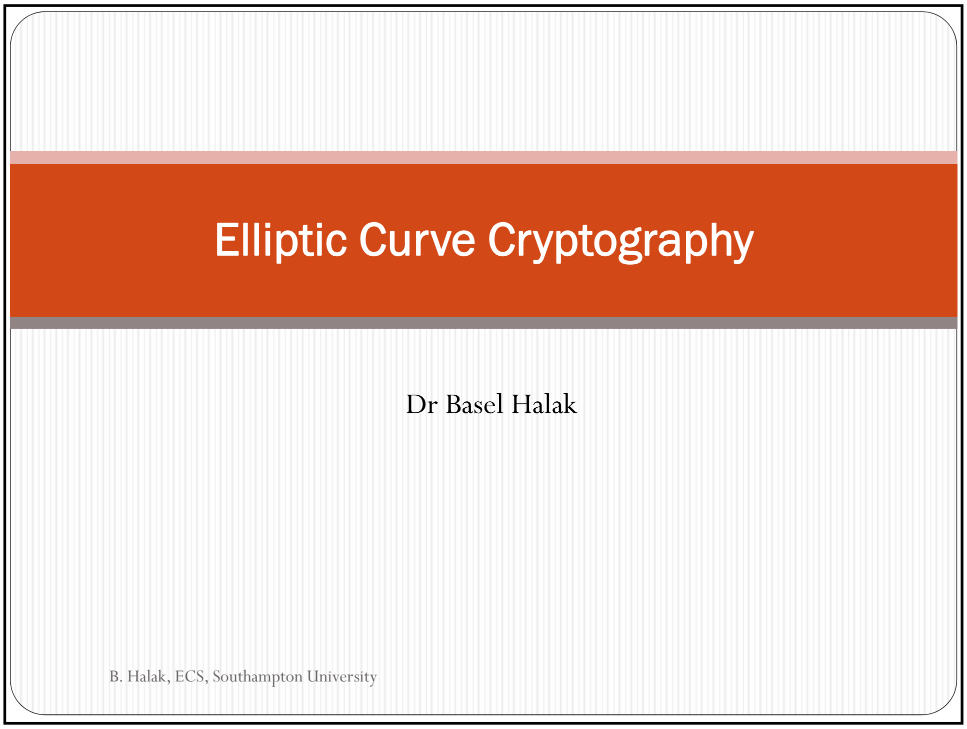
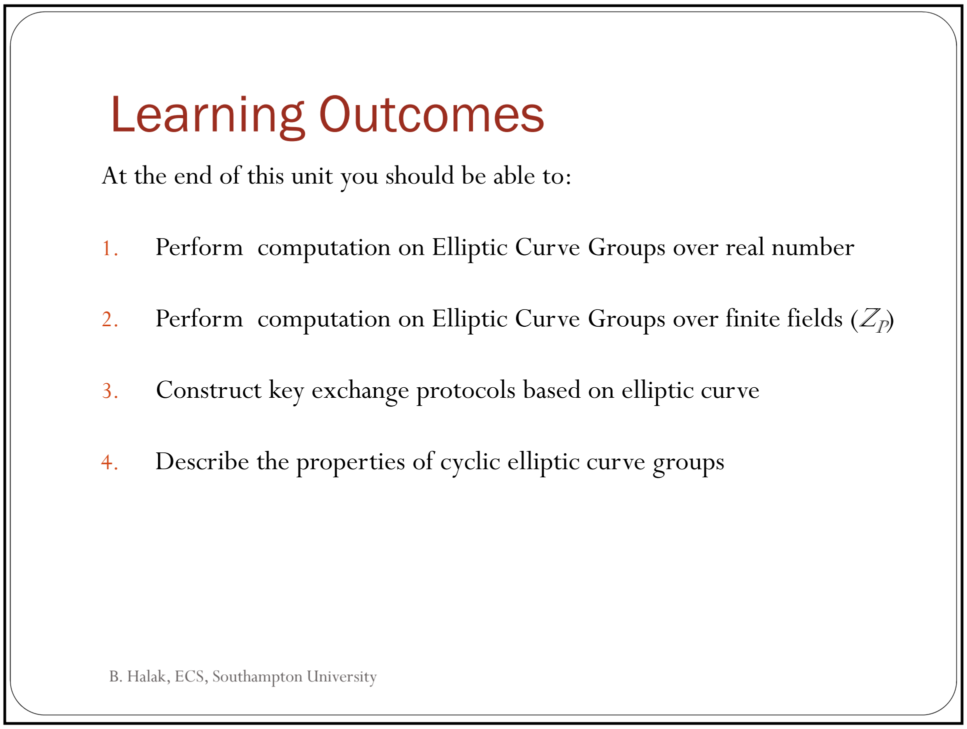


Elliptic Curve Cryptography

Dr Basel Halak



Learning Outcomes

At the end of this unit you should be able to:

1. Perform computation on Elliptic Curve Groups over real number
2. Perform computation on Elliptic Curve Groups over finite fields (Z_p)
3. Construct key exchange protocols based on elliptic curve
4. Describe the properties of cyclic elliptic curve groups

Learning Outcomes

At the end of this unit you should be able to:

1. Perform computation on Elliptic Curve Groups over real number
2. Perform computation on Elliptic Curve Groups over finite fields (Z_P)
3. Construct key exchange protocols based on elliptic curve
4. Describe the properties of cyclic elliptic curve groups

Elliptic Curves

- Elliptic curves as algebraic entities have been studied extensively for the past 150 years.
- The application of Elliptic curve systems to cryptography were first proposed in 1985 independently by Neal Koblitz from the University of Washington, and Victor Miller, who was then at IBM,Yorktown Heights.
- In the late 1990`s, ECC was standardized by a number of organizations and it started receiving commercial acceptance.
- As computational power evolves, the key's size of the conventional systems is required to be increased dramatically. There is a trend that conventional public key cryptographic systems are gradually replaced with ECC systems as the latter require smaller keys.

What is an Elliptic Curve?

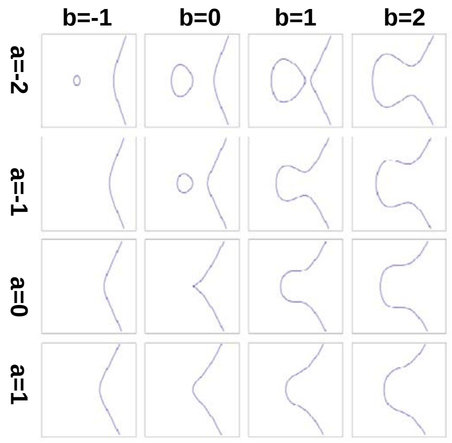
- An elliptic curve E is the graph of an equation of the form

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

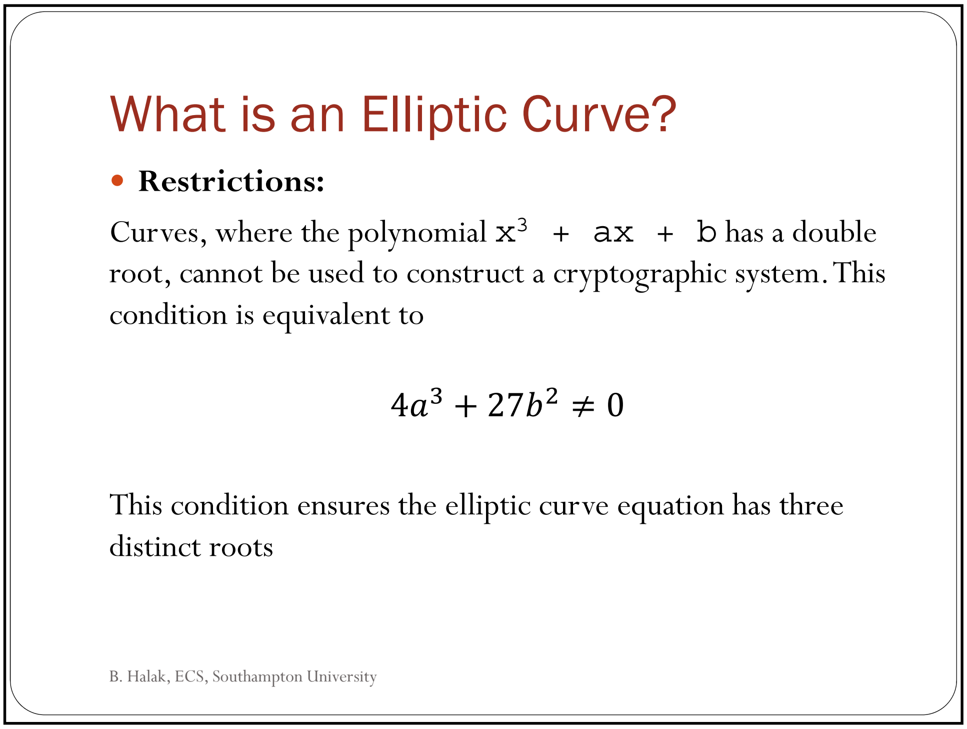
- Also includes a “point at infinity”

What is an Elliptic Curve?

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



B. Halak, ECS, Southampton University



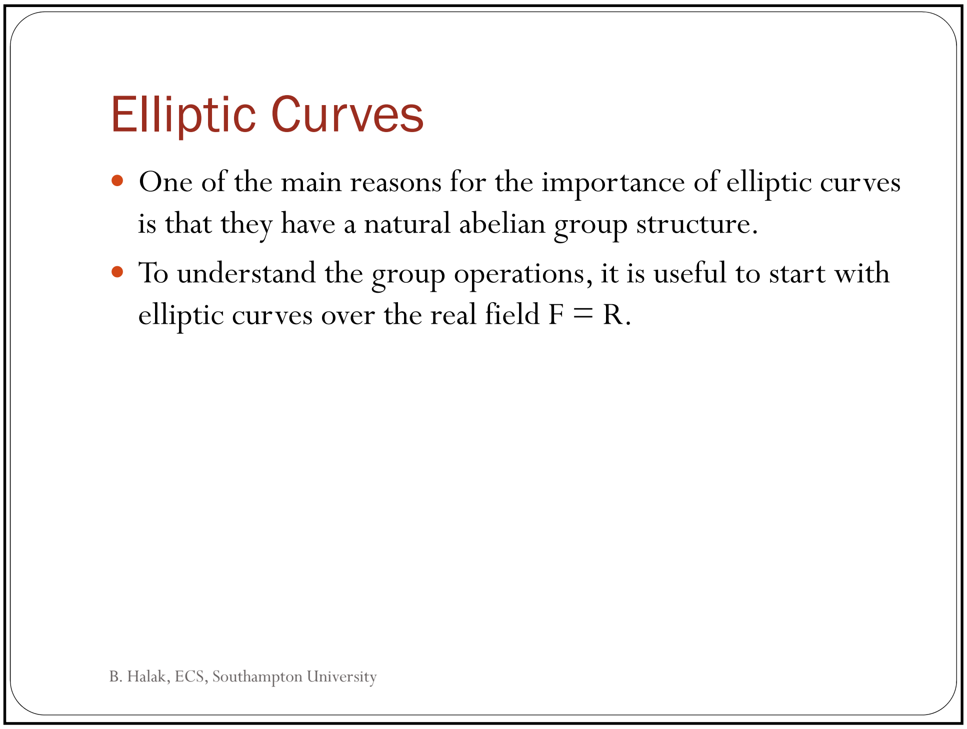
What is an Elliptic Curve?

- **Restrictions:**

Curves, where the polynomial `x`^{3} `+ ax + b` has a double root, cannot be used to construct a cryptographic system. This condition is equivalent to

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

This condition ensures the elliptic curve equation has three distinct roots



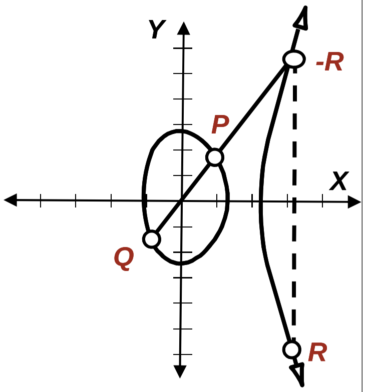
Elliptic Curves

- One of the main reasons for the importance of elliptic curves is that they have a natural abelian group structure.
- To understand the group operations, it is useful to start with elliptic curves over the real field F = R.

Addition in Elliptic Curve

- **Given P and Q as two distinct points** on an elliptic curve, and the P is not -Q.
- **Geometric Addition**: To add two distinct points P and Q, a line is drawn through the two points. This line will intersect the elliptic curve in exactly one more point, call -R. The point -R is reflected in the x-axis to the point R.
- **By definition :** addition in an elliptic curve group is

P + Q = R



Algebraic Addition in Elliptic Curve

- **Given P and Q as two distinct points**

$P = (x_1, y_1)$

$\mathrm{Q} = (x_2\ y_2)$

$P + Q = R = (x_R, y_R)$

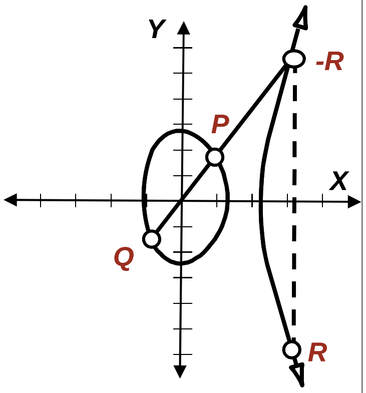
Where:

$x_R = \boldsymbol{\lambda}^2 - x_1 - x_2$

$y_R = -y_1 + \boldsymbol{\lambda}(x_1 - x_R)$

Where :

$$\boldsymbol{\lambda} = \frac{y_2 - y_1}{x_2 - x_1}$$

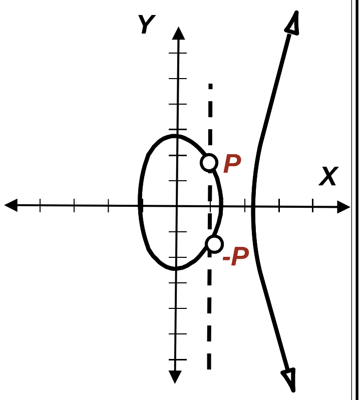


Addition in Elliptic Curve

- **Adding the points P and -P** on an elliptic curve
- The line through P and -P is a vertical line which does not intersect the elliptic curve at a third point; thus the points P and -P cannot be added as previously. It is for this reason that the elliptic curve group includes the point at infinity O.
- **By definition,**

  P + (-P) = O

- As a result of this equation, P + O = P in the elliptic curve group . O is called the additive identity of the elliptic curve group.



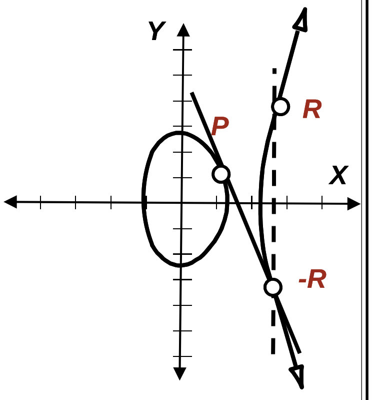
Addition in Elliptic Curve

- **Doubling the Point:**

Case 1: $y_p \neq 0$

To double the point , draw a tangent line to the curve is drawn at the point P. This line intersects the elliptic curve at exactly one other point, -R. -R is reflected in the x-axis to R.

P + P = 2P = R



Addition in Elliptic Curve

- **Doubling the Point:**

Case 1: $\boldsymbol{y_p \neq 0}$

$P = (x_1, y_1)$
$2P = R = (x_R, y_R)$

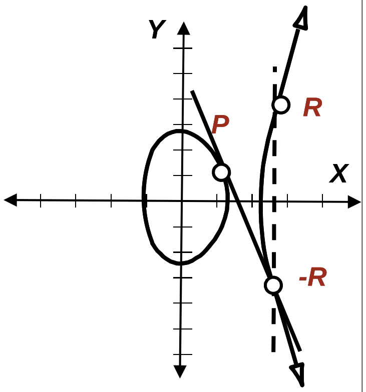
Where:

$x_R = \boldsymbol{\lambda}^2 - 2x_1$

$y_R = -y_1 + \boldsymbol{\lambda}(x_1 - x_R)$

Where :

$$\boldsymbol{\lambda} = \frac{3{x_1}^2 + a}{2y_1}$$



Algebraic Addition in Elliptic Curve

- **Given P and Q as two distinct points** $(x_1 \neq x_2)$

$P = (x_1, y_1)$
$\text{Q} = (x_2\ y_2)$

$P + Q = R = (x_R, y_R)$

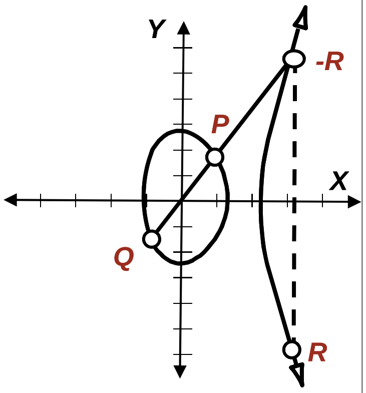
Where:

$x_R = \boldsymbol{\lambda}^2 - x_1 - x_2$

$y_R = -y_1 + \boldsymbol{\lambda}(x_1 - x_R)$

Where :

$$\boldsymbol{\lambda} = \frac{y_2 - y_1}{x_2 - x_1}$$

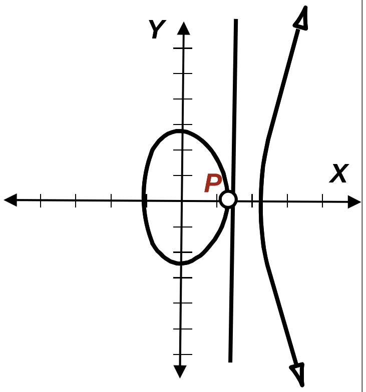


Addition in Elliptic Curve

- **Doubling the Point:**

Case 2: $y_p = 0$

In this case the tangent line to the elliptic curve at P is vertical and does not intersect the elliptic curve at any other point.



- **By definition:**

2P = O for such a point P.

- **Note**: To find 3P in this situation, one can add 2P + P. This becomes P + O = P Thus 3P = P.

  3P = P, 4P = O, 5P = P, 6P = O, 7P = P, etc.

Groups

Let G be a non-empty set, and let * be a binary operation on G. This means that for every two points a, b ∈ G, a value a * b is defined.

We say that G is a group if it has the following properties:

1. **CLOSURE**: ∀ a, b ∈ G then (a * b) ∈ G .
2. **ASSOCIATIVITY**: ∀ a, b, c ∈ G then (a * b) * c = a *(b * c).
3. **IDENTITY**: there exists e ∈ G such that a * e = a = e * a for all a ∈ G.
4. **INVERTABILITY**: for every a ∈ G there exists ai ∈ G such that a * ai = e = ai * a.

Abelian Groups

A group G is said to be commutative (or abelian) if (a* b)= (b *a) for all a, b ∈ G

Abelian Groups on Elliptic Curves

- **Theorem**: Any elliptic curve E over a filed F is an abelian group under the operation + defined above.

  Where

$$E = E(F) = \{(x,y)|x,y \in F, y^3 = x^2 + ax + b\} \cup \{\infty,\infty\}$$

Provided:

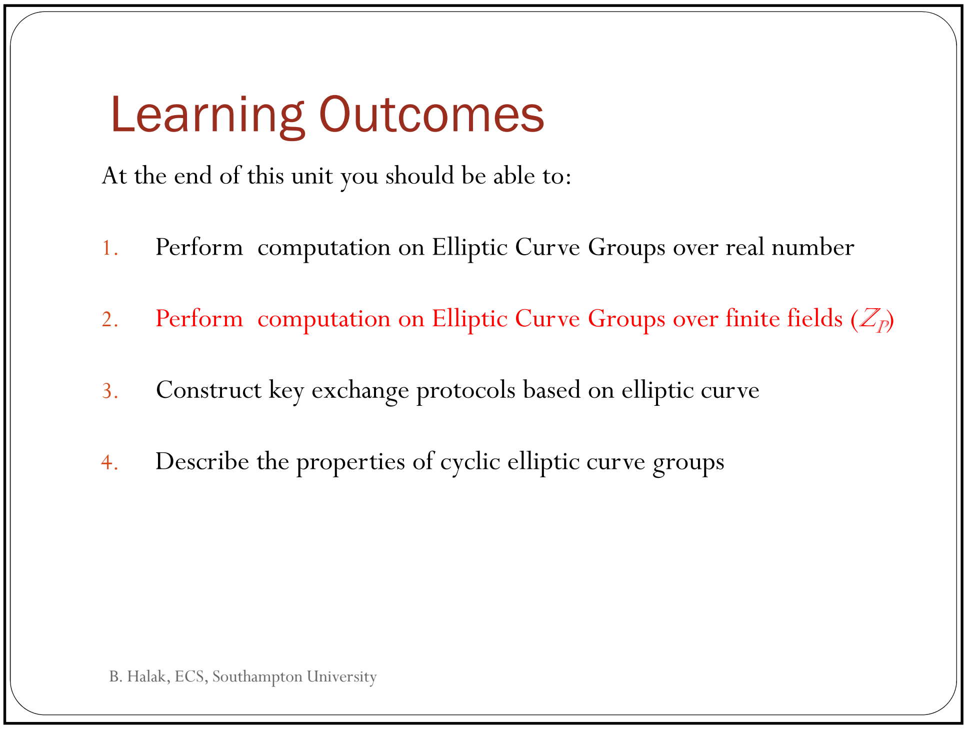
$$4a^3 + 27b^2 \neq 0$$

Abelian Groups on Elliptic Curves

- **Proof:**

1. **CLOSURE**:For P and Q on the curve , point P +Q always exist and is on the curve.
2. **ASSOCIATIVITY**: P+(Q+R) = (P+Q)+R(associativity,hard to prove but holds).
3. **IDENTITY**: P+O=P
4. **INVERTABILITY**: P+ -P =O
5. **COMMUTATIVITY:** P + Q = Q + P (obvious)

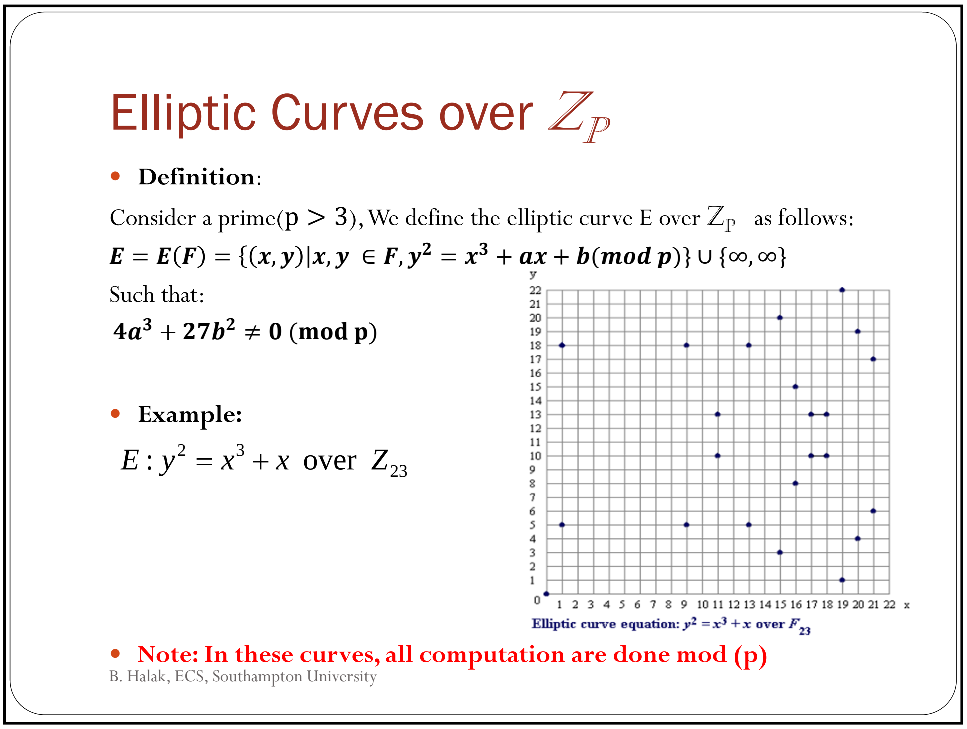
- **Note**: although we have used the field F = R to provide motivation and to enable visualization, we can in fact use the same formulae to define an abelian group structure over any field.



Learning Outcomes

At the end of this unit you should be able to:

1. Perform computation on Elliptic Curve Groups over real number
2. Perform computation on Elliptic Curve Groups over finite fields (Z_P)
3. Construct key exchange protocols based on elliptic curve
4. Describe the properties of cyclic elliptic curve groups



Elliptic Curves over Z_P

- **Definition**:

Consider a prime($p > 3$), We define the elliptic curve E over Z_P as follows:

$$\boldsymbol{E = E(F) = \{(x,y) | x, y \in F, y^2 = x^3 + ax + b (mod\ p)\} \cup \{\infty, \infty\}}$$

Such that:

$$\mathbf{4a^3 + 27b^2 \neq 0\ (mod\ p)}$$

- **Example:**

$$E : y^2 = x^3 + x \text{ over } Z_{23}$$

Elliptic curve equation: $y^2 = x^3 + x$ over F_{23}

- **Note: In these curves, all computation are done mod (p)**

Elliptic Curves over Z_P

- **Exercise**: find all points on the elliptic curve below

$E: y^2 = x^3 + 2x + 1 \text{ over } Z_5$

Elliptic Curves over Z_P

- **Exercise**: find all points on the elliptic curve below

$E: y^2 = x^3 + 2x + 1 \text{ over } Z_5$

First check that validity of the equation:

$\mathbf{4a^3} + \mathbf{27b^2} = \mathbf{59} = \mathbf{4} \bmod(5)$

Then we calculate the points on the elliptic curve

x = 0 , $y^2 = 1 \Rightarrow y = 1,4$
x = 1 , $y^2 = 4 \Rightarrow y = 2,3$ (mod 5)
x = 2 , $y^2 = 13 = 3 \Rightarrow$ no solution (mod 5)
x = 3 , $y^2 = 34 = 4 \Rightarrow y = 2,3$ (mod 5)
x = 4 , $y^2 = 73 = 3 \Rightarrow$ no solution (mod 5)

Then points on the elliptic curve are

(0,1) (0,4) (1,2)(1,3)(3,2) (3,3) and the point at infinity: O

Properties of Elliptic Curves

- **The order of an elliptic curve** E over a finite filed Z_p is denoted $|E|$ and it refers to the number of points on the curve plus O.

- **Hasse's theorem** gives the upper and lower bounds for $|E|$ as follows:

  For an elliptic curve E curve over a finite filed Z_p

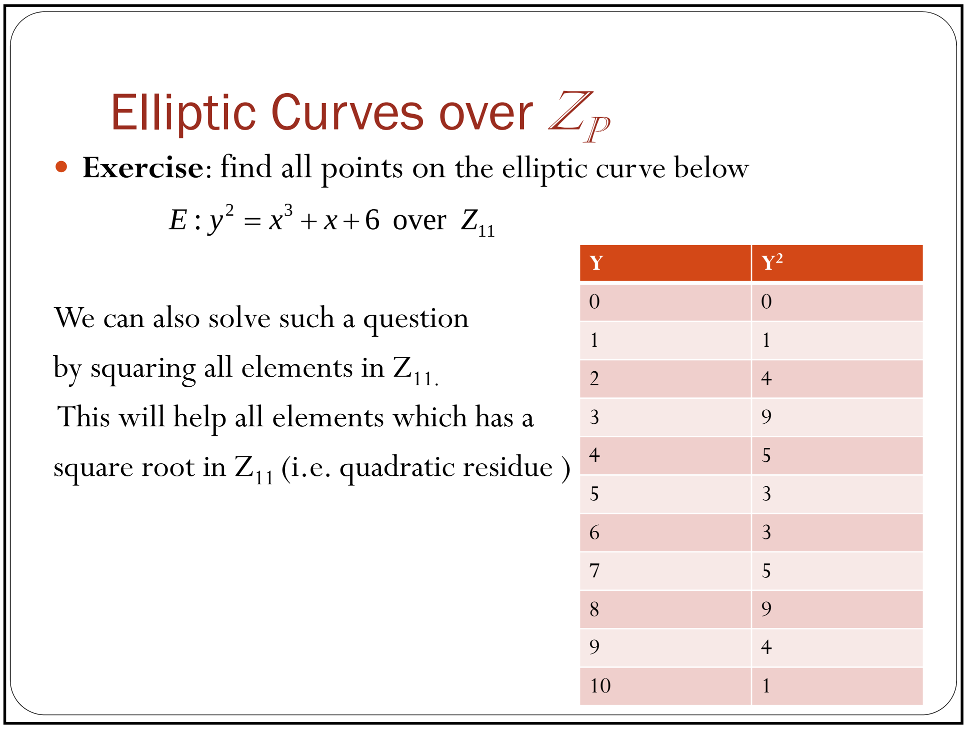
$$p+1-2\sqrt{p} \le |E| \le p+1+2\sqrt{p}.$$

Thus, taking a large field guarantees a large elliptic curve

Elliptic Curves over Z_P

- **Exercise**: find all points on the elliptic curve below

  $E: y^2 = x^3 + x + 6$ over Z_{11}



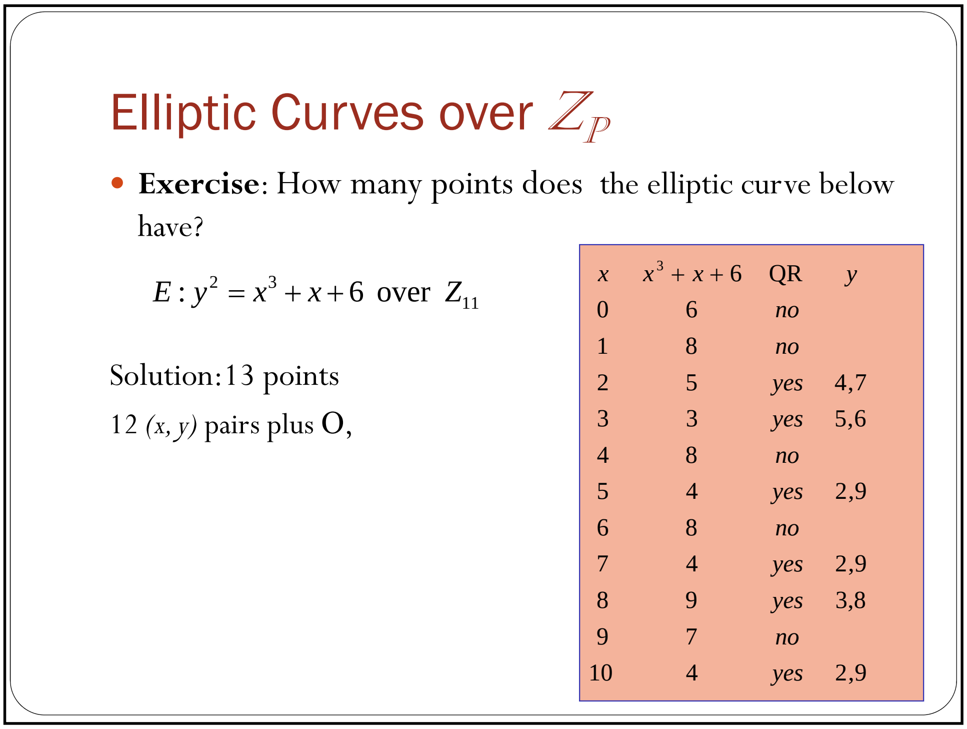
Elliptic Curves over Z_p

- **Exercise**: find all points on the elliptic curve below

$$E: y^2 = x^3 + x + 6 \text{ over } Z_{11}$$

We can also solve such a question by squaring all elements in Z_{11}.
This will help all elements which has a square root in Z_{11} (i.e. quadratic residue)

Y	Y²
0	0
1	1
2	4
3	9
4	5
5	3
6	3
7	5
8	9
9	4
10	1



Elliptic Curves over Z_p

- **Exercise**: How many points does the elliptic curve below have?

$$E: y^2 = x^3 + x + 6 \text{ over } Z_{11}$$

Solution:13 points

12 *(x, y)* pairs plus O,

x	x^3+x+6	QR	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

Point Addition Example Elliptic Curves over Z_P

- **Exercise**: Given E below and P= $(2, 7)$, find $2P$

$$E : y^2 = x^3 + x + 6 \text{ over } Z_{11}$$

Addition in Elliptic Curve

- **Doubling the Point:**

Case 1: $\boldsymbol{y_p \neq 0}$

$P = (x_1, y_1)$
$2P = R = (x_R, y_R)$

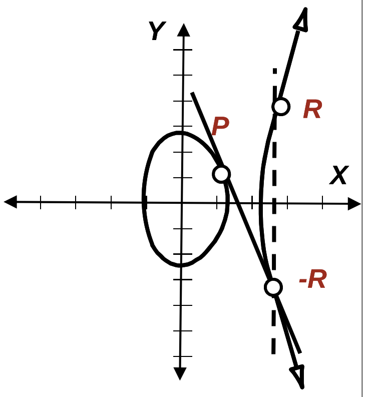
Where:

$x_R = \boldsymbol{\lambda}^2 - 2x_1$

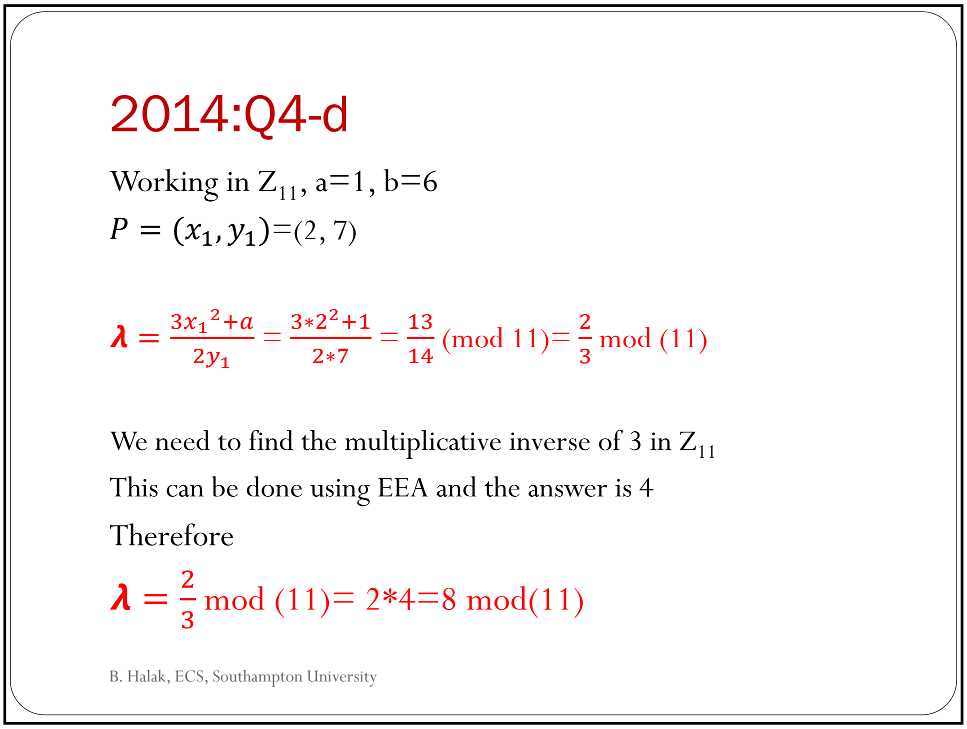
$y_R = -y_1 + \boldsymbol{\lambda}(x_1 - x_R)$

Where :

$$\boldsymbol{\lambda} = \frac{3{x_1}^2 + a}{2y_1}$$



B. Halak, ECS, Southampton University



2014:Q4-d

Working in Z_{11}, a=1, b=6

$P = (x_1, y_1)$=(2, 7)

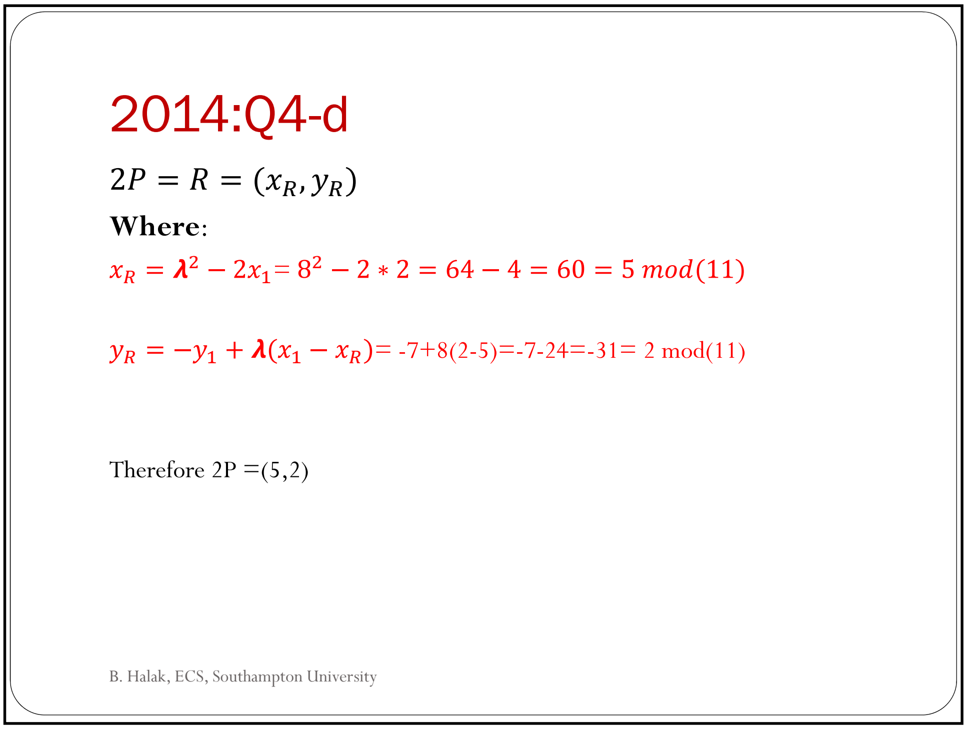
$$\boldsymbol{\lambda} = \frac{3{x_1}^2+a}{2y_1} = \frac{3*2^2+1}{2*7} = \frac{13}{14} \text{ (mod 11)} = \frac{2}{3} \text{ mod (11)}$$

We need to find the multiplicative inverse of 3 in Z_{11}

This can be done using EEA and the answer is 4

Therefore

$$\boldsymbol{\lambda} = \frac{2}{3} \text{ mod (11)} = 2*4=8 \text{ mod(11)}$$



2014:Q4-d

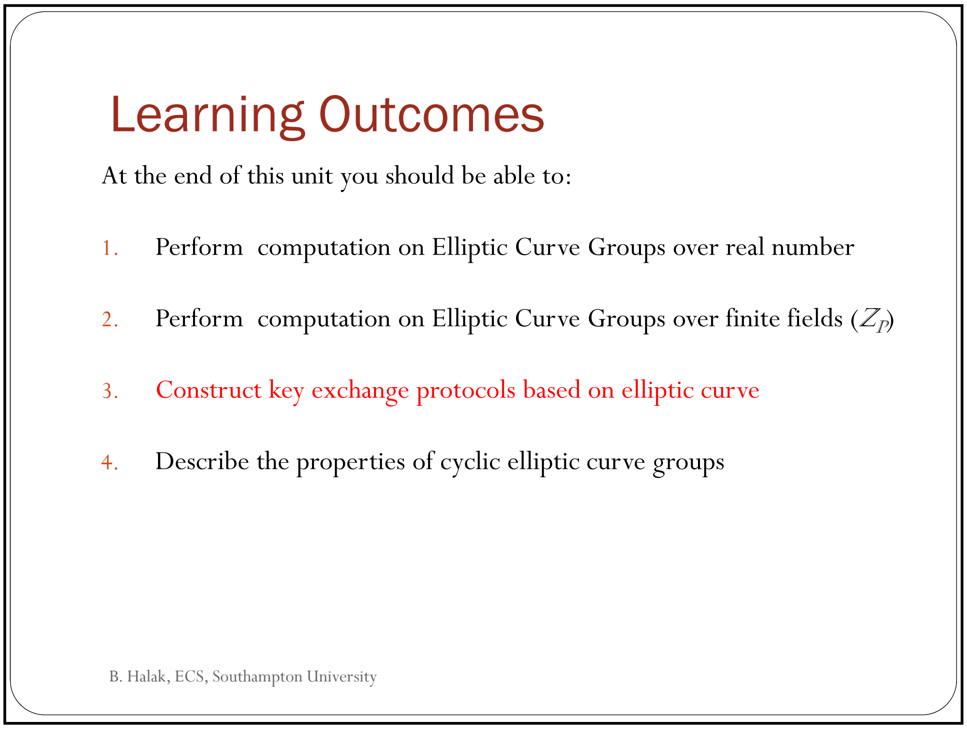
$2P = R = (x_R, y_R)$

Where:

$x_R = \boldsymbol{\lambda}^2 - 2x_1 = 8^2 - 2 * 2 = 64 - 4 = 60 = 5\ mod(11)$

$y_R = -y_1 + \boldsymbol{\lambda}(x_1 - x_R)$= -7+8(2-5)=-7-24=-31= 2 mod(11)

Therefore 2P =(5,2)

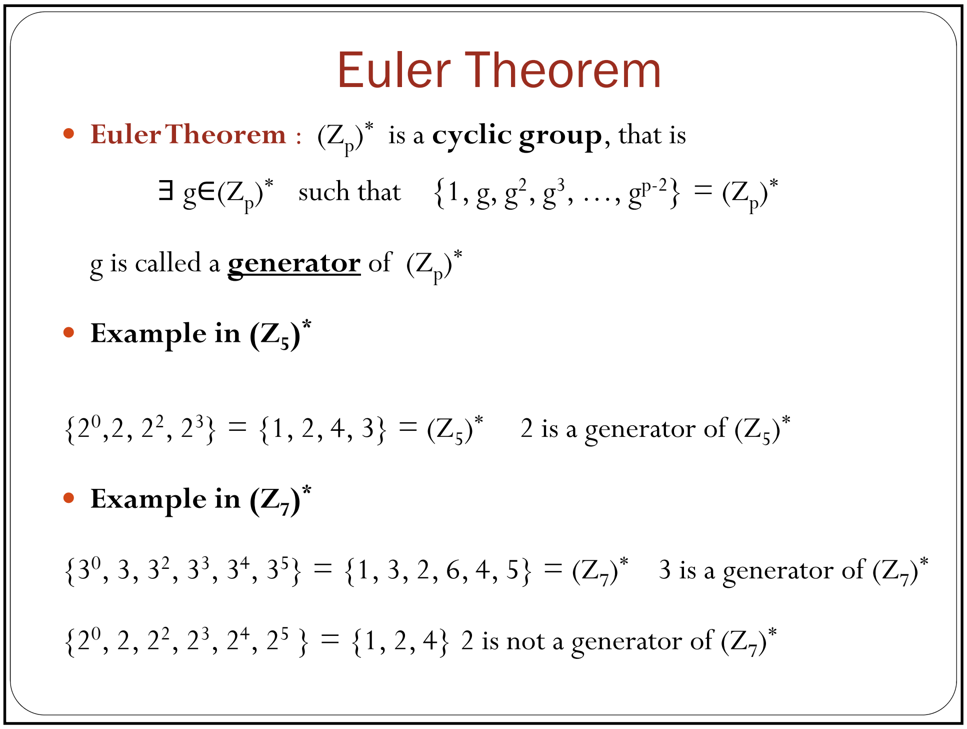


Learning Outcomes

At the end of this unit you should be able to:

1. Perform computation on Elliptic Curve Groups over real number
2. Perform computation on Elliptic Curve Groups over finite fields (Z_p)
3. Construct key exchange protocols based on elliptic curve
4. Describe the properties of cyclic elliptic curve groups

B. Halak, ECS, Southampton University



Euler Theorem

- **Euler Theorem :** $(Z_p)^*$ is a **cyclic group**, that is

  $\exists\ g \in (Z_p)^*$ such that $\{1, g, g^2, g^3, \ldots, g^{p-2}\} = (Z_p)^*$

  g is called a **generator** of $(Z_p)^*$

- **Example in $(Z_5)^*$**

$\{2^0, 2, 2^2, 2^3\} = \{1, 2, 4, 3\} = (Z_5)^*$ 2 is a generator of $(Z_5)^*$

- **Example in $(Z_7)^*$**

$\{3^0, 3, 3^2, 3^3, 3^4, 3^5\} = \{1, 3, 2, 6, 4, 5\} = (Z_7)^*$ 3 is a generator of $(Z_7)^*$

$\{2^0, 2, 2^2, 2^3, 2^4, 2^5\} = \{1, 2, 4\}$ 2 is not a generator of $(Z_7)^*$

The Order of an element in a group

- For $g \in (Z_p)^*$ the set $\{1 , g , g^2, g^3, \dots \}$ is called

  the **group generated by g**, denoted $<g>$

- **The order** of $g \in (Z_p)^*$ is the size of $<g>$

$\mathrm{ord}_p(g) = |<g>| =$ (smallest $a>0$ s.t. $g^a = 1$ in Z_p)

- **Examples $(Z_7)^*$** :

$\mathrm{ord}_7(3) = 6$; $\mathrm{ord}_7(2) = 3$; $\mathrm{ord}_7(1) = 1$

The Order of an element in an Elliptic Curve group

- **Definition**: For $P \in E(F_Q)$ the set $\{O , P , 2P, 3P, \dots (m-1)P \}$ is called

  the **group generated by P**, denoted $<P>$

Where $mP=O$.

Beyond mP, this pattern repeats in a cycle of length m

- **The order** of $P \in E(F_Q)$ is the size of $<P>$

The Order of an element in an Elliptic Curve group

- **Example**:

$$E : y^2 = x^3 + 2 \text{ over } Z_5$$

The elements of this group are $\{(2, 0), (3,\pm 2), (4,\pm 1) , O\}$.

If we take P = (4, 1) we find that

2P = (3,−2), 3P = (2, 0), 4P = (3, 2), 5P = (4,−1) 6P = O,

The order of P is 6

Therefore P is a generator and E is a cyclic group.

- **Excises: Verify the multiples of P above**

Addition in Elliptic Curve

- **Doubling the Point:**

Case 1: $\boldsymbol{y_p \neq 0}$

$P = (x_1, y_1)$

$2P = R = (x_R, y_R)$

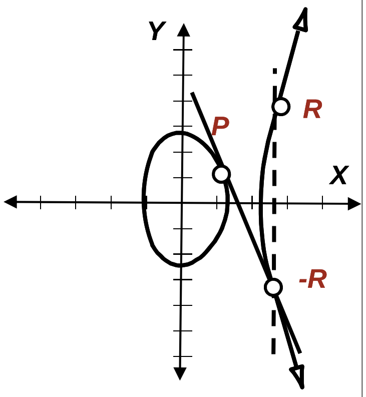
Where:

$x_R = \boldsymbol{\lambda}^2 - 2x_1$

$y_R = -y_1 + \boldsymbol{\lambda}(x_1 - x_R)$

Where :

$$\boldsymbol{\lambda} = \frac{3{x_1}^2 + a}{2y_1}$$



- **Solution:** we calculate sums and multiples in E, working with the field $F = Z5$.
- **For instance**, to calculate $2P = 2(4, 1)$ we have $a = 0$, $x_1 = 4$ and $y_1 = 1$,so $\boldsymbol{\lambda} = (3x_1^{\,2} + a)/2y_1 = 4$, giving $x_3 = \boldsymbol{\lambda}^2 - 2x_1 = 3$ and $y_3 = y_1 + \boldsymbol{\lambda}(x_3 - x_1) = 2$, and hence $2P = (x_3, -y_3) = (3, -2)$.

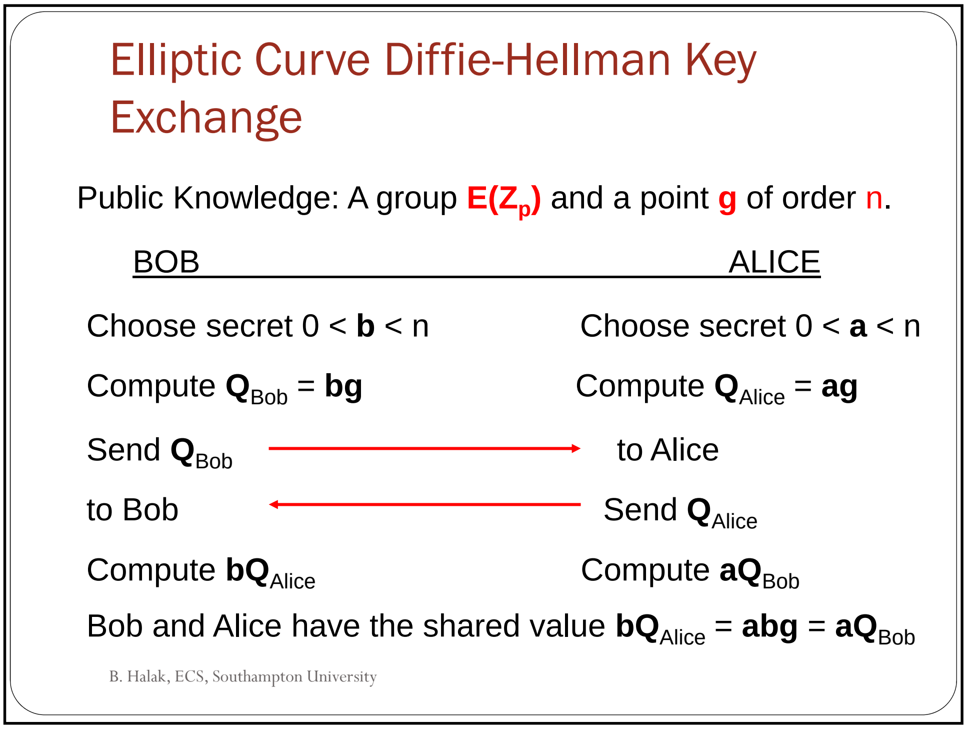
The other calculations are similar.

Elliptic Curve Discrete Logarithm Problem

- **Problem** Given two points ***P*** and ***Q*** in an elliptic curve E over a finite filed Z_p, find an integer ***i*** satisfying

$$\boxed{Q = \boldsymbol{i}.P}$$

- The security of ECC depends on how difficult it is to determine *i* given *iP* and P. This is referred to as the elliptic curve logarithm problem (ECDLP)
- One of the fastest known technique's to solve ECDLP is called *Pollard rho method*
- Compared to factoring integers or polynomials, one can use much smaller numbers for equivalent levels of security.



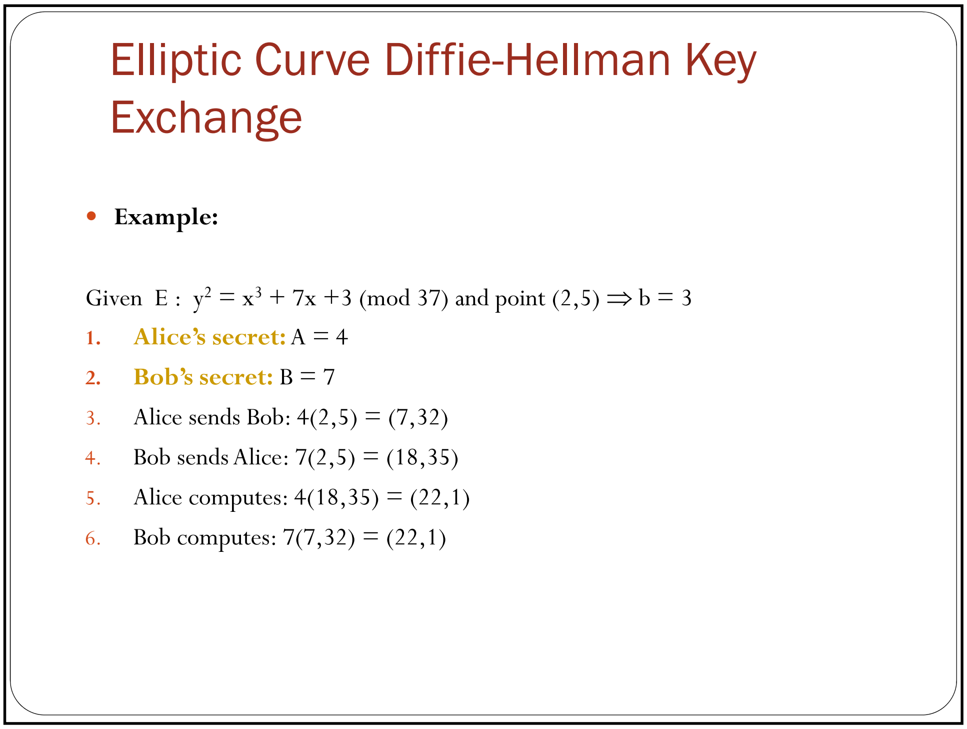
Elliptic Curve Diffie-Hellman Key Exchange

Public Knowledge: A group **$E(Z_p)$** and a point **g** of order n.

BOB		ALICE
Choose secret 0 < **b** < n		Choose secret 0 < **a** < n
Compute $\mathbf{Q}_{Bob}$ = **bg**		Compute $\mathbf{Q}_{Alice}$ = **ag**
Send $\mathbf{Q}_{Bob}$	$\longrightarrow$	to Alice
to Bob	$\longleftarrow$	Send $\mathbf{Q}_{Alice}$
Compute $\mathbf{bQ}_{Alice}$		Compute $\mathbf{aQ}_{Bob}$

Bob and Alice have the shared value $\mathbf{bQ}_{Alice}$ = **abg** = $\mathbf{aQ}_{Bob}$

B. Halak, ECS, Southampton University

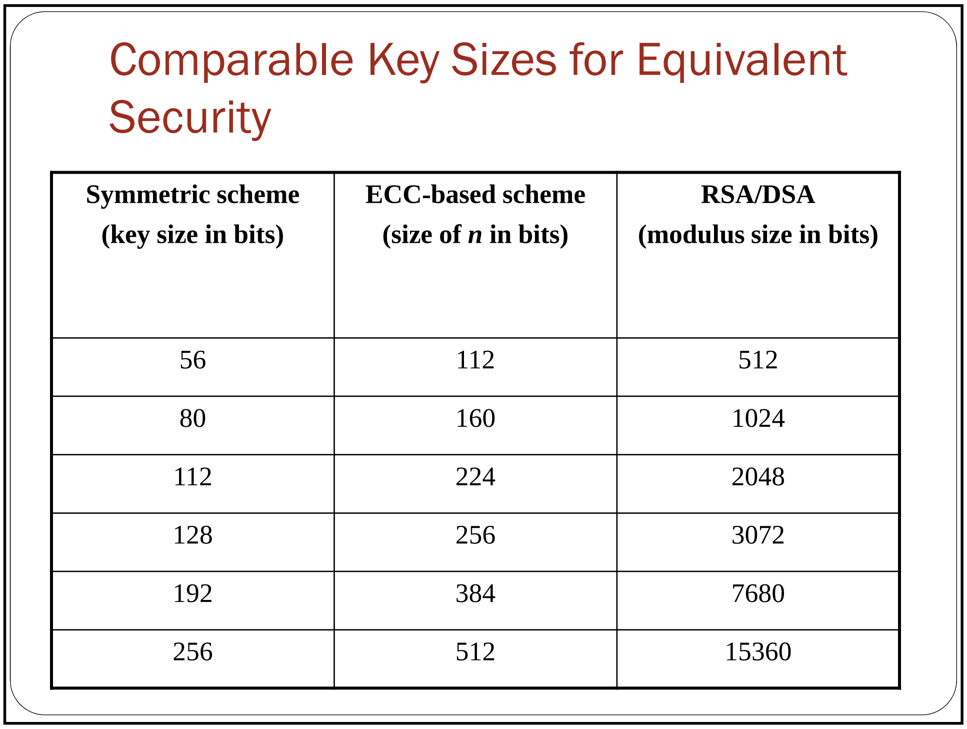


Elliptic Curve Diffie-Hellman Key Exchange

- **Example:**

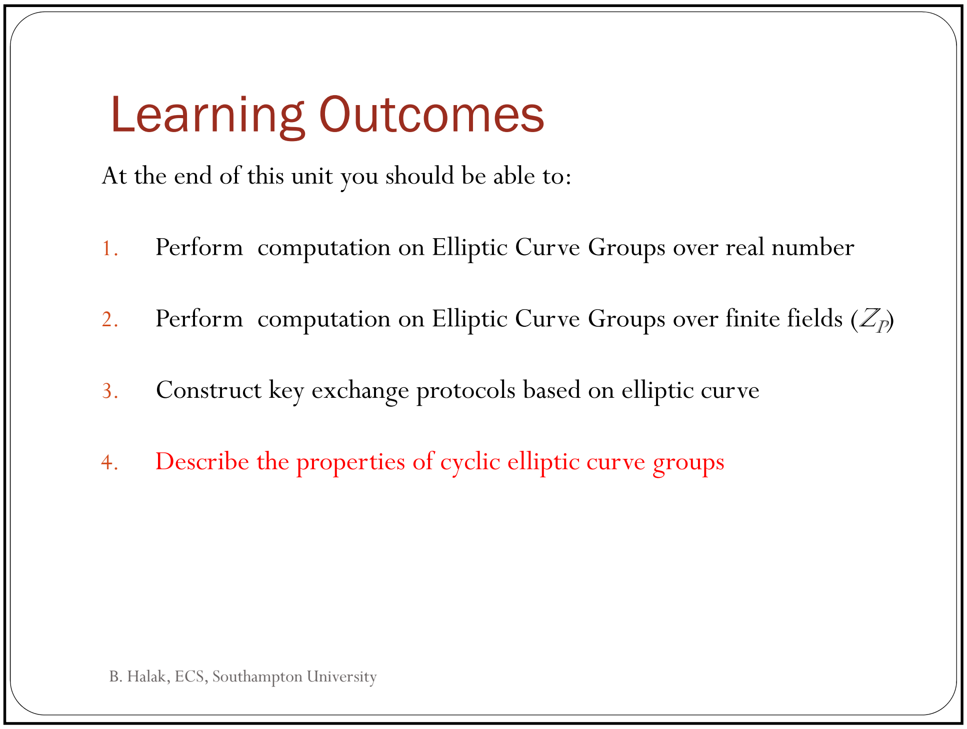
Given E : $y^2 = x^3 + 7x + 3 \pmod{37}$ and point (2,5) $\Rightarrow$ b = 3

1. **Alice's secret:** A = 4
2. **Bob's secret:** B = 7
3. Alice sends Bob: 4(2,5) = (7,32)
4. Bob sends Alice: 7(2,5) = (18,35)
5. Alice computes: 4(18,35) = (22,1)
6. Bob computes: 7(7,32) = (22,1)



Comparable Key Sizes for Equivalent Security

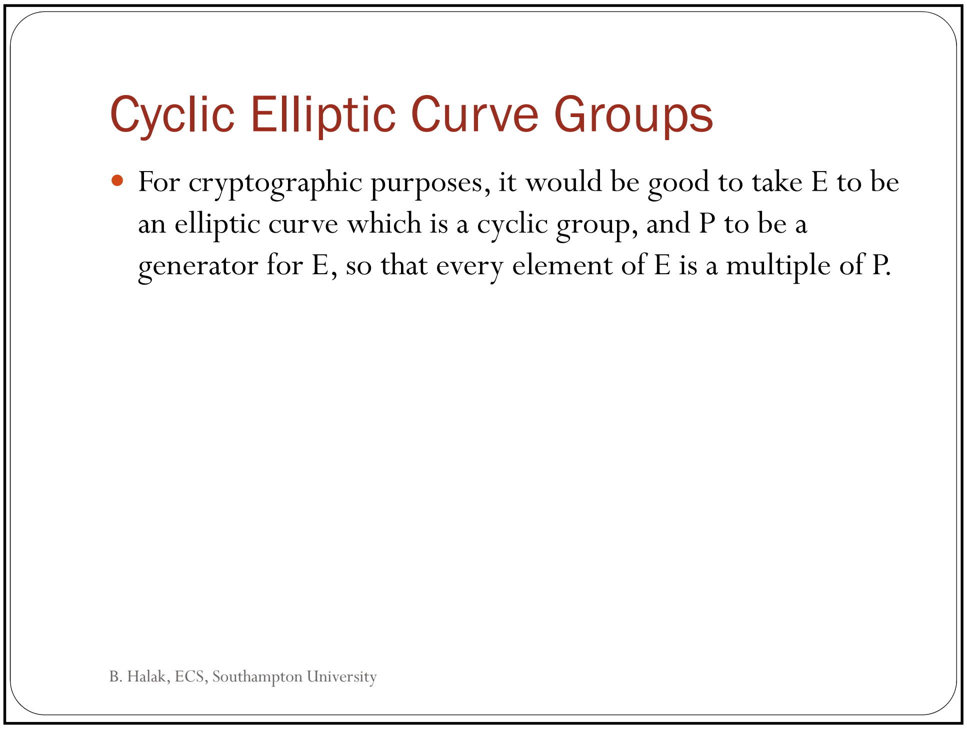
Symmetric scheme (key size in bits)	**ECC-based scheme (size of *n* in bits)**	**RSA/DSA (modulus size in bits)**
56	112	512
80	160	1024
112	224	2048
128	256	3072
192	384	7680
256	512	15360



Learning Outcomes

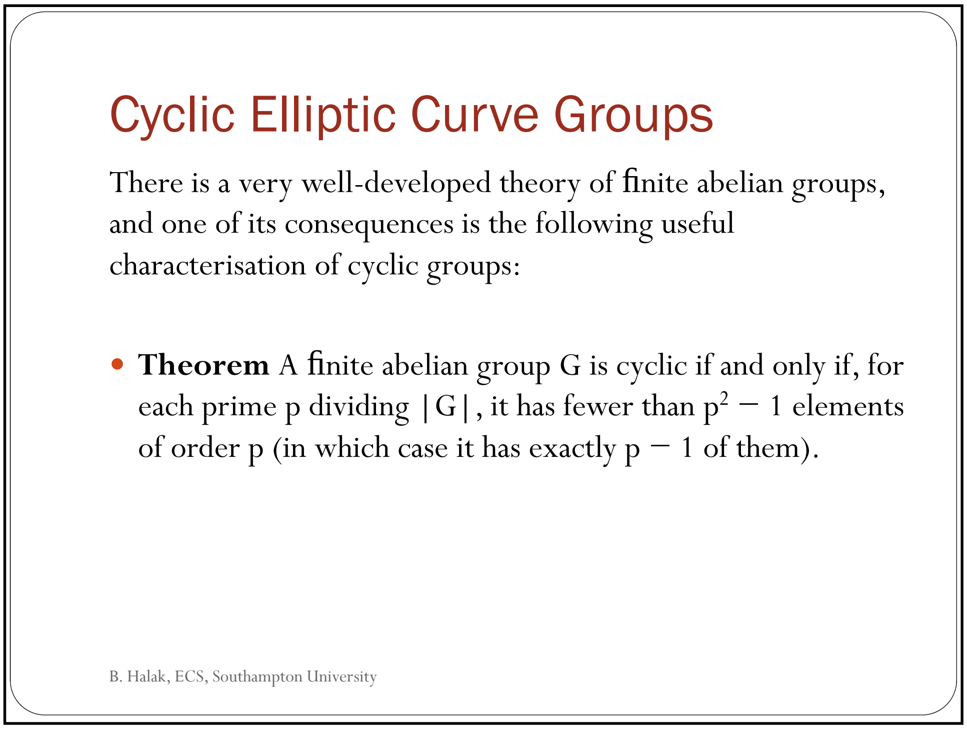
At the end of this unit you should be able to:

1. Perform computation on Elliptic Curve Groups over real number
2. Perform computation on Elliptic Curve Groups over finite fields (Z_p)
3. Construct key exchange protocols based on elliptic curve
4. Describe the properties of cyclic elliptic curve groups



Cyclic Elliptic Curve Groups

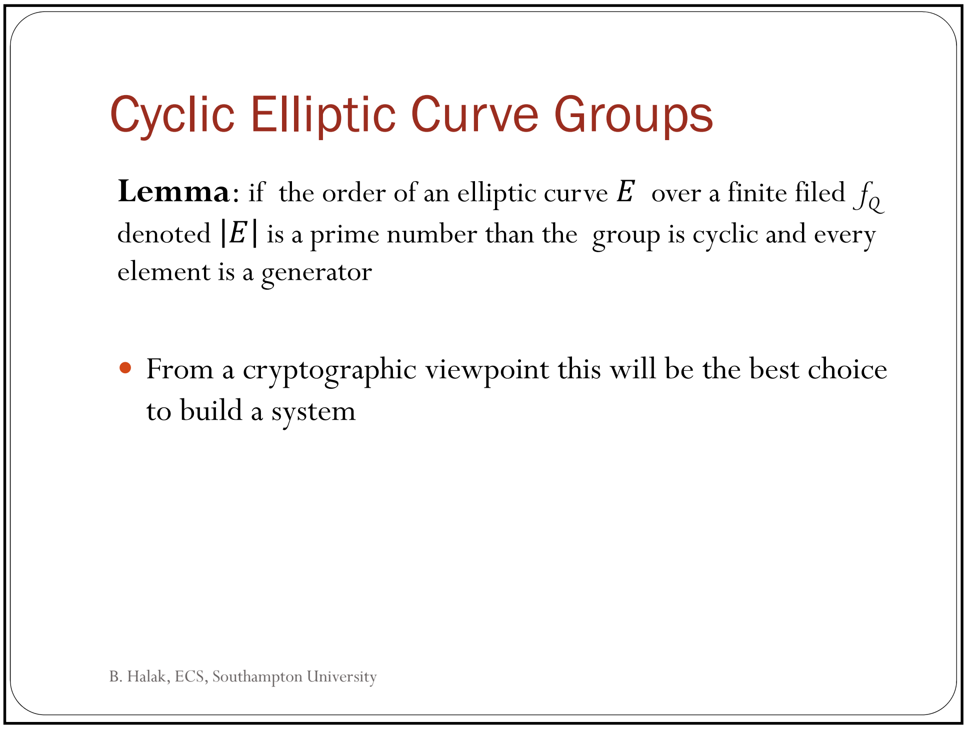
- For cryptographic purposes, it would be good to take E to be an elliptic curve which is a cyclic group, and P to be a generator for E, so that every element of E is a multiple of P.



Cyclic Elliptic Curve Groups

There is a very well-developed theory of finite abelian groups, and one of its consequences is the following useful characterisation of cyclic groups:

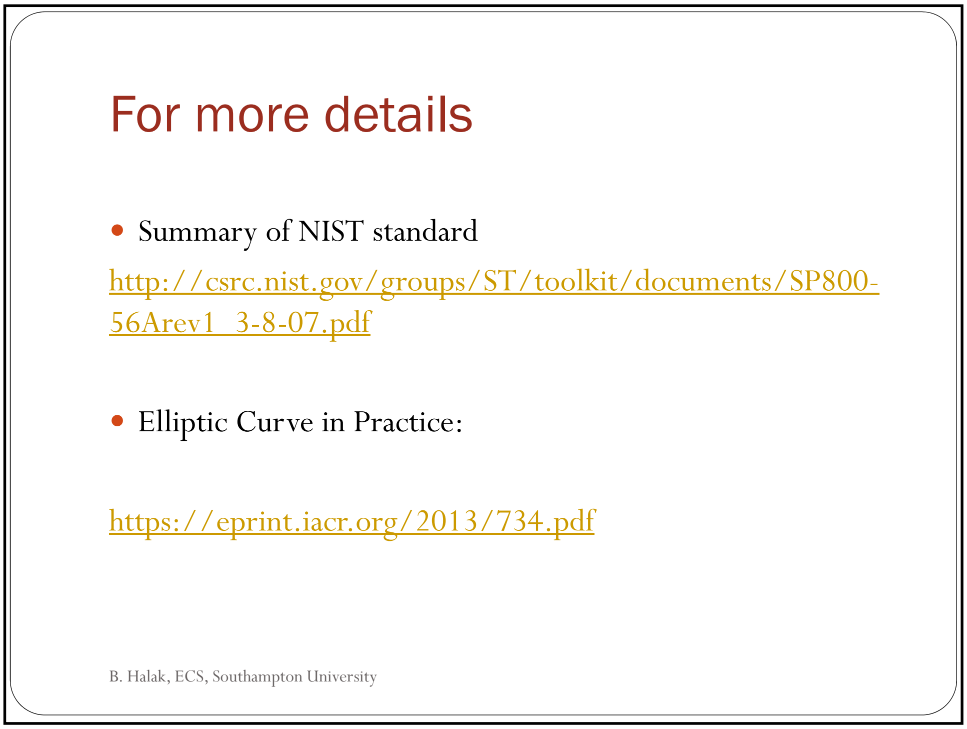
- **Theorem** A finite abelian group G is cyclic if and only if, for each prime p dividing $|G|$, it has fewer than $p^2 - 1$ elements of order p (in which case it has exactly $p - 1$ of them).



Cyclic Elliptic Curve Groups

Lemma: if the order of an elliptic curve E over a finite filed f_Q denoted $|E|$ is a prime number than the group is cyclic and every element is a generator

- From a cryptographic viewpoint this will be the best choice to build a system



For more details

- Summary of NIST standard

http://csrc.nist.gov/groups/ST/toolkit/documents/SP800-56Arev1_3-8-07.pdf

- Elliptic Curve in Practice:

https://eprint.iacr.org/2013/734.pdf