BCT 2314: CRYPTOGRAPHY AND COMPUTER SECURITY

Course Outline

1. Traditional and Modern cryptography and ciphers
2. Security in computing

- Encryption
- Decryption
- Public key cryptography

3. Security in computing environments

- Encryption
- Protocols
- Security programs

4. Operating systems, networks and communication

- Legal, Ethical and Human factors in computer security

Course Outline

1. **Introduction**
2. **Security in computing**

- Block Ciphers and Data Encryption Standards
- Block Cipher Standards
- The Data Encryption Standards
  - The DES Strength
- 3DES
- Differential and Linear Cryptanalysis
- Block Cipher Design Principles
- Advanced Encryption Standard
- Block Cipher Modes of operation
  - Electronic Code Block (ECB), Cipher Block Chaining (CBC), Cipher Feedback (CFB), Output Feedback (OFB), Counter (CTR)

3. **Public Key Cryptography**

- Elliptic Curve Arithmetic, Elliptic Curve Cryptography

4. **Message Authentication and Hash Functions**

- Message Authentication Codes (Covered)
- Hash Functions, Security of Hash Functions
- Secure Hash Algorithms i.e. SHA

5. **System and Network Security**

- Intruders, Malicious Software
- Port Scanning, Spoofs, Spam, DoS, Firewalls

6. **Legal, Ethical and Human factors in computer security**

Elliptic Curve Cryptography

Lecture Outline

Public Key Cryptography

- Elliptic Curve Arithmetic
- Elliptic Curve Cryptography
- Elliptic Curves over Real Numbers
- Elliptic Curves over $GF(p) = \mathbb{Z}_p$
- Elliptic Curve Cryptography Simulating ElGamal

ELLIPTIC CURVE CRYPTOSYSTEMS

- Proposed by Neal Koblitz and Victor Miller in 1985
- ECC was standardized by a number of organizations and it started receiving commercial acceptance in the late 1990`s.
- Mainly used in the resource constrained environments, such as ad-hoc wireless networks and mobile networks.
- As computational power evolves, the key size of the conventional systems is required to be increased dramatically.

ELLIPTIC CURVE CRYPTOSYSTEMS

- Elliptic curves have been studied by mathematicians for over a hundred years and have been deployed in diverse areas

Number theory: proving Fermat`s Last Theorem in 1995

- The equation $x^n + y^n = n^n$ has no nonzero integer solutions for x, y, z when the integer n is greater than 2.

Modern physics: String theory

- The notion of a point-like particle is replaced by a curve-like string.

Elliptic Curve Cryptography

- An efficient public key cryptographic system.

ELLIPTIC CURVE CRYPTOSYSTEMS

- Researchers have looked for alternatives that give the same level of security with smaller key sizes. One of these promising alternatives is the elliptic curve cryptosystem (ECC).
- However, the confidence level in ECC is not yet as high as that in RSA.
- ECC is fundamentally more difficult to explain than either RSA or Diffie-Hellman

ELLIPTIC CURVE CRYPTOSYSTEMS

- ECC is an approach to public key cryptography based on the algebraic structure of elliptic curves over finite fields.
- Its security is based on the possibility of efficient additive exponentiation and absence of efficient (classical) algorithms for additive logarithm.
- Two families commonly used:
  - Prime curves $E_p(a, b)$ defined over $\mathbb{Z}_p$
    - Use integers modulo a prime
    - Best in software
  - Binary curves $E_{2^m}(a, b)$ defined over $GF(2^n)$
    - Use polynomials with binary coefficients
    - Best in hardware

Number Theory Review

Abelian Group

An abelian group G, also denoted as $(G,\cdot)$, is a set of elements with a binary operation denoted $\cdot$, that associates to each ordered pair $(\mathrm{a}\cdot b)$ in G such that the following axioms are obeyed;

1. Closure: If a and b belong to G, then $\mathrm{a}\cdot b$ is also in G
2. Associative: $a\cdot(b\cdot c)=(a\cdot b)\cdot c\ \forall a,b,c\in G$
3. Identity element: There is an element $e\in G$ such that $a\cdot e=e\cdot a\ \forall a\in G$
4. Inverse element: For each $a\in G, \exists a'\in G$ such that $a\cdot a'=a'\cdot a=\mathrm{e}$
5. Commutative: $a\cdot \mathrm{b}=\mathrm{b}\cdot a\ \forall a,b\in G$

Number Theory Review

Abelian Group in ECC

- Given two points $P, Q \in in\ E(\mathbb{F}_p)$ there is a third point, denoted by $P + Q$ on $E(\mathbb{F}_p)$, and the following relations hold for all $P, Q, R \in in\ E(\mathbb{F}_p)$

1. $P + Q = Q + P$: Commutativity
2. $(P + Q) + R = P + (Q + R)$: Associativity
3. $P + O = O + P = P$: Existence of an identity element
4. There exists $(-P)$ such that $-P + P = P + (-P) = O$: Existence of inverses

Number Theory Review

- A number of public-key ciphers are based on the use of an abelian group.

Example: Diffie-Hellman key exchange involves multiplying pairs of nonzero integers

- Keys are generated by exponentiation over the group, with exponentiation defined as repeated multiplication.
- Example, $a^k mod\ q = (\underbrace{a \times a \times \cdots \times a}_{\text{k times}})\ mod\ q$
- To attack Diffie-Hellman, the attacker must determine k given a and a^k; this is the discrete logarithm problem.

Number Theory Review

- Elliptic curves are not ellipses. They are so named because they are described by cubic equations, similar to those used for calculating the circumference of an ellipse.
- In general, cubic equations for elliptic curves take the following form, known as a Weierstrass equation: $y^2 + axy = x^3 + cx^2 + dx + e$ where a, b, c, d, e are real numbers and take on values in the real numbers.
- It is sufficient to limit ourselves to equations of the form

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

- Such equations are said to be cubic, or of degree 3, because the highest exponent they contain is a 3.

Number Theory Review

- Elliptic curves are not ellipses
- An elliptic curve is defined by an equation in two variables x & y, with coefficients
- Consider a cubic elliptic curve of form

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

  where x, y, a, b are all real numbers

  also define O (point at infinity)

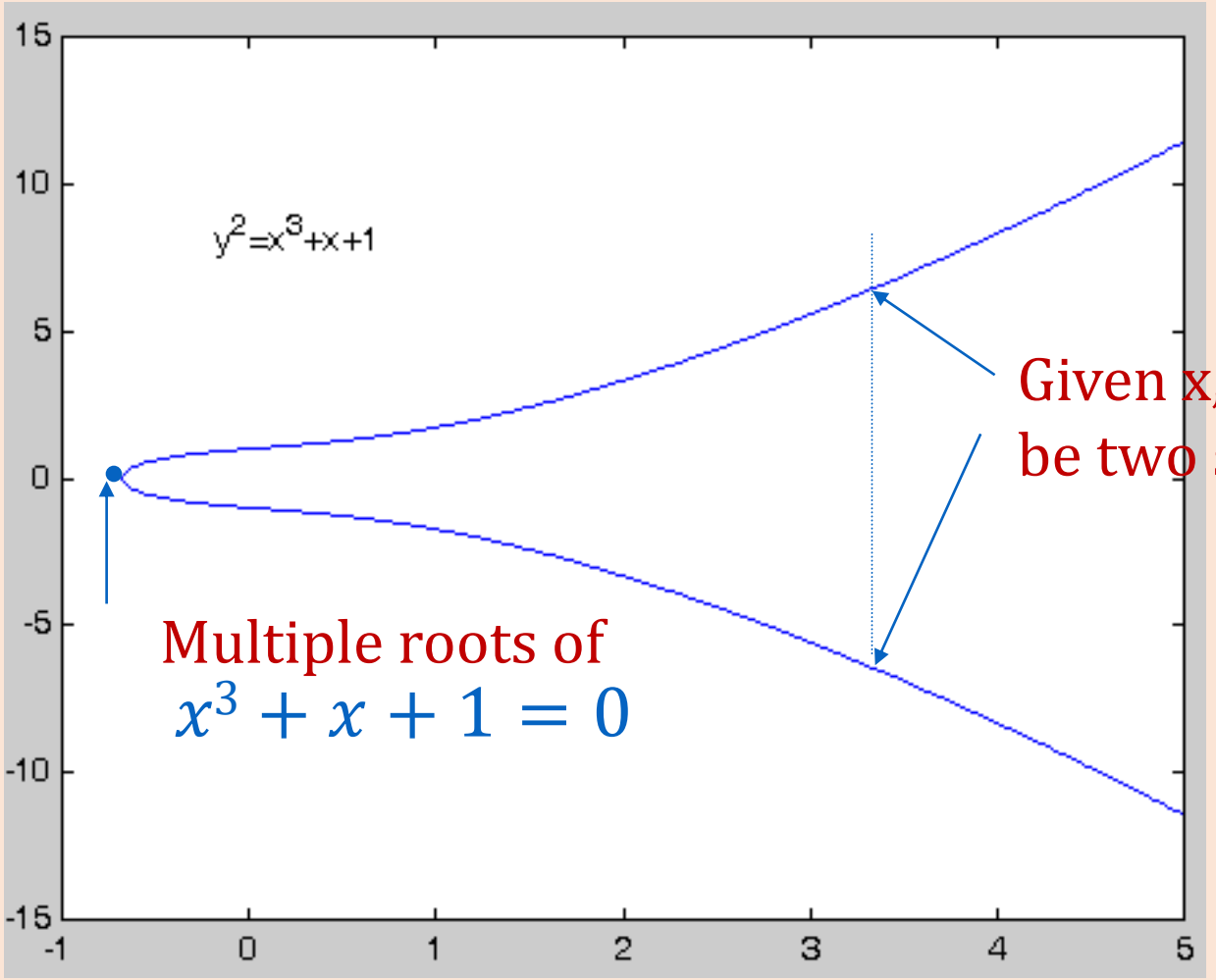
Number Theory Review

- Also included in the definition of an elliptic curve is a single element denoted *o* and called the *point at infinity or the zero point*.
- To plot such a curve, we need to compute

$$y = \sqrt{x^3 + ax + b}$$

Number Theory Review

- Example



Elliptic Curve Picture

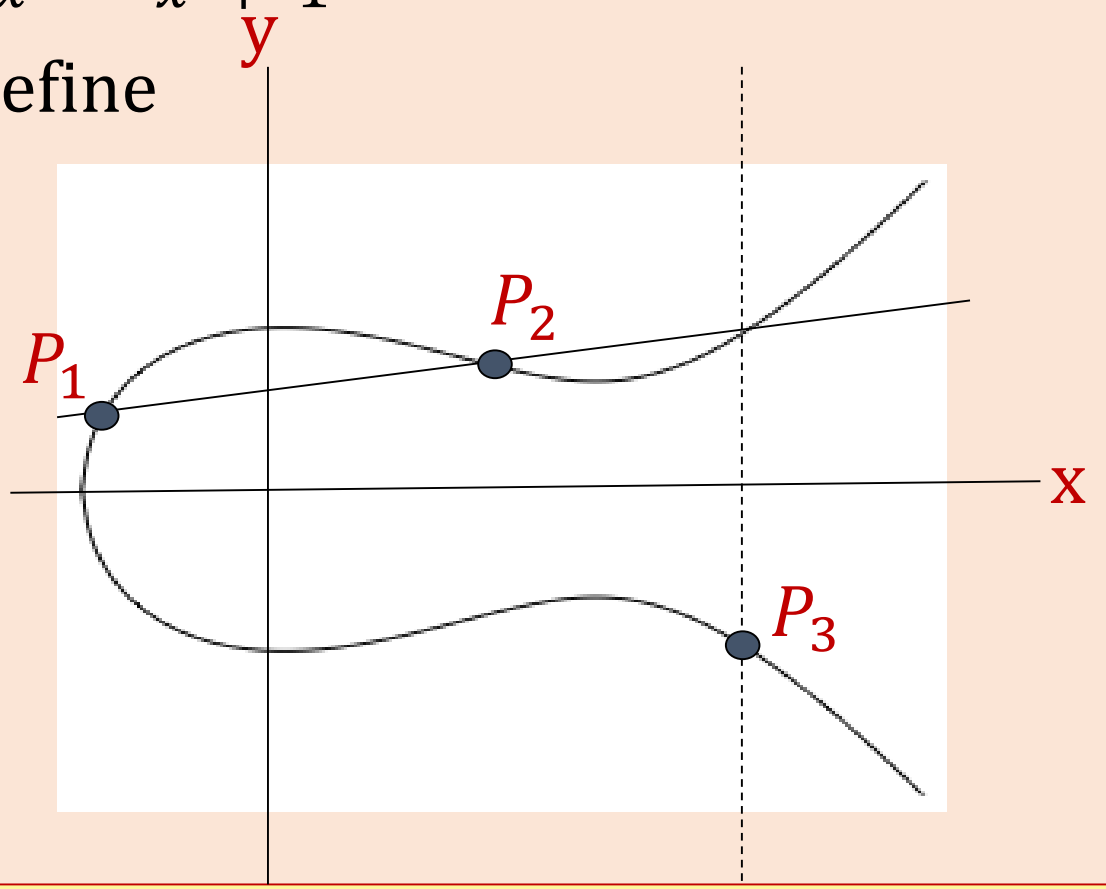
- Consider elliptic curve

$$E: \; y^2 = x^3 - x + 1$$

- If P_1 and P_2 are on E, we can define

$$P_3 = P_1 + P_2$$

Addition is all we need



Number Theory Review

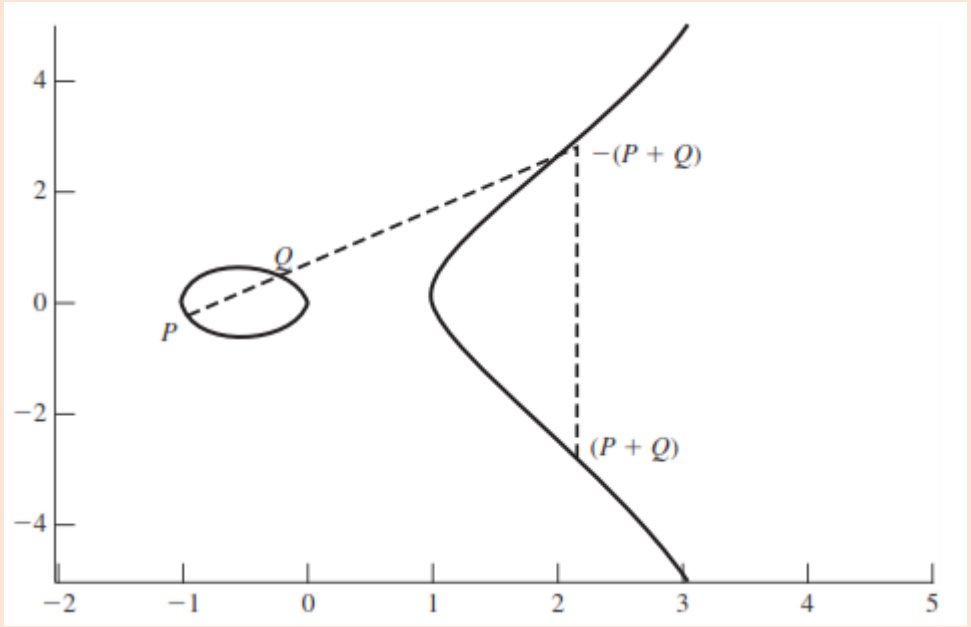
- For given values of a and b, the plot consists of positive and negative values of y for each value of x.
- Thus, each curve is symmetric about $y = 0$.

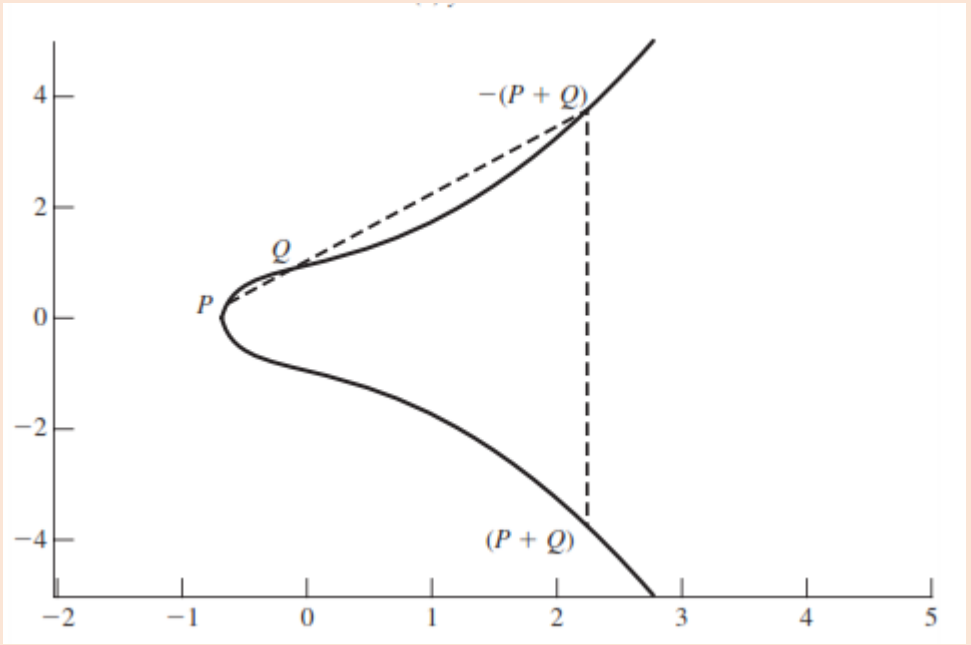
Number Theory Review

- Now, consider the set of points $E(a,b)$ consisting of all of the points (x, y) that satisfy equation $y^2 = x^3 + ax + b$ together with the element 0 .
- Using a different value of the pair (a,b) results in a different set $E(a,b)$.
- Using this terminology, the two curves below depict the sets $E(-1,0)$ and $E(1,1)$, respectively.

Number Theory Review

Examples of Elliptic Curves





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

$$y^2 = x^3 + x + 1$$

GEOMETRIC DESCRIPTION OF ADDITION

- A group can be defined based on the set $E(a, b)$ for specific values of a and b in equation $y^2 = x^3 + bx + b$, provided the following condition is met:

$$4a^3 + 27b^2 \neq 0$$

- To define the group, we define an operation, called addition and denoted by $+$, for the set $E(a, b)$, where a and b satisfy Equation $4a^3 + 27b^2 \neq 0$.

GEOMETRIC DESCRIPTION OF ADDITION

If three points on an elliptic curve lie on a straight line, their sum is 0. From this definition, we can define the rules of addition over an elliptic curve as follows .

1. 0 serves as the additive identity. Thus $0 = -0$; for any point on the elliptic curve, $P + 0 = P$. Henceforth, we assume $P \neq 0$ and $Q \neq 0$

If P is the point at infinity O, then –P=O and P+Q = Q. [i.e. O servers as the identity (zero)]

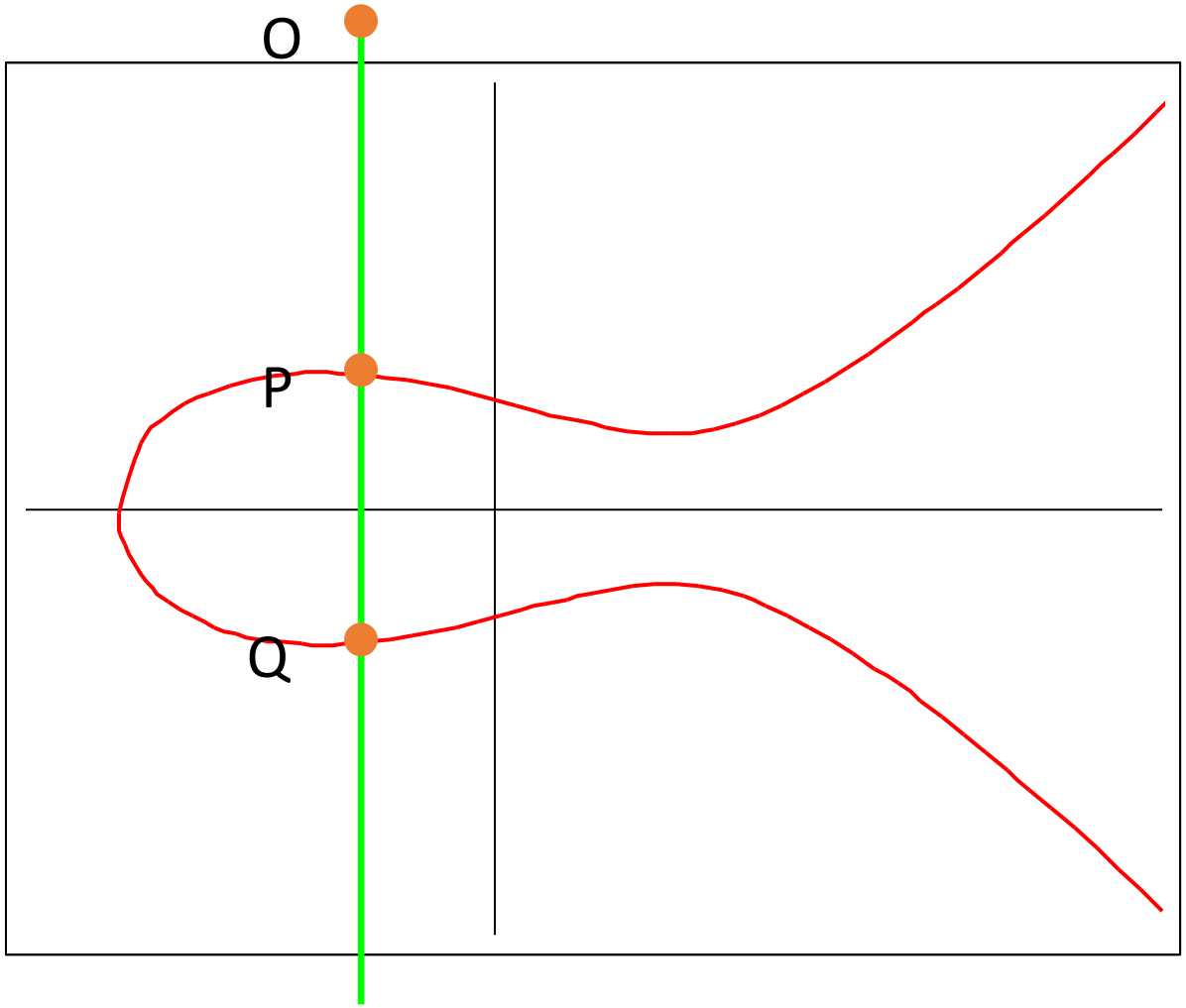
GEOMETRIC DESCRIPTION OF ADDITION

In geometric terms, the rules for addition can be stated as follows:

2. The negative of a point P is the point with the same x coordinate but the negative of the y coordinate; that is, if $P = (x, y)$, then $-P = (x, -y)$.Note that these two points can be joined by a vertical line. Note that $P + (-P) = P - P = 0$

$P = (x, y)$ then $-P = (x, -y)$.[$-P$ must lie on elliptic curve]

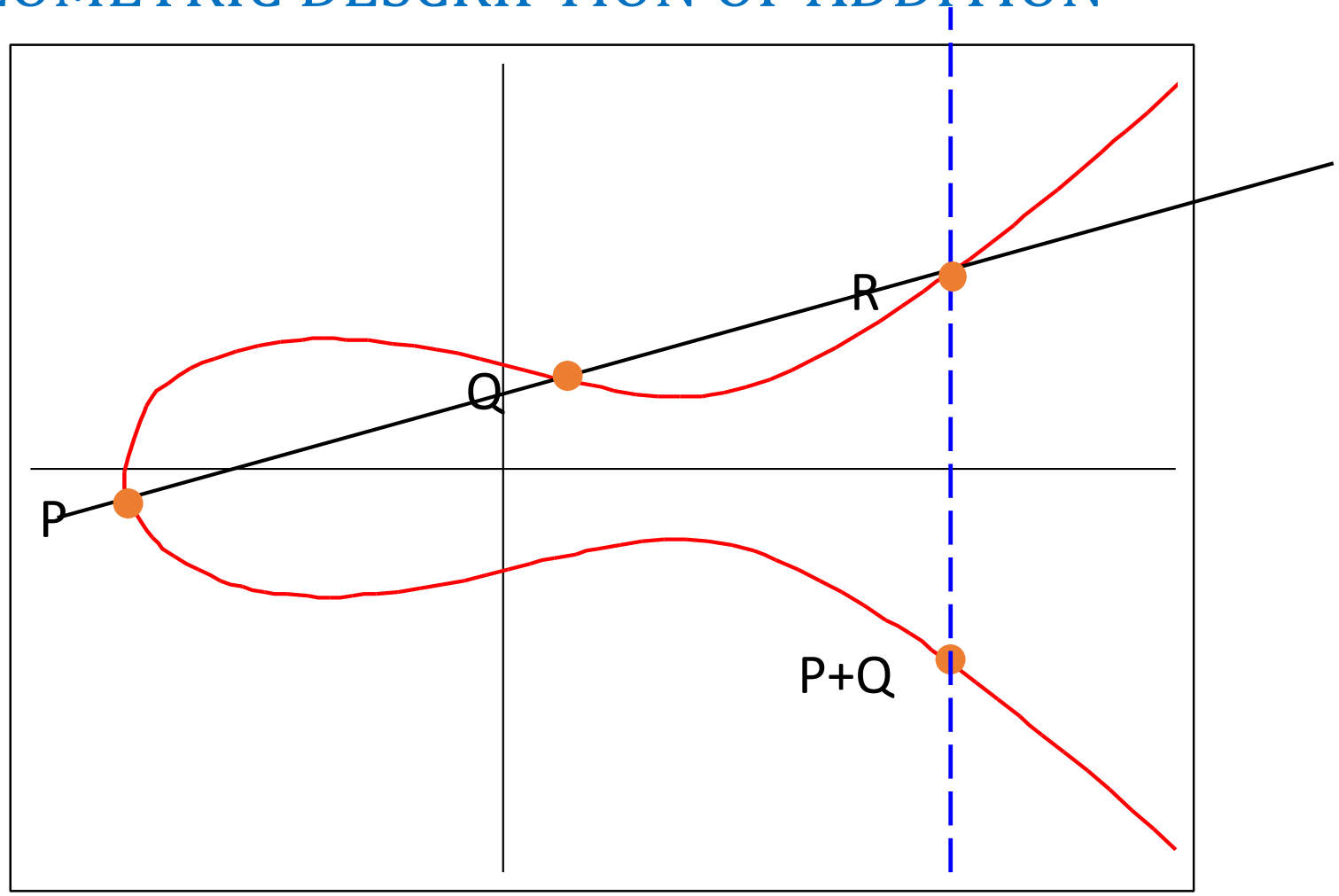
GEOMETRIC DESCRIPTION OF ADDITION



GEOMETRIC DESCRIPTION OF ADDITION

3. To add two points P and Q with different x coordinates, draw a straight line between them and find the third point of intersection R .
   - There is a unique R point that is the point of intersection (unless the line is tangent to the curve at either P or Q, in which case we take $\mathrm{R} = P$ or $\mathrm{R} = \mathrm{Q}$, respectively).
   - To form a group structure, we need to define addition on these three points: $P + Q = -R$. That is, we define $P + Q$ to be the mirror image (with respect to the x axis) of the third point of intersection. Construction illustrated below.

GEOMETRIC DESCRIPTION OF ADDITION



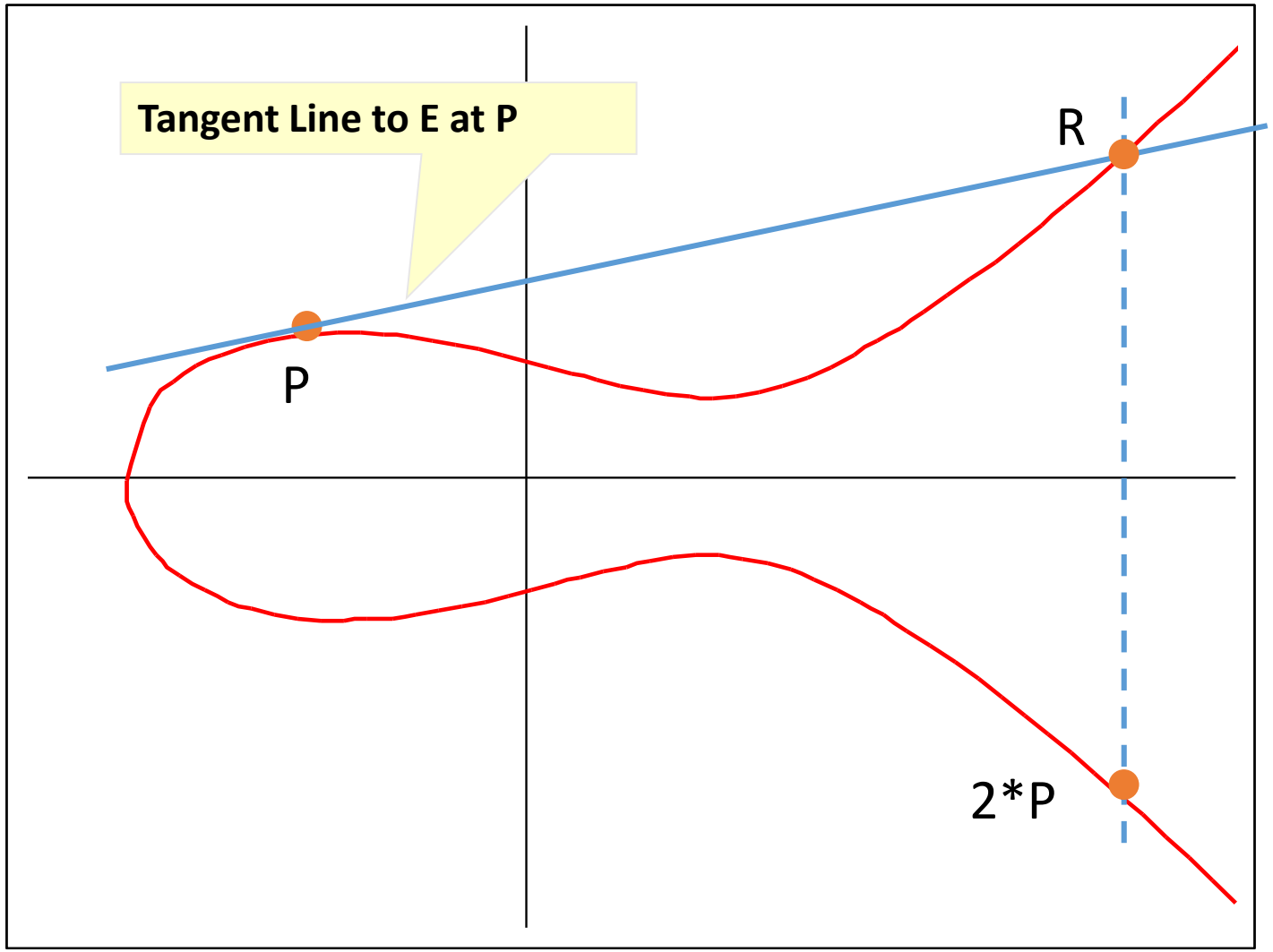
GEOMETRIC DESCRIPTION OF ADDITION

4. The geometric interpretation of the preceding item also applies to two points, P and $-P$, with the same x coordinate. The points are joined by a vertical line, which can be viewed as also intersecting the curve at the infinity point. We therefore have $P + (-P) = 0$, which is consistent with item (2).

5. To double a point Q , draw the tangent line and find the other point of intersection S. Then $Q + Q = 2Q = -S$

- With the preceding list of rules, it can be shown that the set $E(a, b)$ is an abelian group.

CURVE DOUBLING



ALGEBRAIC DESCRIPTION OF ADDITION

- For two distinct points, $P = (x_P, y_P)$ and , $Q = (x_Q, y_Q)$, that are not negatives of each other, the slope of the line l, that joins them is , $\Delta = (y_Q - y_P)/(x_Q - x_P)$.
- There is exactly one other point where l intersects the elliptic curve, and that is the negative of the sum of P and Q .
- The sum as $P + Q$,

$$x_R = \Delta^2 - x_P - x_Q$$
$$y_R = \Delta(x_P - x_R) - y_P$$

ALGEBRAIC DESCRIPTION OF ADDITION

- We also need to be able to add a point to itself: $P + P = 2P = R$. When $y_P \neq 0$, the expressions are

$$x_R = \left(\frac{3x_P^2 + a}{2y_P}\right)^2 - 2x_P$$

$$y_R = \left(\frac{3x_P^2 + a}{2y_P}\right)^2 - (x_P - x_R) - y_P$$

Elliptic Curve Cryptography

- ECC addition is analog of modulo multiply
- ECC repeated addition is analogous to modulo exponentiation
- Need "hard" problem equivalent to discrete log
  - $Q = kP$, where QP belong to a prime curve
  - Is "easy" to compute Q given k, P
  - But "hard" to find k given Q, P
  - Known as the elliptic curve logarithm problem (ECLP)

Elliptic Curves Over Real Numbers

- The generalized Weierstrass Equation for an elliptic curve is

$$y^2 + b_1xy + b_2y = x^3 + a_1x^2 + a_2x + a_3$$

- Elliptic curves over real numbers use a special class of elliptic curves of the form

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

where

$$4a^3 + 27b^2 \neq 0$$

Elliptic Curves Over Real Numbers

- Elliptic curves over real numbers use a special class of elliptic curves of the form

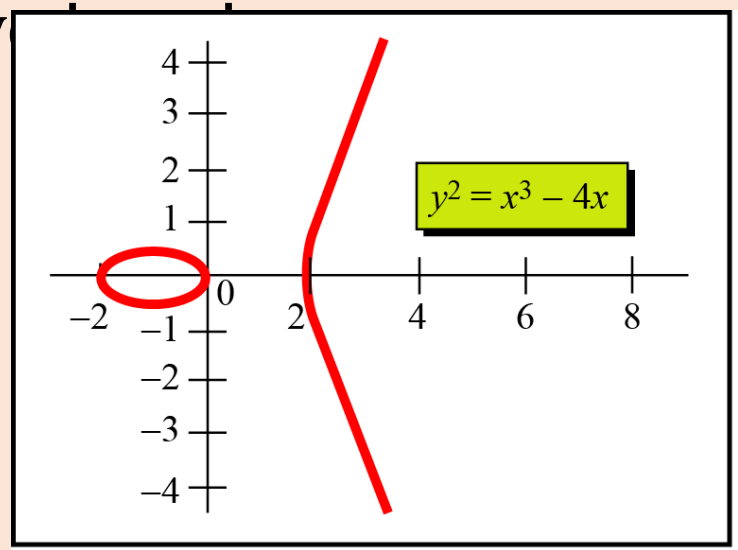
$$y^2 = x^3 + ax + b$$

- The left-hand side has a degree of 2 while the right-hand side has a degree of 3. This means that a horizontal line can intersects the curve in three points if all roots are real. However, a vertical line can intersects the curve at most in two points.

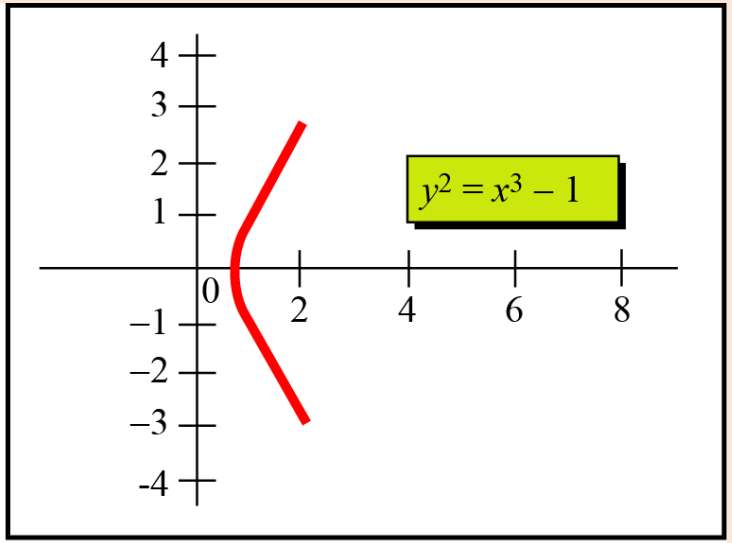
Elliptic Curves Over Real Numbers

Example

- Figure below shows two elliptic curves with equations $y^2 = x^3 - 4x$ and $y^2 = x^3 - 1$. However, the first has three real roots ($x = -2$, $x = 0$, and $x = 2$), but the second has only one real root ($x = 1$) and tw



a. Three real roots



b. One real and two imaginary roots

Elliptic Curves Over Real Numbers

An Abelian (commutative) Group

- All points on an elliptic curve. A tuple $P(x_1, y_1)$ represents a point on the curve if x_1 and y_1 are coordinates of a point on the curve that satisfy the equation of the curve.
- For example, the points $P(2,0), Q(0,0), R(-2,0), S(10,30.98)$ are all points on the curve
- Each point is represented by two real number

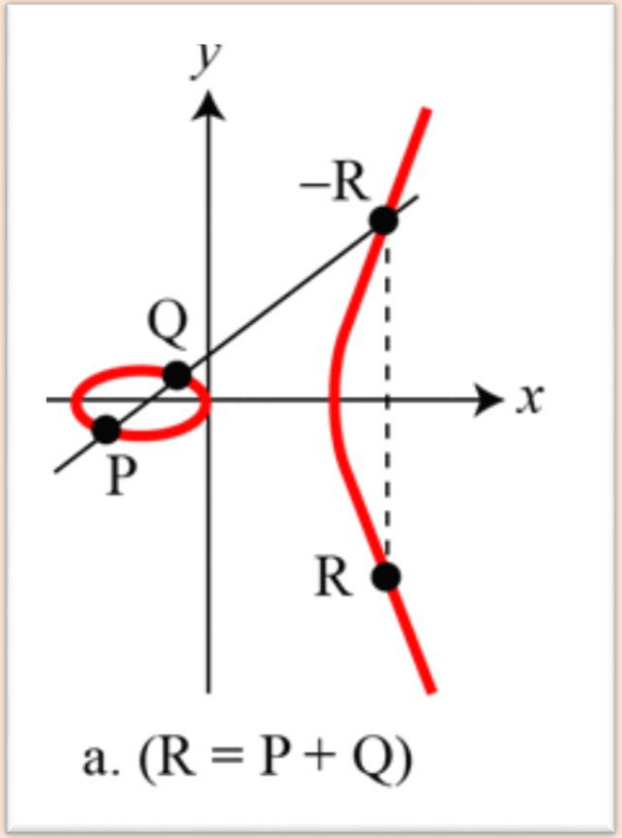
$$y^2 = x^3 - 4x$$

Elliptic Curves Over Real Numbers

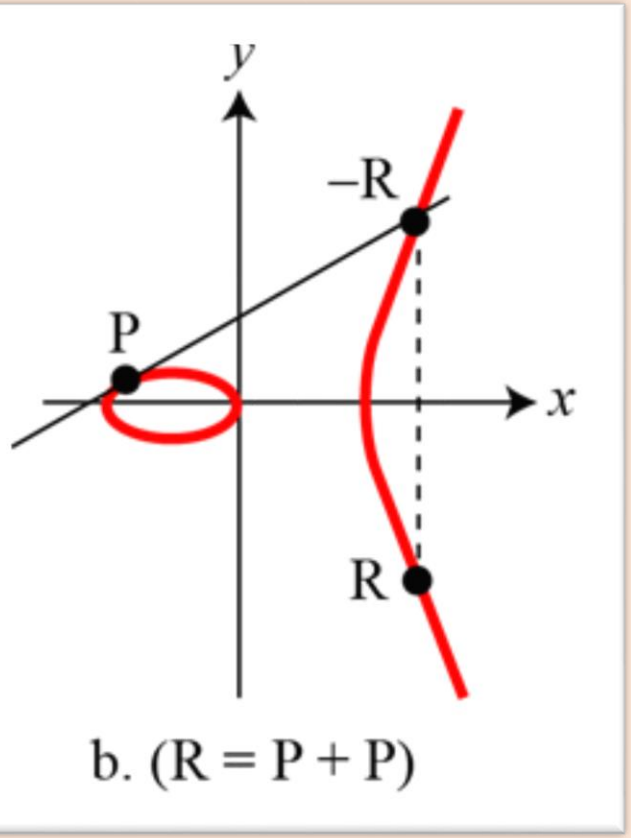
- Set
  - We define the set as the points on the curve, where each point is a pair of real numbers
    $E = \{(2, 0), (0, 0), (-2, 0), (10, 30.98)\ (10, -30.98)\}$
- Operation
  - We can define an addition operation on the points of the curve. Addition operation is different from the integer addition.

Elliptic Curves Over Real Numbers

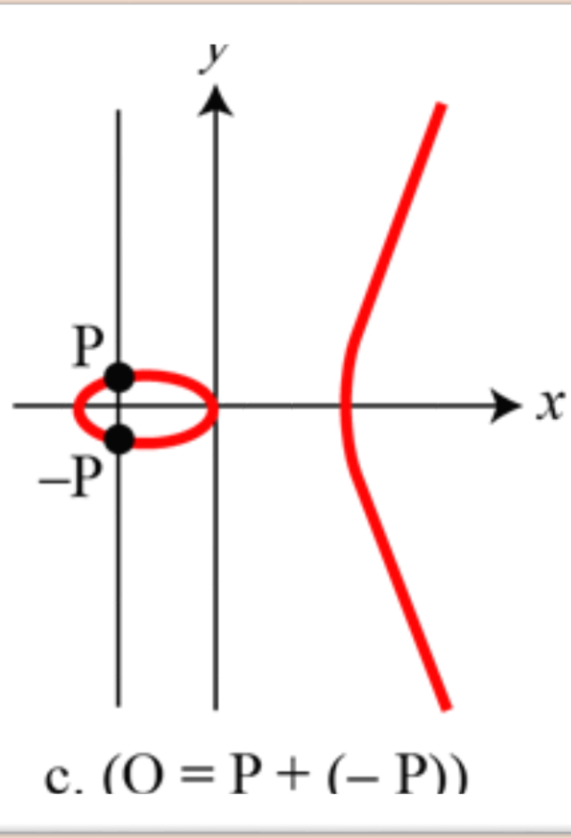
Three adding cases in an elliptic curve



a. (R = P + Q)



b. (R = P + P)



c. (O = P + (– P))

Elliptic Curves Over Real Numbers

Adding in an elliptic curve

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1}$$
$$x_3 = \lambda^2 - x_1 - x_2$$
$$y_3 = \lambda(x_1 - x_3) - y_1$$

$$\lambda = \frac{(3x_1^2 + a)}{2y_1}$$
$$x_3 = \lambda^2 - x_1 - x_2$$
$$y_3 = \lambda(x_1 - x_3) - y_1$$

The intercepting point is at infinity; a point O as the point at infinity or zero point, which is the additive identity of the group.

Elliptic Curves Over $Z_p(GF(p)$

Galois Field

- It is a finite field and it consists of a set of integers {0,1,2,3….p-1} where p is a prime number. Additionally it satisfies the following arithmetic operations :

1. **Addition :** if $a, b \in GF(p)$, then $a + b = r$ where r is the remainder of the division of $a + b$ by p and $0 \leq r \leq p - 1$. This operation is called **addition modulo** p.

2. **Multiplication** : if $a, b \in GF(p)$, then $a \,.\, b = s$ where s is the remainder of the division of $a \,.\, b$ by p and $0 \leq s \leq p - 1$.. This operation is called **multiplication modulo** p.

Elliptic Curves Over Z_p

- Elliptic curve cryptography makes use of elliptic curves in which the variables and coefficients are all restricted to elements of a finite field.
- Two families of elliptic curves are used in cryptographic applications:

1. Prime curves over Z_p
2. Binary curves over $GF(2^m)$.

- For a prime curve over Z_p , we use a cubic equation in which the variables and coefficients all take on values in the set of integers from 0 through $p-1$ and in which calculations are performed modulo p .
- For a binary curve defined over $GF(2^m)$, the variables and coefficients all take on values in $GF(2^m)$ and calculations are

Elliptic Curves Over Z_p

- Prime curves are best for software applications, because the extended bit-fiddling operations needed by binary curves are not required.
- Binary curves are best for hardware applications, where it takes remarkably few logic gates to create a powerful, fast cryptosystem.
- There is no obvious geometric interpretation of elliptic curve arithmetic over finite fields. The algebraic interpretation used for elliptic curve arithmetic over real numbers does readily carry over, and this is the approach we take.
- For elliptic curves over Z_p, as with real numbers, we limit ourselves to equations of the form of Equation $y^2 = x^3 + ax + b$ but in this case with coefficients and variables limited to : $y^2 mod\ p = (x^3 + ax + b)^2 mod\ p$

Elliptic Curves Over Z_p

Example

- For example, equation $y^2 = x^3 + ax + b$ is satisfied for $a = 1, b = 1, x = 9, y = 7, \alpha = 1, p = 23$

$$7^2 \; mod \; 23 = (9^3 + 9 + 1)^2 mod \; 23$$

$$49 \; mod \; 23 = 739 \; mod \; 23$$

$$3 = 3$$

Elliptic Curves Over Z_p

Lets consider the set consisting of all pairs of integers that satisfy equation $y^2 = x^3 + ax + b$ together with a point at infinity O.

The coefficients a and b and the variables x and y are all elements of Z_p

Elliptic Curves Over Z_p

Example 1

- Example: $E: y^2 = x^3 + x + 6$ over $\mathbb{Z}_{11}$

Find all (x, y) and O:

- Fix x and determine y
- O is an artificial point

Result =12 (x, y) pairs plus O,

and have $\#E = 13$

x	$x^3 + x + 6$	quad res?	y
0	6	*no*	
1	8	*no*	
2	5	*yes*	4,7
3	3	*yes*	5,6
4	8	*no*	
5	4	*yes*	2,9
6	8	*no*	
7	4	*yes*	2,9
8	9	*yes*	3,8
9	7	*no*	
10	4	*yes*	2,9

Elliptic Curves Over Z_p

Example 1(Cont.)

- There are 13 points on the group $E(Z_{11})$ and so any non-identity point (i.e. not the point at infinity, noted as O) is a generator of $E(Z_{11})$.
- Choose generator $\beta = (2,7)$

Compute $2\beta = (x_3, y_3)$ and have

$$\lambda = \frac{3x_1^2 + a}{2y_1} = \frac{3(2)^2 + 1}{2 \times 7} = \frac{13}{14} = 2 \times 3^{-1} = 2 \times 4 = 8 \mod 11$$

$$x_2 = \lambda^2 - 2x_1 = (8)^2 - 2 \times (2) = 5 \mod 11$$

$$y_2 = (x_1 - x_2)\lambda - y_1 = (2-5) \times 8 - 7 = 2 \mod 11$$

Elliptic Curves Over Z_p

Example 1(Cont.)

- There are 13 points on the group $E(Z_{11})$ and so any non-identity point (i.e. not the point at infinity, noted as O) is a generator of $E(Z_{11})$.

$\beta = (2,7), 2\beta = (5,2)$

Compute $3\beta = (x_3, y_3)$ and have

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1} = \frac{2-7}{5-2} = 2 \mod 11$$

$$x_3 = \lambda^2 - x_1 - x_2 = 2^2 - 2 - 5 = 8 \mod 11$$

$$y_3 = (x_1 - x_3)\lambda - y_1 = (2-8) \times 2 - 7 = 3 \mod 11$$

Elliptic Curves Over Z_p

Example 1(Cont.)

- We can therefore compute

$$\alpha = (2,7) \qquad 2\alpha = (5,2) \qquad 3\alpha = (8,3)$$

$$4\alpha = (10,2) \qquad 5\alpha = (3,6) \qquad 6\alpha = (7,9)$$

$$7\alpha = (7,2) \qquad 8\alpha = (3,5) \qquad 9\alpha = (10,9)$$

$$10\alpha = (8,8) \qquad 11\alpha = (5,9) \qquad 12\alpha = (2,4)$$

Note: E.g. Computing 9β can be achieved by $8\beta + \beta, 5\beta + 4\beta, 6\beta + 3\beta$

Elliptic Curves Over Z_p

Example 1(Cont.)

Note: E.g. Computing 9β can be achieved by

$8\beta + \beta, 5\beta + 4\beta, 6\beta + 3\beta$

Try it out!