Elliptic Curves and Elliptic Curve Cryptography

OKAYAMA UNIV.

Khandaker Md. Al-Amin (PhD Student)
Secure Wireless System Lab
Information and Communication Systems
Okayama University

Outline

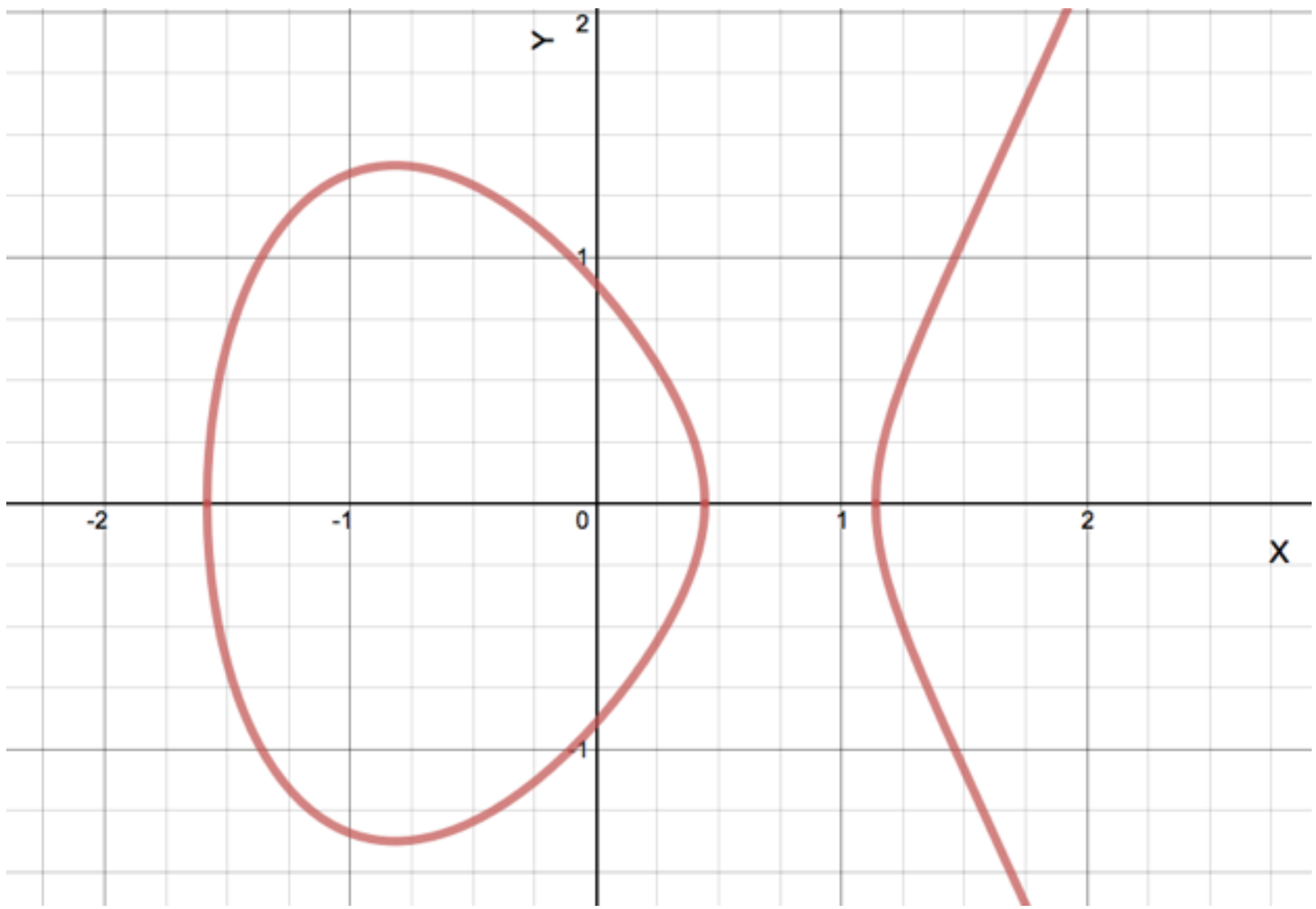
- Groups, Abelian Groups and Fields
- Elliptic Curves Over the Real Numbers
- Elliptic Curves Over a Finite Field
- Elliptic Curve Discrete Logarithm Problem

Elliptic Curves: Background

- Elliptic Curve itself is not a crypto-system.
- Elliptic curves have been extensively studied long before it is introduced in Cryptography as algebraic/ geometric entities.
- Elliptic curve was applied to cryptography in 1985. It was independently proposed by Neal Koblitz from the University of Washington, and Victor Miller, at IBM.

What is Elliptic Curve?

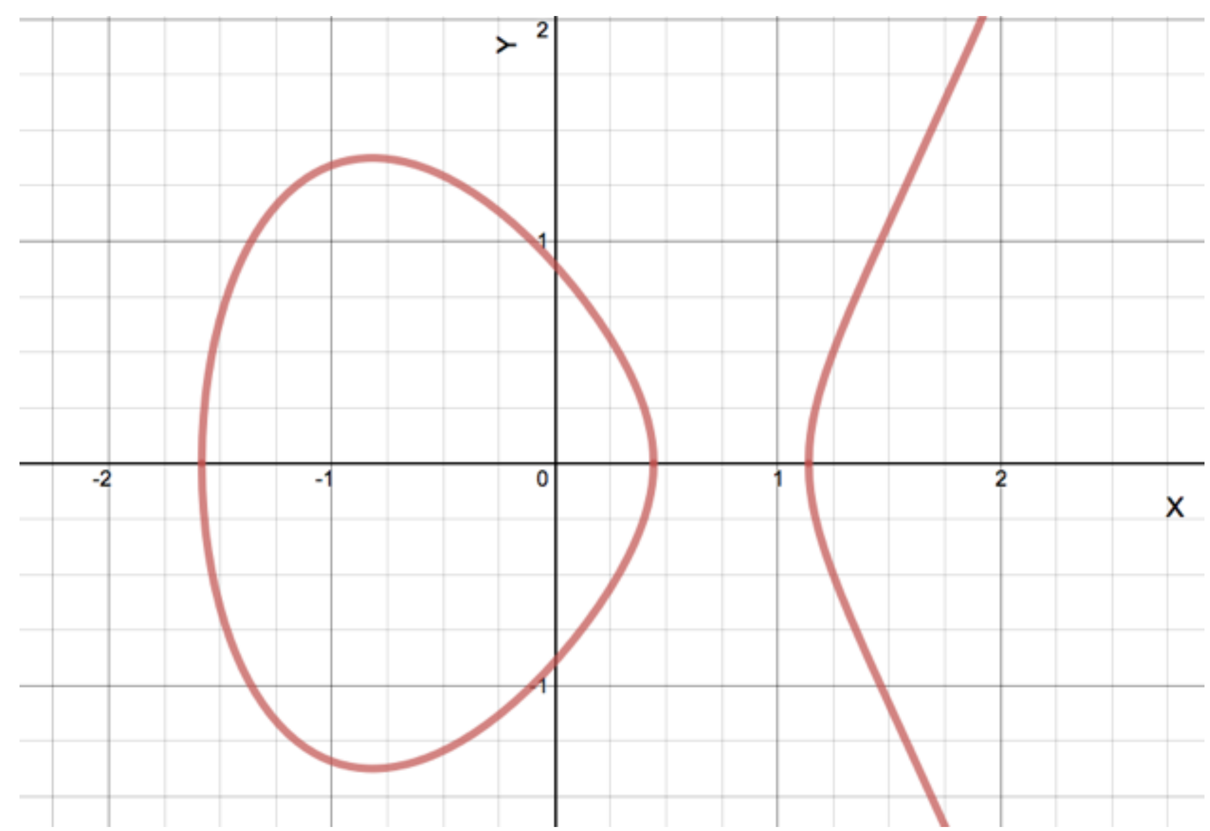
- An elliptic curve E is the graph of an equation of the form $y^2 = x^3 + ax + b$
- Also includes a "Point at infinity" denoted by 'O'.
- What do elliptic curves over Real numbers look like?



$y^2=x^3-2x+0.8$

Elliptic Curves Over the Real Numbers

- Let a and b be real numbers. An elliptic curve E over the field of real numbers R is the set of points (x,y) with x and y in R that satisfy the equation $y^2 = x^3 + ax + b$
- If the cubic polynomial x^3+ax+b has no repeated roots, we say the elliptic curve is non-singular.
- A necessary and sufficient condition for the cubic polynomial x^3+ax+b to have distinct roots is $4a^3 + 27 b^2 \neq 0$.



Group Definition

1. A group is a non-empty set G with a binary operation * that satisfies the following axioms for all a, b, c in G:
2. Closure: a*b in G
3. Associativity: (a*b)*c = a*(b*c)
4. Identity: There exists an element e in G such that a* e = a = e*a. We call e the identity element of G.
5. Inverse: For each a in G, there exists an element d in G such that a*d = e = d*a. We call d the inverse of a.
6. If a group G also satisfies the following axiom for all a, b in G:
7. Commutativity: a*b = b*a, we say G is an abelian group.
8. The order of a group G, denoted |G| is the number of elements in G. If |G| < Infinity, we say G has finite order.

Field Definition

1. A field F is a non-empty set with two binary operations, usually denoted + and *, which satisfy the following axioms for all a, b, c in F:
1. a+b is in F
2. (a+b)+c = a+(b+c)
3. a+b = b+a
4. There exists 0_F in F such that a+0_F = a = 0_F+a. We call 0_F the additive identity.
5. For each a in F, there exists an element x in F such that a+x = 0_F = x+a. We call x the additive inverse of a and write x = -a.

Field Definition (cont.)

6. Field axioms (cont.): For all a, b, c in F,
7. a*b in F
8. (a*b)*c = a*(b*c)
9. a*b = b*a
10. There exists 1_F in F, $1_F \neq 0_F$, such that for each a in F, $a*1_F = a = 1_F*a$. We call 1_F the multiplicative identity.
11. For each $a \neq 0_F$ in F, there exists an element y in F such that $a*y = 1_F = y*a$. We call y the multiplicative inverse of a and write $y = a^{-1}$.
12. a*(b+c) = a*b + a*c and (b+c)*a = b*a + c*a. (Distributive Law)

Field Examples

- Note that any field is an abelian group under + and the non-zero elements of a field form an abelian group under *.
- Some examples of fields:
- Real numbers
- Z_p, the set of integers modulo p, where p is a prime number is a finite field.
- For example,
- $Z_7 = \{0, 1, 2, 3, 4, 5, 6\}$ and $Z_{23} = \{0, 1, 2, 3, \dots, 22\}$.

An Elliptic Curve Lemma

Elliptic Curve Lemma:

Any line containing two points of a non-singular elliptic curve contains a unique third point of the curve, where

- Any vertical line contains O, the point at infinity.
- Any tangent line contains the point of tangency twice.

Geometric Addition of Elliptic Curve

- Using the Elliptic Curve Lemma, we can define a way to geometrically “add” points P and Q on a non-singular elliptic curve E.
- First, define the point at infinity to be the additive identity, i.e. for all P in E,

  $P + O = P = O + P$.
- Next, define the negative of the point at infinity to be $-O = O$.

Geometric Addition of Elliptic Curve (cont.)

- For $P = (x_P, y_P)$, define the negative of P to be $-P = (x_P, -y_P)$, the reflection of P about the x-axis.
- From the elliptic curve equation, $y^2 = x^3 + ax + b$ we see that whenever P is in E, -P is also in E.

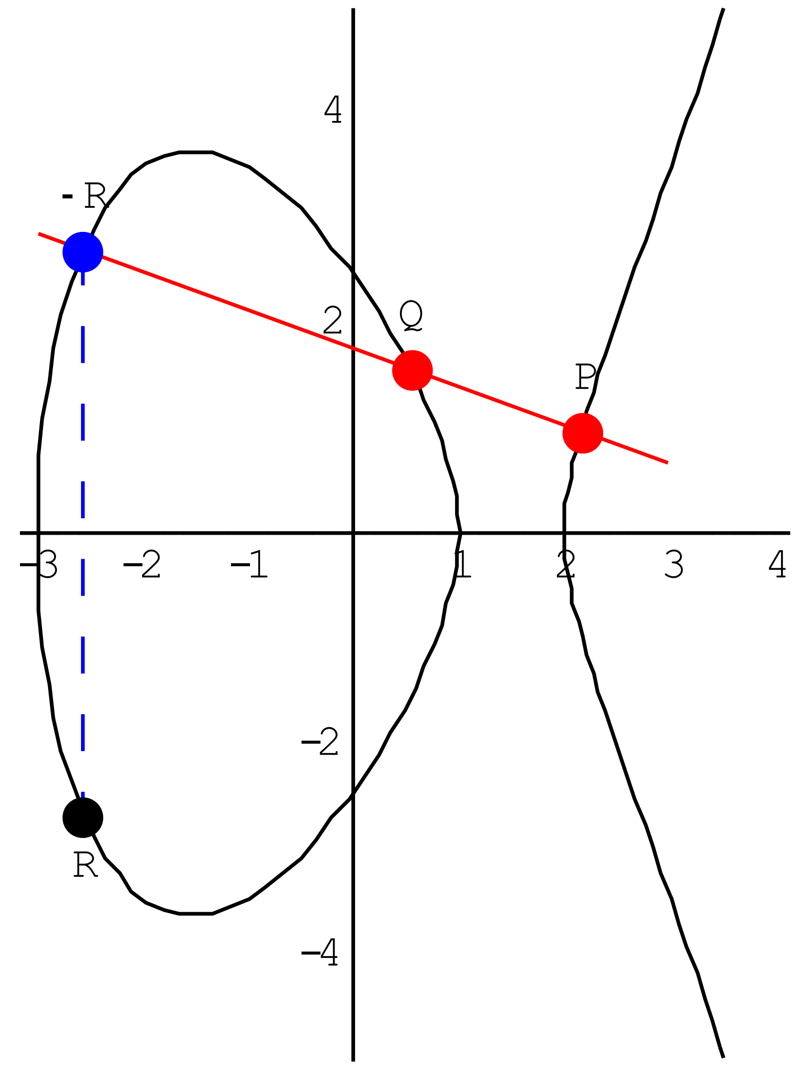
Geometric Addition of Elliptic Curve (cont.)

- Assume that neither P nor Q is the point at infinity.
- For $P = (x_P, y_P)$ and $Q = (x_Q, y_Q)$ in E, there are three cases to consider:

1. P and Q are distinct points with $x_P \neq x_Q$.
2. $Q = -P$, so $x_P = x_Q$ and $y_P = -y_Q$.
3. $Q = P$, so $x_P = x_Q$ and $y_P = y_Q$.

Geometric Case 1: $x_P \neq x_Q$

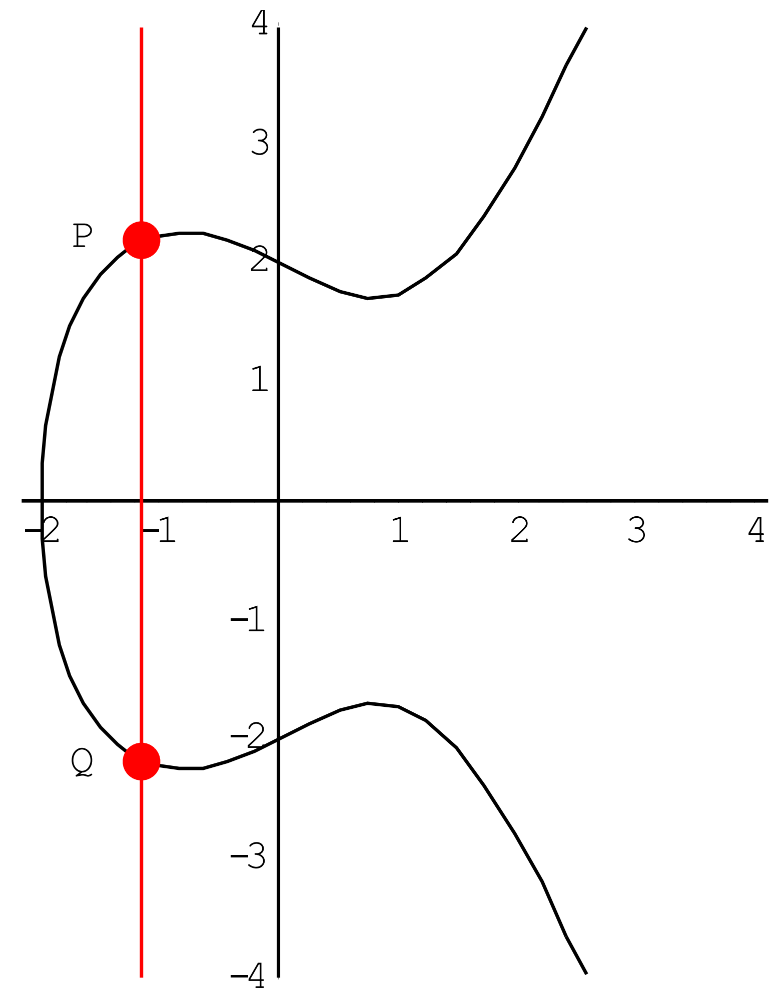
- By the Elliptic Curve Lemma, the line L through P and Q will intersect the curve at one other point.
- Call this third point -R.
- Reflect the point -R about the x-axis to point R.
- P+Q = R



$y^2 = x^3 - 7x + 6$

Geometric Case 2: $x_P = x_Q$ and $y_P = -y_Q$

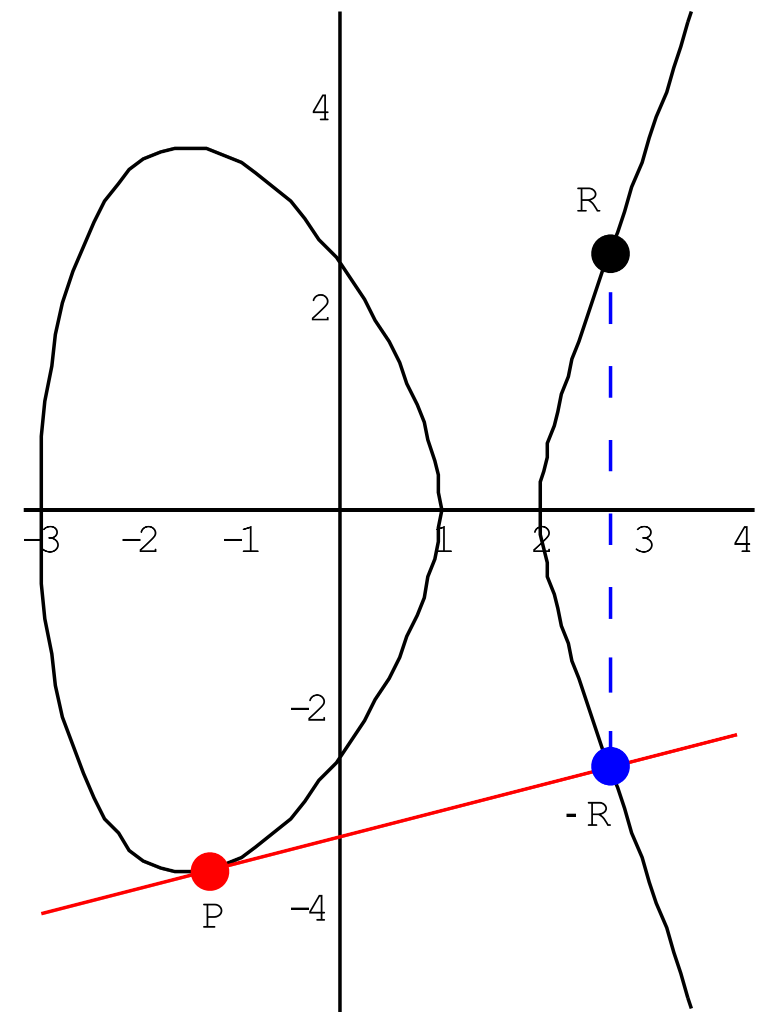
- In this case, the line L through P and $Q = -P$ is vertical.
- By the Elliptic Curve Lemma, L will also intersect the curve at O.
- $P+Q = P+(-P) = O$
- It follows that the additive inverse of P is -P.



$y^2 = x^3-2x+4$

Geometric Case 3: $x_P = x_Q$ and $y_P = y_Q$

- Since P = Q, the line L through P and Q is tangent to the curve at P.
- If $y_P = 0$, then P = -P, so we are in Case 2, and P+P = O.
- For $y_P \neq 0$, the Elliptic Curve Lemma says that L will intersect the curve at another point, -R.
- As in Case 1, reflect -R about the x-axis to point R.
- P+P = R
- Notation: 2P = P+P



$y^2 = x^3 - 7x + 6$

Algebraic Elliptic Curve Addition

- Geometric elliptic curve addition is useful for illustrating the idea of how to add points on an elliptic curve.
- Using algebra, we can make this definition more clear for implementation point of view.
- As in the geometric definition, the point at infinity is the identity, $-O = O$, and for any point P in E, $-P$ is the reflection of P about the x-axis.

Algebraic Elliptic Curve Addition (cont.)

1. In what follows, assume that neither P nor Q is the point at infinity.
2. As in the geometric case, for $P = (x_P, y_P)$ and $Q = (x_Q, y_Q)$ in E, there are three cases to consider:
   1. P and Q are distinct points with $x_P \neq x_Q$.
   2. $Q = -P$, so $x_P = x_Q$ and $y_P = -y_Q$.
   3. $Q = P$, so $x_P = x_Q$ and $y_P = y_Q$.

Algebraic Case 1: $x_P \neq x_Q$

- First we consider the case where P = (x_P,y_P) and Q = (x_Q,y_Q) with $x_P \neq x_Q$.
- The equation of the line L though P and Q is y = λ x+v, where

$$\lambda = \frac{y_Q - y_P}{x_Q - x_P} \quad \text{and} \quad \nu = y_P - \lambda x_P = y_Q - \lambda x_Q.$$

- In order to find the points of intersection of L and E, substitute λ x + v for y in the equation for E to obtain the following:

$$(\lambda x + \nu)^2 = x^3 + ax + b, \qquad (2)$$

- The roots of (2) are the x-coordinates of the three points of intersection.
- Expanding (2), we find:

Algebraic Case 1: $x_P \neq x_Q$ (cont.)

$$x^3 - \lambda^2 x^2 + (a - 2\lambda\nu)x + b - \nu^2 = 0, \qquad (3)$$

- Since a cubic equation over the real numbers has either one or three real roots, and we know that x_P and x_Q are real roots, it follows that (3) must have a third real root, x_R.
- Writing the cubic on the left-hand side of (3) in factored form

$$x^3 - \lambda^2 x^2 + (a - 2\lambda\nu)x + b - \nu^2 = (x - x_P)(x - x_Q)(x - x_R),$$

$$x_R = \lambda^2 - x_P - x_Q.$$

we can expand and equate coefficients of like terms to find

Algebraic Case 1: $x_P \neq x_Q$ (cont.)

- We still need to find the y-coordinate of the third point, $-R = (x_R, -y_R)$ on the curve E and line L.
- To do this, we can use the fact that the slope of line L is determined by the points P and -R, both of which are on L:

$$\lambda = \frac{-y_R - y_P}{x_R - x_P}.$$

- Thus, the sum of P and Q will be the point $R = (x_R, y_R)$ with

$$x_R = \lambda^2 - x_P - x_Q \quad \text{and} \quad y_R = \lambda(x_P - x_R) - y_P,$$

where

$$\lambda = \frac{y_Q - y_P}{x_Q - x_P}.$$

Algebraic Case 2: $x_P = x_Q$ and $y_P = - y_Q$

- In this case, the line L through P and Q = -P is vertical, so L contains the point at infinity.

- As in the geometric case, we define P+Q = P+(-P) = O, which makes P and -P additive inverses.

Algebraic Case 3: $x_P=x_Q$ and $y_P = y_Q$

- Finally, we need to look at the case when Q = P.
- If $y_P = 0$, then P = -P, so we are in Case 2, and P+P = O.
- Therefore, we can assume that $y_P \neq 0$.
- Since P = Q, the line L through P and Q is the line tangent to the curve at (x_P,y_P).

Algebraic Case 3: $x_P=x_Q$ and $y_P = y_Q$

- The slope of L can be found by implicitly differentiating the equation $y^2 = x^3 + ax + b$ and substituting in the coordinates of P:

$$\lambda = \frac{3x_P^2 + a}{2y_P}.$$

- Arguing as in Case 1, we find that
  P+P = 2P = R, with R = (x_R, y_R), where

$$x_R = \lambda^2 - 2x_P \text{ and } y_R = \lambda(x_P - x_R) - y_P.$$

Elliptic Curve Groups

From these definitions of addition on an elliptic curve, it follows that:

1. Addition is closed on the set E.
2. Addition is commutative.
3. *O* is the identity with respect to addition.
4. Every point P in E has an inverse with respect to addition, namely -P.
5. The associative axiom also holds.

Elliptic Curves Over Finite Fields

- Instead of choosing the field of real numbers, we can create elliptic curves over other fields.
- Let a and b be elements of Z_p for p prime, $p > 3$. An elliptic curve E over Z_p is the set of points (x,y) with x and y in Z_p that satisfy the equation

$$y^2 \pmod{p} = x^3 + ax + b \pmod{p},$$

  together with a single element O, called the point at infinity.
- As in the real case, to get a non-singular elliptic curve, we'll require $4a^3 + 27\,b^2 \pmod{p} \neq 0 \pmod{p}$.
- Elliptic curves over Z_p will consist of a finite set of points.

Addition on Elliptic Curves over Z_p

- Just as in the real case, we can define addition of points on an elliptic curve E over Z_p, for prime $p>3$.
- This is done in the essentially the same way as the real case, with appropriate modifications.

Addition on Elliptic Curves over Z_p (cont.)

- Suppose P and Q are points in E.
- Define P + O = O + P = P for all P in E.
- If Q = -P (mod p), then P+Q = O.
- Otherwise, P+Q = R = (x_R, y_R), where

$$x_R = \lambda^2 - x_P - x_Q \pmod{p} \quad \text{and} \quad y_R = \lambda(x_P - x_R) - y_P \pmod{p},$$

with

$$\lambda = \begin{cases} (y_Q - y_P)(x_Q - x_P)^{-1} \pmod{p}, & \text{if } P \neq Q \pmod{p} \\ (3x_P^2 + a)(2y_P)^{-1} \pmod{p}, & \text{if } P = Q \pmod{p}. \end{cases}$$

Cryptography on an Elliptic Curve

- Using an elliptic curve over a finite field, we can exchange information securely.
- For example, we can implement a scheme invented by Whitfield Diffie and Martin Hellman in 1976 for exchanging a secret key.

Diffie-Hellman Key Exchange via an Elliptic Curve

1. Alice and Bob publicly agree on an elliptic curve E over a finite field Z_p.
2. Next Alice and Bob choose a public base point B on the elliptic curve E.
3. Alice chooses a random integer $1<\alpha<|E|$, computes $P = \alpha B$, and sends P to Bob. Alice keeps her choice of α secret.
4. Bob chooses a random integer $1<\beta<|E|$, computes $Q = \beta B$, and sends Q to Alice. Bob keeps his choice of β secret.

1. Alice and Bob choose E to be the curve $y^2 = x^3+x+6$ over Z_7.
2. Alice and Bob choose the public base point to be $B=(2,4)$.
3. Alice chooses $\alpha = 4$, computes $P = \alpha B = 4(2,4) = (6,2)$, and sends P to Bob. Alice keeps α secret.
4. Bob chooses $\beta = 5$, computes $Q = \beta B = 5(2,4) = (1,6)$, and sends Q to Alice. Bob keeps β secret.

Diffie-Hellman Key Exchange via an Elliptic Curve (cont.)

5. Alice computes $K_A = \alpha Q = \alpha(\beta B)$.
6. Bob computes $K_B = \beta P = \beta(\alpha B)$.
7. The shared secret key is $K = K_A = K_B$.
   Even if Eve knows the base point B, or P or Q, she will not be able to figure out α or β, so K remains secret!

5. Alice computes $K_A=\alpha Q = 4(1,6) = (4,2)$.
6. Bob computes $K_B = \beta P = 5(6,2) = (4,2)$.
7. The shared secret key is $K = (4,2)$.

Elliptic Curve Discrete Logarithm Problem

- At the foundation of every crypto-system is a hard mathematical problem that is computationally infeasible to solve.
- The discrete logarithm problem is the basis for the security of many crypto-systems including the Elliptic Curve Crypto-system.
- ECC relies upon the difficulty of the Elliptic Curve Discrete Logarithm Problem (ECDLP).
- Recall that we examined two geometrically defined operations over certain elliptic curve groups. These two operations were point addition and point doubling.
- By selecting a point in a elliptic curve group, one can double it to obtain the point 2P.
- After that, one can add the point P to the point 2P to obtain the point 3P.
- The determination of a point nP in this manner is referred to as Scalar Multiplication of a point.
- The ECDLP is based upon the intractability of scalar multiplication products.

Scalar Multiplication

- Scalar Multiplication of Point in EC Additive group is a combination of point doubling and point addition.
- Under additive notation: computing kP by adding together k copies of the point P.
- If k = 23; then, kP = 23*P = 2(2(2(2P) + P) + P) + P
- Using multiplicative notation, this operation consists of multiplying together k copies of the point P, yielding the point P*P*P*P*…*P = Pk.

Elliptic Curve Discrete Logarithm Problem

- In multiplicative group $Z_p{}^*$, DLP is: given elements r and q of the group, and a prime p, find a number k such that $r = q^k \bmod p$.
- If the elliptic curve groups is described using multiplicative notation, then the elliptic curve discrete logarithm problem is: given points P and Q in the group, find a number that $P^k = Q$; k is called the discrete logarithm of Q to the base P.
- When the elliptic curve group is described using additive notation, the elliptic curve discrete logarithm problem is: given points P and Q in the group, find a number k such that [k]P = Q

Elliptic Curve Discrete Logarithm Problem

- In the elliptic curve group defined by $y^2 = x^3 + 9x + 17$ over F_{23}, What is the discrete logarithm k of $Q = (4,5)$ to the base $P = (16,5)$?
- Naive way to find k is to compute multiples of P until Q is found. The first few multiples of P are:

  $P = (16,5)$
  $2P = (20,20)$
  $3P = (14,14)$
  $4P = (19,20)$
  $5P = (13,10)$
  $6P = (7,3)$
  $7P = (8,7)$
  $8P = (12,17)$
  $9P = (4,5)$
- Since $9P = (4,5) = Q$, the discrete logarithm of Q to the base P is $k = 9$.
- In a real application, k would be large enough (e.g. 192bit) such that it would be infeasible to determine k in this manner.

ElGamal Cryptography

- Public-key crypto-system related to D-H
- Uses exponentiation in a finite field
- With security based difficulty of computing discrete logarithms, as in D-H.
- Each user generates their key
- Chooses a secret key (number): $1 < x_A < q-1$
- Compute their public key: $y_A = a^{x_A} \bmod q$

ElGamal Message Exchange

1. Bob encrypts a message to send to Alice computing
    1. Represent message M in range 0 <= M <= q-1
    2. chose random integer k with 1 <= k <= q-1
    3. compute one-time key K = y_A^k mod q
    4. Encrypt M as a pair of integers (C1,C2) where C1 = a^k mod q ; C2 = KM mod q.
2. Alice then recovers message by
    1. Recovering key K as K = C1^xA mod q
    2. computing M as M = C2 K ^-1 mod q
3. A unique k must be used each time otherwise result is insecure

ElGamal Example

1. Let's us consider field GF(19) q=19 and a=10
2. Alice computes her key:
    1. Chooses x_A= 5 & computes y_A=10^5 mod 19 = 3
3. Bob send message m=17 as (11,5) by
    1. choosing random k=6
    2. computing K = y_A^k mod q = 3^6 mod 19 = 7
    3. computing C1 = ak mod q = 10^6 mod 19 = 11;
    4. C2 = KM mod q = 7.17 mod 19 = 5
4. Alice recovers original message by computing:
    1. recover K = C1^x_A mod q = 11^5 mod 19 = 7
    2. compute inverse K^-1 = 7^-1 = 11
    3. recover M = C2 K^-1 mod q = 5.11 mod 19 = 17

ElGamal With Elliptic Curve

- Set up an elliptic curve E over a field $\mathbb{F}q$ and a point P of order N.
- We need a public function $f{:}m \mapsto Pm$, which maps messages m to points Pm on E. It should be invertible, and one way is to use m in the curve's equation as x and calculate the according y
- Choose a secret key $x \in [1, N-1]$ randomly, publish the point $Y=[x]P$ as public key.
- Encryption: choose random $k \in [1,N-1]$,then calculate $C1 = [k]P$ and $C2 = kY$ and calculate $Pm = f(m)$. The cipher text is the tuple $(C1,C2+Pm)$.
- Decryption: From a cipher text (C,D), calculate $C'=[x]C$ and retrieve the point Pm with $Pm=D-C'=(k([x]P)+Pm)-(x(kP))$.
- Then calculate the message m with f^-1(Pm).

Thank you