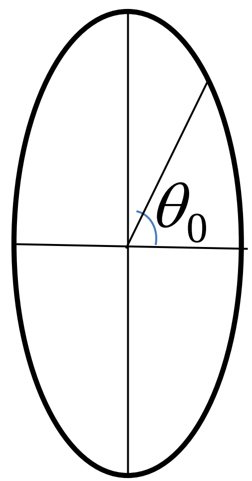
Elliptic Curve Cryptography

Prof AK Bhateja
Indian Institute of Technology Delhi

Why are they called "Elliptic" Curves?

- Consider ellipse $x^2/a^2 + y^2/b^2 = 1$



- Length of the arc on the ellipse for $0 \le \theta \le \theta_0$ using $x = a\cos\theta$, $y = b\sin\theta$

$$AL = \int_0^{\theta_0} \sqrt{a^2 sin^2\theta + b^2 cos^2\theta}\, d\theta$$

$$= \int_0^{\theta_0} \sqrt{a^2 sin^2\theta + b^2(1 - sin^2\theta)}\, d\theta$$

$$= b\int_0^{\theta_0} \sqrt{1 - k^2 sin^2\theta}\, d\theta \quad \text{where } k^2 = \frac{b^2 - a^2}{b^2}$$

$$AL = b\int_0^{\theta_0} \sqrt{1-k^2 sin^2\theta}\, d\theta \quad \text{where } k^2 = \frac{b^2-a^2}{b^2}$$

- if $k = 0$, then $a = b$, and this is just a circle.
- If $k = 1$, then $a = 0$, and this is a line segment.
- When $0 < k < 1$. Substitute $x = \sin^2\theta$

The antiderivative becomes$= \int \sqrt{1-k^2x}\left(\frac{dx}{2\sqrt{x}\sqrt{1-x}}\right) = \frac{1}{2}\int \frac{\sqrt{1-k^2x}}{\sqrt{x(1-x)}}dx$

$$= \frac{1}{2}\int \frac{1-k^2x}{\sqrt{x(1-x)}\sqrt{1-k^2x}}dx$$

Here $k \neq 0$ and $k \neq 1$

In general, integrals is of the form

$$\int \frac{\text{polynomial}}{\sqrt{\text{cubic with three distict roots}}}dx$$

Because this integral arose from the ellipse arclength problem, this was dubbed the name elliptic integrals.

The denominators made to look at the curve

$$y = \sqrt{\text{cubic with three distict roots}}$$

Square both sides, and get elliptic curves.

Elliptic Curve

- Let K be a field. K may be either R, Q, C, or F_q, $q = p^r$.
- Definition: Let K be a field of characteristic $\neq 2, 3$, and let $x^3 + ax + b$ (where $a, b \in K$) a cubic polynomial with no multiple roots. An elliptic curve over K is an equation

$$y^2 = x^3 + ax + b$$

where $a, b \in K$ satisfy $\Delta = 4a^3 + 27b^2 \neq 0$.

The condition $\Delta \neq 0$ ensures that the equation

$x^3 + ax + b = 0$ does not have a double root.

- The set $E(K)$ consists of all points (x, y), $x \in K$, $y \in K$, which satisfy the equation of the elliptic curve E over K, together with O (point at infinity).

Elliptic curve over field K

- General form of elliptic curve over field K (Weierstrass equation) is

  $E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$

  where $a_1, a_2, a_3, a_4, a_6 \in K$ and $\Delta \neq 0$, where Δ is the discriminant of E and is defined as follows:

  $\Delta = -d_2^2 d_8 - 8d_4^3 - 27d_6^2 + 9d_2 d_4 d_6$

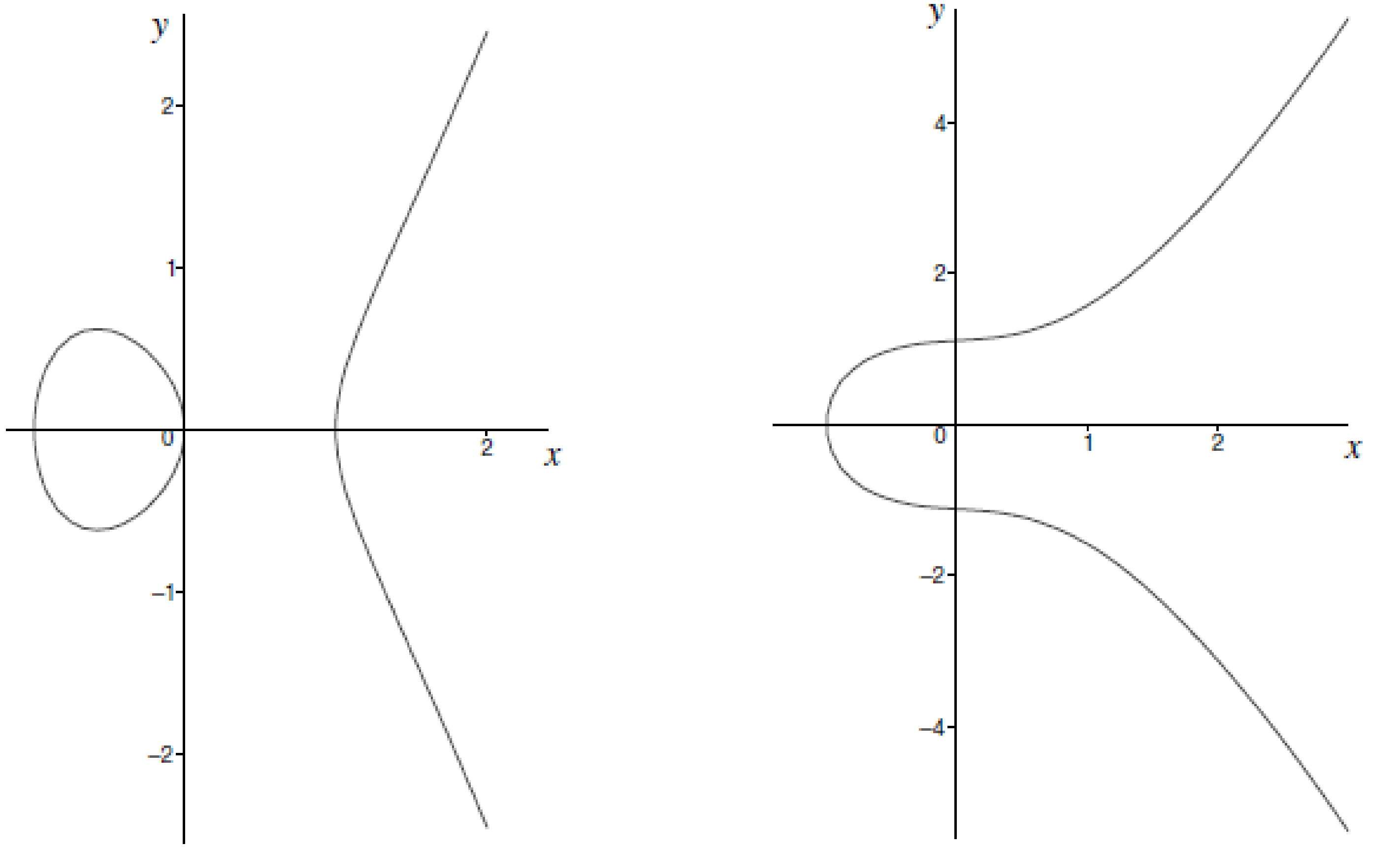
  $d_2 = a_1^2 + 4a_2$

  $d_4 = 2a_4 + a_1a_3$

  $d_6 = a_3^2 + 4a_6$

  $d_8 = a_1^2 a_6 + 4a_2 a_6 - a_1 a_3 a_4 + a_2 a_3^2 - a_4^2.$

Example: Elliptic Curves over reals i.e. $K = R$

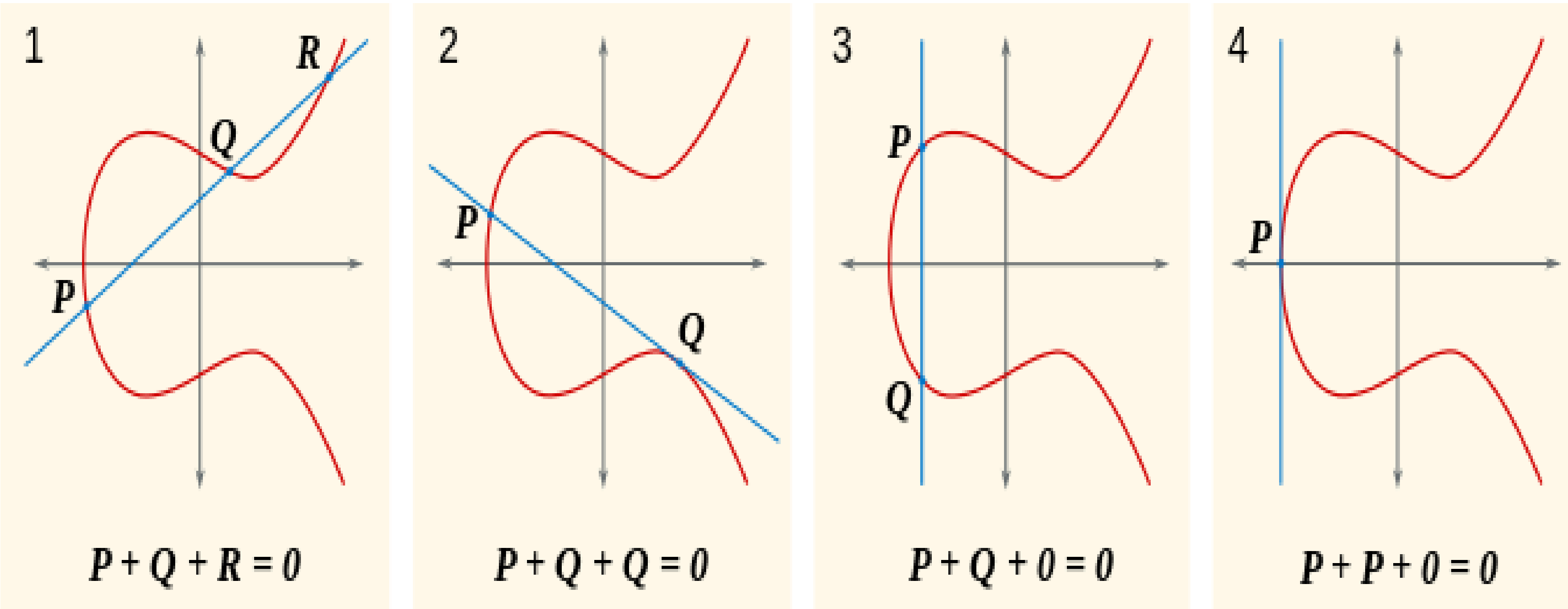


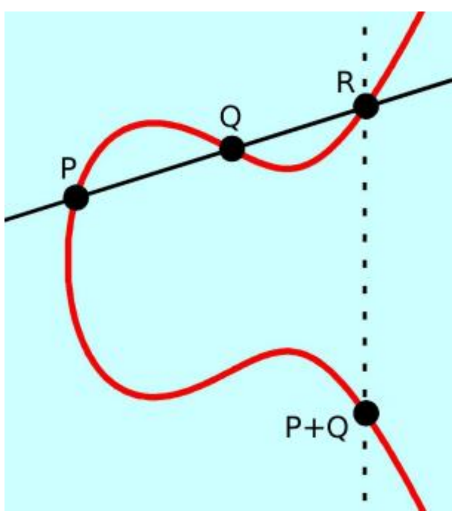
(a) $E_1 : y^2 = x^3 - x$

(b) $E_2 : y^2 = x^3 + \frac{1}{4}x + \frac{5}{4}$

- A rational point is one where both coordinates are rational, such as (1/2, 1/3), but not (1, √2).

Addition of two points on elliptic curve





Group law for $E(K) : y^2 = x^3 + ax + b$, char$(K) \neq 2,3$

- Identity: $P + O = O + P = P$ for all $P \in E(K)$
- Inverse: If $P = (x, y) \in E(K)$, then $(x, y) + (x, -y) = O$. The point $(x, -y)$ is denoted by $-P$ and is called the *negative* of P; $-P$ is a point in $E(K)$. Also, $-O = O$.
- Point addition: Let $P = (x_1, y_1) \in E(K)$ and $Q = (x_2, y_2) \in E(K)$, where $P \neq \pm Q$. Then $P + Q = (x_3, y_3)$, where

$$x_3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - x_1 - x_2 \;\;\&\;\; y_3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)(x_1 - x_3) - y_1$$

Point doubling:

$$x_3 = \left(\frac{3x_1^2 + a}{2y_1}\right)^2 - 2x_1 \;\;\&\;\; y_3 = \left(\frac{3x_1^2 + a}{2y_1}\right)(x_1 - x_3) - y_1$$

- Associativity: '+' operation is associative i.e. $(P + Q) + R = P + (Q + R)$

Hence $(E(K)$, '+'$)$ is a group.

Example: On the elliptic curve E: $y^2 = x^3 - 36x$, let P = (-3, 9) and Q = (-2, 8). Find P + Q and 2P.

Here $x_1 = -3$, $y_1 = 9$, $x_2 = -2$, $y_2 = 8$

$$x_3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - x_1 - x_2 \quad \& \quad y_3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)(x_1 - x_3) - y_1$$

$\Rightarrow x_3 = 6, y_3 = 0 \qquad \therefore$ P + Q = (6, 0)

For 2P

$$x_3 = \left(\frac{3x_1^2 + a}{2y_1}\right)^2 - 2x_1 \quad \& \quad y_3 = \left(\frac{3x_1^2 + a}{2y_1}\right)(x_1 - x_3) - y_1$$

$x_3 = 25/4$, $y_3 = -35/8 \quad \therefore$ 2P = (25/4, -35/8)

Elliptic curves over finite fields

- Definition: Let $p > 3$ be a prime. An elliptic curve E defined over F_p is an equation

$$y^2 = x^3 + ax + b$$

where $a, b \in K$ satisfy $4a^3 + 27b^2 \neq 0$.

The condition $\Delta \neq 0$ ensures that the equation $x^3 + a_2 x^2 + a_4 x + a_6 = 0$ does not have a double root.

- The curve includes an additional special point O called the point at infinity.

Number of points on elliptic curve

- Hasse's Theorem. Let N be the number of points on an elliptic curve E defined over F_q. Then
$$|N - (q + 1)| \leq 2\sqrt{q}$$
- The number of points of a curve grows roughly as the number of elements in the field. The exact number of such points is, however, rather difficult to calculate.

  Reference: Silverman, J.: The Arithmetic of Elliptic Curves, Graduate Texts in Mathematics, Springer-Verlag, Berlin Heidelberg New York

Example: Let E be the curve $y^2 = x^3 + x + 1$ over F_5.

The points lying on $E(F_5)$ are (0, 1), (0, 4), (2, 1), (2, 4), (3, 1), (3, 4), (4, 2), (4, 3), O

Discrete logarithm Problem on $E(F_q)$

- If E is an elliptic curve over F_q, and B is a point of E, then the discrete log problem on E (to the base B) is the problem, given a point $P \in E$, of finding an integer $x \in Z$ such that $xB = P$ if such an integer x exists.
- No efficient algorithm to compute discrete logarithm problem for elliptic curves is known and also no good general attacks.
- kP can be in $O(\log k)$ steps by the usual Double-and-Add Method.
  - First write

    $$k = k_0 + k_1 \cdot 2 + k_2 \cdot 2^2 + \ldots + k_r \cdot 2^r \text{ with } k_0, \ldots, k_r \in \{0, 1\}.$$

  - Then kP can be computed as

    $$kP = k_0 \cdot P + k_1 \cdot 2P + k_2 \cdot 2^2 P + \ldots + k_r \cdot 2^r P.$$

Diffie-Hellman Key Exchange Protocol

– Alice and Bob agree upon and make public two numbers α and p, where p is a prime and α is a generator of Z_p^*.

Alice		Bob
choose a random number a		
compute $u = \alpha^a \pmod{p}$	$\xrightarrow{\quad u \quad}$	u
		choose a random number b
v	$\xleftarrow{\quad v \quad}$	compute $v = \alpha^b \pmod{p}$
Compute v^a		compute u^b
i.e. $v^a = (\alpha^b)^a \pmod{p}$		$u^b = (\alpha^a)^b \pmod{p}$

The key $k = \alpha^{ab} \pmod{p}$

Elliptic curve version of the Diffie-Hellman key protocol

- Let Alice and Bob agree on a prime p, on an elliptic curve $E_p(a, b)$ and on a point P on $E_p(a, b)$.
- Alice chooses an integer x_a, computes $x_a P$ and sends it to Bob.
- Bob chooses an integer x_b, computes $x_b P$ and sends it to Alice.
- Alice computes $x_a (x_b P)$ and Bob computes $x_b (x_a P)$.

This way both have the same key.

Factorization: Pollard's p - 1 Algorithm

- Suppose n be a composite number, which is to be factored.
- Let n has a prime factor $p \leq \sqrt{n}$.
- Fermat's Little Theorem, if a is any integer, $a^{p-1} - 1 \equiv 0 \bmod p$, so $p \mid (a^{(p-1)m} - 1)$. Therefore $p \mid \gcd(a^{(p-1)m} - 1, n)$.
- Suppose that p - 1 is the product of small primes to small powers. Then k is the product of many small primes to small powers s.t. $k = (p - 1)\, m$ for some m.
- If $(p - 1) \mid k$, then $a^k \equiv 1 \bmod p$. If $(p - 1) \nmid k$, then increase k and hope that $(p - 1) \mid k$ the next time.

Elliptic Curves for Factorization

- The elliptic curve factorization method of H. Lenstra is a generalization of the so-called ($p - 1$)-factorization algorithm of Pollard.
- Using Lenstra's Algorithm, Instead of raising a random number a to a certain power k, take a multiple kP of a point $P \in E(Z_n)$.
- Order of a point $P \in E(Z_n)$ is the smallest positive integer k s.t. $kP = O$ i.e. there must be some k for which $kP = O$.
- Then the line between ($k – 1$) P and P must have undefined slope.
- This occurs when the difference of the x-values shares a common factor with n.

Algorithm: Elliptic Curves Factorization

To factorize n

- Choose random a, point $P(x_1, y_1)$ such that $1 < a; x_1, y_1 < n$.
- Let $b = y_1^2 - x^3 - ax_1 \bmod n$. Then $E: y^2 = x^3 + ax + b$ over Z_n
- Ensure that the curve is nonsingular on Z_n i.e.
  $\gcd(4a^3 + 27b^2, n) = 1$
- If it equals n, then choose a different b. If it is between 1 and n, then $\gcd(4a^3 + 27b^2, n)$ is a factor of n.
- Evaluate $k!\,P$ for $k = 2, 3, 4, \ldots$ using addition of two points.
- In general this requires $d^{-1} \bmod n$, d is denominator of slope.
- If d lacks an inverse in Z_n, then d & n must have a common divisor, which is a factor of n.

Elliptic Curves Factorization

- ECM is the third-fastest known factoring method. The second-fastest is the multiple polynomial quadratic sieve, and the fastest is the general number field sieve.
- It is sub-exponential running time, algorithm for integer factorization.
- Running time is dominated by the size of the smallest factor p rather than by the size of the number n to be factored. Time complexity: $L_p(1/2, \sqrt{2})$.
- When n is a product of two primes of roughly the same size, the expected running time of the elliptic curve algorithm is L_n [1/2, 1], which is the same as that of the quadratic sieve.