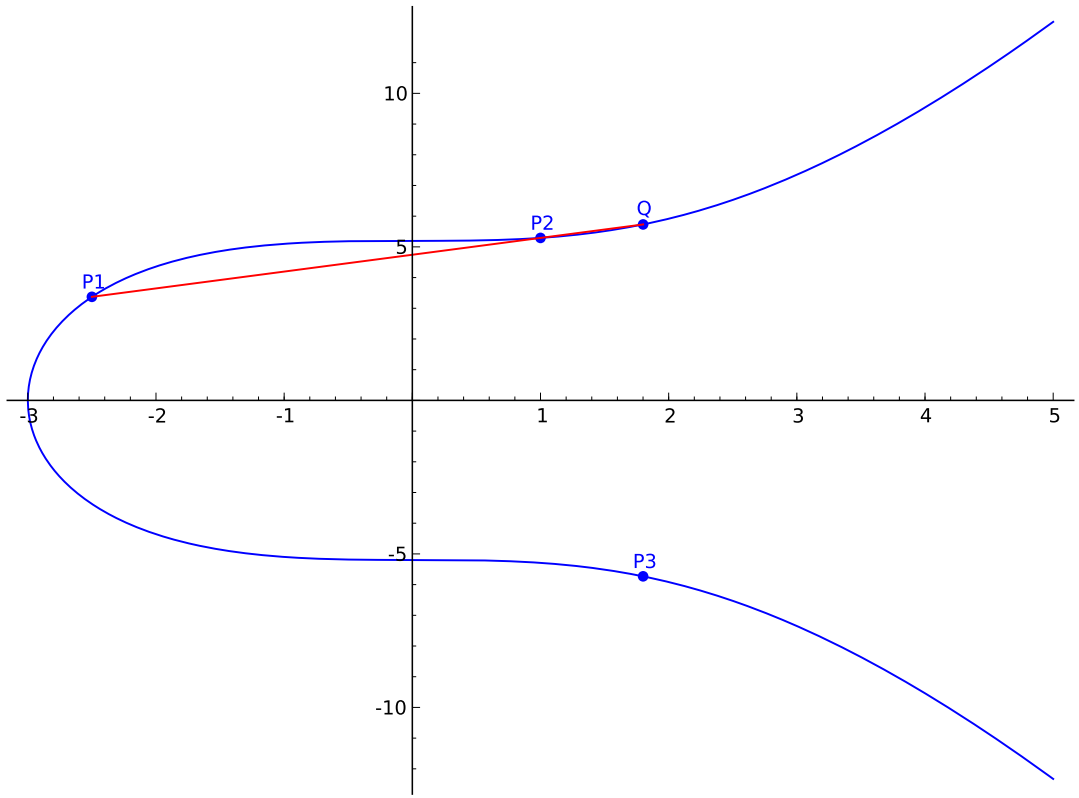
1. Elliptic Curve Cryptography

- Square Roots in $\mathbb{Z}_p$
- Elliptic Curves over $\mathbb{R}$
- Addition Law
- Elliptic Curves over $\mathbb{Z}_p$
- Applications to Cryptography

Addition Law

General Case

Given two points $P_1, P_2 \in E$, the line through P_1 and P_2 intersects the curve in a third point. Call this point Q. The result of the operation $P_1 + P_2$ is the point P_3, symmetric to Q w.r.t. the x-axis.



Special Cases and Properties

There are some special cases

- If $P_1 = P_2$ the line between P_1 and P_2 is the line tangent to E in P_1
- If P_1 and P_2 are symmetric w.r.t. the x-axis, the intersection is the point at infinity
- If $P_1 = P_2$ lies on the x-axis, the intersection is the point at infinity

Some properties

- $(E, +)$ is an Abelian group
- If $P = (x, y)$, then $-P = (x, -y)$
- The identity element is the point at infinity

Computation of the Sum ($P_1 \neq P_2$)

Consider the equation $y^2 = x^3 + bx + c$ and the points $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2)$, with $P_1 \neq P_2$.
We want to calculate $P_3 = (x_3, y_3) = P1 + P2$.

The line through P_1 and P_2 has angular coefficient

$$m = \frac{y_2 - y_1}{x_2 - x_1}$$

and equation $y = m(x - x_1) + y_1 = mx + (y_1 - mx_1)$.
Substituing in the curve equation, we obtain a third-grade equation with three solutions: $x^3 - m^2x^2 + \ldots$
Since we know two of the solutions, we exploit the property that the sum of the solutions is equal to minus the coefficient of x^2.
So:

$$x_1 + x_2 + x_3 = m^2$$

We calculate y_3 by substituting in the line equation and changing the sign.

Computation of the Sum ($P_1 = P_2$)

Consider the equation $y^2 = x^3 + bx + c$ and the point $P_1 = (x_1, y_1)$.
We want to calculate $P_3 = (x_3, y_3) = 2P1$.

To compute the line tangent to E in P_1 we use the differentials.

$$d(y^2) = d(x^3 + bx + c)$$
$$2ydy = (3x^2 + b)dx$$

So the angular coefficient of the tangent is

$$m = \frac{dy}{dx} = \frac{3x_1^2 + b}{2y_1}$$

The, we proceed like the previous case:

$$2x_1 + x_3 = m^2$$

Computation of the Sum

Point Addition over Elliptic Curves

Given $y^2 = x^3 + bx + c$ and the point P_1 and P_2, to compute $P_3 = P_1 + P_2$ we have the following formulas:

$$m = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1} & \text{if } P_1 \neq P_2 \\ \frac{3x_1^2 + b}{2y_1} & \text{if } P_1 = P_2 \end{cases}$$

$$x_3 = m^2 - x_1 - x_2$$

$$y_3 = m(x_1 - x_3) - y_1$$

Note that

- If $P_1 \neq P_2$ but $x_1 = x_2$, then $P_1 = -P_2$ and $P_3 = \infty$.
- If $P_1 = P_2$ and $y_1 = 0$, then $P_1 = -P_1$ and $P_3 = \infty$.

1. Elliptic Curve Cryptography

- Square Roots in $\mathbb{Z}_p$
- Elliptic Curves over $\mathbb{R}$
- Addition Law
- Elliptic Curves over $\mathbb{Z}_p$
- Applications to Cryptography

Elliptic Curves over $\mathbb{Z}_p$

When working over $\mathbb{Z}_p$, with p odd prime, the equation becomes:

$$y^2 \equiv x^3 + bx + c \pmod{p}$$

We will consider nonsingular curves, i.e. with $4b^3 + 27c^2 \bmod p \neq 0$. The condition ensures that there are no repeated roots.
There are finitely many points in the curve and it is not trivial to find the actual number, N. Roughly, there are $p + 1$ points plus an error term, which may be large.

Theorem (Hasse's Theorem)

$$|N - p - 1| < 2\sqrt{p}$$

Elliptic Curves over $\mathbb{Z}_p$

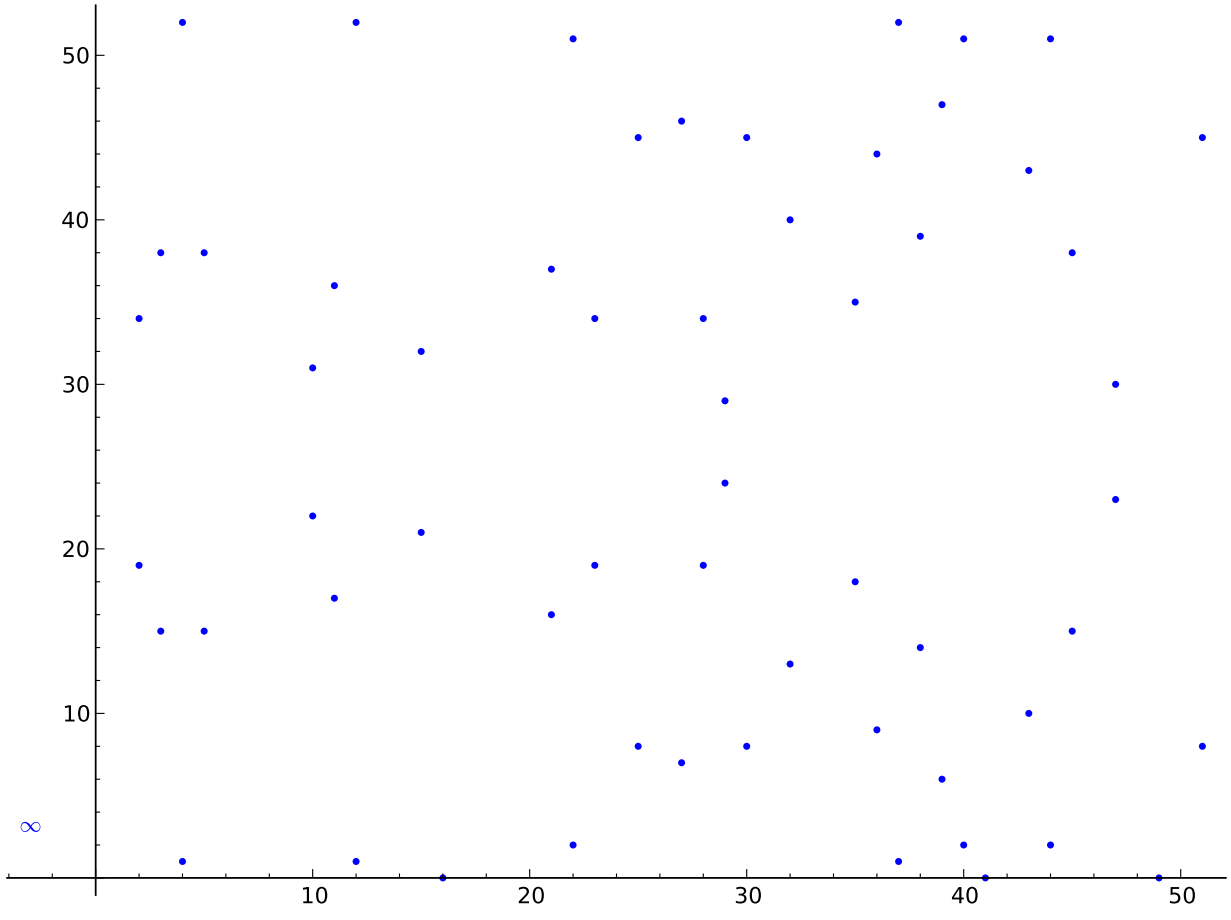


Figure: The curve $y^2 \equiv x^3 + 4x + 27 \pmod{53}$

Elliptic Curves over $\mathbb{Z}_p$

Addition law

The addition law is analogous to the real case. Obviously, the derivation of the rules follows a different path, since there are no derivatives in the discrete case.

Point Addition over Elliptic Curves

Given $y^2 \equiv x^3 + bx + c \pmod{p}$ and the point P_1 and P_2, to compute $P_3 = P_1 + P_2$ we have the following formulas:

$$m = \begin{cases} (y_2 - y_1)(x_2 - x_1)^{-1} \bmod p & \text{if } P_1 \neq P_2 \\ (3x_1^2 + b)(2y_1)^{-1} \bmod p & \text{if } P_1 = P_2 \end{cases}$$

$$x_3 = m^2 - x_1 - x_2 \bmod p$$

$$y_3 = m(x_1 - x_3) - y_1 \bmod p$$

Similarly to the real case, if m cannot be calculated, then $P_3 = \infty$.

Elliptic Curves over $\mathbb{Z}_p$ as Finite Groups

- Elliptic Curves over $\mathbb{Z}_p$ form a finite, cyclic group with order N. The optimal case for cryptographic usage is when N is prime.
- Given a generator point A and a random point B, finding an integer $0 \leq k < N$ such that $B = kA$ is a DLP. It is estimated that finding the discrete log over a curve with $p \simeq 160$ bit has a complexity similar to finding the log over $\mathbb{Z}_q$ with $q \simeq 1880$ bit.
- Building a curve for cryptographic usage is a difficult task, mainly because there is no easy way to calculate N for a curve with random parameters. Further, several families of curves are subject to mathematical attacks. Therefore standarization bodies publish several sets of curves with various sizes.

1. Elliptic Curve Cryptography

- Square Roots in $\mathbb{Z}_p$
- Elliptic Curves over $\mathbb{R}$
- Addition Law
- Elliptic Curves over $\mathbb{Z}_p$
- Applications to Cryptography

Elliptic Curve Diffie-Hellman Key Exchange (ECDHKE)

ECDHKE Protocol

Common Input:

- a security parameter n
- a curve E, a generator G, its order $q \geq 2^n$
- a key derivation function $KDF(\cdot)$ that maps a point of the curve into $\{0,1\}^n$

Protocol:

1. Alice chooses $x \leftarrow \mathbb{Z}_q$ uniformly at random and computes $H_1 := xG$
2. Alice sends H_1 to Bob
3. Bob receives H_1. He chooses $y \leftarrow \mathbb{Z}_q$ uniformly at random and computes $H_2 := yG$. Bob sends H_2 to Alice and outputs the key $k_B := KDF(yH_1)$.
4. Alice receives H_2 and outputs the key $k_A := KDF(xH_2)$.

Comments on ECDHKE

No particular differences from standard DHKE.

The curve points are generally encoded in compressed form for transmission. For a given x there are at most two points, one having y odd and the other having y even. Therefore it is sufficient to send the x-coordinate and the y-coordinate mod 2. The receiver can recover the full point by using the curve's equation.

EC Integrated Encryption Scheme (ECIES)

Setup

ECIES is the most used hybrid encryption scheme over elliptic curves. It is used by Alice for sending messages to Bob.

ECIES Setup

Bob chooses

- a key derivation function KDF, a MAC scheme, a symmetric encryption scheme Enc
- a curve, a generator G
- his private key x and public key $K_B = xG$

EC Integrated Encryption Scheme (ECIES)

Encryption

Encryption

To encrypt a message m, Alice does the following

1. generate a random nonce $r \leftarrow \mathbb{Z}_q^*$ with $q = \text{ord}(G)$
2. calculate $R = rG$ and $P = (x_P, y_P) = rK_B$
3. derive a shared secret $s = x_P$ and compute the MAC and symmetric encryption keys $k_E \| k_M = KDF(s)$
4. encrypt the message $c = \text{Enc}_{k_E}(m)$
5. compute the MAC tag $t = MAC_{k_M}(c)$
6. send $R \| c \| t$

Decryption exploits the relation $P = xR = xrG = rK_B$.

ECDSS/ECDSA

Setup

The analogous of DSS/DSA over EC.

ECIES Setup

Bob chooses

- a hash function $H(\cdot)$.
- a curve, a point G with order q (G may not be a generator)
- his private key x and public key $K_B = xG$

ECDSS/ECDSA

Signature

ECDSS Signature (Sign)

On input a message $m \in 0,1^*$

1. Choose a security nonce $k \leftarrow \mathbb{Z}_q^*$ and set

$$R := kG$$
$$s := (H(m) + xx_R)k^{-1} \bmod q$$

2. Output (R, s)

ECDSS/ECDSA Signature Verification

ECDSS Signature (Vrfy)

On input a message m and a signature (R, s)

1. Compute

$$u_1 := H(m)s^{-1} \bmod q$$
$$u_2 := x_R s^{-1} \bmod q$$

2. Output 1 if

$$R = u_1 G + u_2 K_B$$