Elliptic Curves

Giulia Mauri

Politecnico di Milano

email: *giulia.mauri@polimi.it*
website: *http://home.deib.polimi.it/gmauri*

May 13, 2015

Overview

1. Elliptic Curves
2. Logarithm Problems on EC
   - Baby Step, Giant Step
   - Pohlig-Hellman Method
3. Elliptic Curve Cryptosystems
   - ElGamal Cryptosystem
   - ECDHKE
   - ECIES

Elliptic Curve

Definition (Elliptic Curve)

An elliptic curve E is the graph of an equation:

$$E : y^2 = x^3 + ax^2 + bx + c$$

Definition (Addition Law)

Let E given by $y^2 = x^3 + bx + c$ and let $P_1 = (x_1, y_1), P_2 = (x_2, y_2)$.
Then $P_1 + P_2 = P_3 = (x_3, y_3)$, where:
$x_3 = m^2 - x_1 - x_2$
$y_3 = m(x_1 - x_3) - y_1$

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

If the slope m is infinite, then $P_3 = \infty$. There is one additional law: $\infty + P = P$ for all points P.

Exercise 1

Exercise

1. *List the points on the elliptic curve* $E : y^2 \equiv x^3 - 2 \pmod 7$.
2. *Given* $P = (3, 2)$ *and* $Q = (5, 5)$, *find the sum* $P + Q$ *on* E.
3. *Given* $P = (3, 2)$ *and* $Q = P$, *find the sum* $P + Q$ *on* E.
4. *Verify if* P *is a primitive generator.*

Exercise 1

Solution

[1]

x	$y^2 \equiv a \pmod 7$	$a^{\frac{p-1}{2}} \pmod 7$	$y \equiv a^{\frac{p+1}{4}} \pmod 7$
0	5	-1	–
1	6	-1	–
2	6	-1	–
3	4	1	± 2
4	6	-1	–
5	4	1	± 2
6	4	1	± 2
∞	–	–	∞

So the points are: $(3,2),(3,5),(5,2),(5,5),(6,2),(6,5),\infty$.

Exercise 1

Solution

[2] $m \equiv (5-2)\cdot(5-3)^{-1} \equiv 3\cdot 2^{-1} \equiv 5 \pmod 7$
$x_3 \equiv 5^2 - 5 - 3 \equiv 3$
$y_3 \equiv 5(3-3) - 2 \equiv 5$

So $P + Q = (3, 5)$.

[3] $m \equiv (3\cdot 9 + 0)(4)^{-1} \equiv 6\cdot 4^{-1} \equiv 5 \pmod 7$
$x_3 \equiv 5^2 - 3 - 3 \equiv 5$
$y_3 \equiv 5(3-5) - 2 \equiv 2$

So $2P = (5, 2)$.

[4] The number of points is 7 that is prime, so P is primitive and it has order 7.

Exercise 2

Exercise

Given an elliptic curve E over $\mathbb{Z}_{29}$ and the base point $P = (8, 10)$:

$$E : y^2 = x^3 + 4x + 20 \bmod 29.$$

Calculate the following point multiplication $k \cdot P$ using the Double-and-Add algorithm. Provide the intermediate results after each step. Use $k = 9$ and $k = 20$.

Solution

$9P = (1001)_2 P$

$$\begin{array}{c|r} 1 & P = (8, 10) \\ 0 & 2P = 2(8, 10) = (0, 22) \\ 0 & 2P + 2P = 2(0, 22) = (6, 17) \\ 1 & 4P + 4P + P = 2(6, 17) + (8, 10) = (4, 10) \end{array}$$

Exercise 2

Solution

$20P = (10100)_2 P$

$$
\begin{array}{c|r}
1 & P = (8, 10) \\
0 & 2P = 2(8, 10) = (0, 22) \\
1 & 2P + 2P + P = 2(0, 22) + (8, 10) = (20, 3) \\
0 & 5P + 5P = 2(20, 3) = (17, 19) \\
1 & 10P + 10P + P = 2(17, 19) + (8, 10) = (19, 13)
\end{array}
$$

BSGS

We have $Q = kP$ and we would like to find k over the Elliptic Curve.
This method requires approximately $\sqrt{M}$ steps and around $\sqrt{M}$ storage.
The procedure is as follows:

1. Fix an integer $M \geq \lceil \sqrt{N} \rceil$, where N is the number of points of the curve.
2. Make and store a list of iP for $0 \leq i < M$.
3. Compute the points $Q - jMP$ for $j = 0, 1, \ldots M - 1$ until one matches an element from the stored list.
4. If $iP = Q - jMP$, we have $Q = kP$ with $k \equiv i + jM \pmod{N}$.

Exercise 3

Exercise

Alice and Bob exchange a session key using the Diffie-Hellman protocol. They publish an elliptic curve $E : y^2 \equiv x^3 + x + 2 \pmod{13}$*.*
This curve has $N = 12$ *points. They also publish* $P = (6, 4)$*.*
Alice sends the message $A = aP = (7, 12)$ *and receives the message* $B = bP = (7, 1)$*.*
Compute b*.*

Exercise 3

Solution

We use the baby step, giant step algorithm. We choose $M = \lceil\sqrt{12}\rceil = 4$*. We compute*

$$-MP = 4(-P) = 4(6,9) = (9,5)$$

and build the table:

i,j	iP	$B - jMP = B + j(-MP)$
0	∞	$(7,1)$
1	$(6,4)$	$(7,1)+(9,5)=(1,11)$
2	$(2,5)$	$\dots$
3	$(1,11)$	$\dots$

We find out that $3P = B - 1\cdot 4P$*, therefore* $B = (3+4)P = 7P$ *and* $b = 7$*.*

PH Method

As before, P, Q are elements in a group G and we want to find an integer k with $Q = kP$. We also know the order O of P and we know the prime factorization:

$$O = \prod_i q_i^{e_i}$$

The idea of Pohlig-Hellman is to find $k \pmod{q_i^{e_i}}$ for each i, then use the Chinese Remainder theorem to combine these and obtain $k \pmod{O}$. We write k as:

$$k = \sum_i a_i O_i y_i \bmod O$$

where $O = ord(P), \quad O_i = O/q_i^{e_i}, \quad y_i = O_i^{-1} \bmod q_i^{e_i}$ and $O_i Q = a_i O_i P$.

Exercise 4

Exercise

Consider the previous problem $B = bP$ and compute b using the Pohlig-Hellman method.

Solution

Since $n = 12$, *the order of P could be 2,3,12.*

$$2P = 2(6,4) = (2,5)$$

$$3P = (2,5) + (6,4) = (1,11)$$

So the order is 12. $O = ord(P) = 2^2 \cdot 3$

Exercise 4

Solution

$$O_i = O/q_i^{e_i} \rightarrow O_1 = 12/4 = 3, \quad O_2 = 12/3 = 4$$

$$y_i = O_i^{-1} \bmod q_i^{e_i} \rightarrow y_1 = 3^{-1} \bmod 4 = 3, \quad y_2 = 4^{-1} \bmod 3 = 1$$

$$O_1 B = a_1 O_1 P \rightarrow 3B = a_1 \cdot 3P \rightarrow (1,2) = a_1(1,11) \rightarrow a_1 = 3$$

$$O_2 B = a_2 O_2 P \rightarrow 4B = a_2 \cdot 4P \rightarrow (9,8) = a_2(9,8) \rightarrow a_2 = 1$$

$$b = \sum_i a_i O_i y_i \bmod O \rightarrow b = 3 \cdot 3 \cdot 3 + 1 \cdot 4 \cdot 1 \bmod 12 = 7$$

ElGamal Cryptosystem

Alice wants to send a message to Bob.
The public parameters are: the curve E, the prime p, and the points A and $B = Aa$.
Bob's secret parameter is the integer a.
To send a message to Bob, Alice does the following:

1. Alice's message is a point P_m on E.
2. Alice chooses a random integer k, computes: $Y_1 = kA$ and $Y_2 = P_m + kB$.
3. She sends the pair Y_1, Y_2 to Bob.

Bob decrypts by calculating: $P_m = Y_2 - aY_1$.

Exercise 5

Exercise

Alice uses the public key ElGamal cryptosystem. She publishes the curve $E : y^2 \equiv x^3 + 2x + 2 \pmod{13}$ *and the point* $A = (3, 3)$ *of order 15. She also chooses a secret number* $a = 7$ *and publishes the point* $B = aA$*. Bob wants to send to Alice a message corresponding to the point* $P_m = (8, 6)$*.*

Questions:

1. *Calculate* B*.*
2. *Cipher the message using* $k = 3$*.*
3. *Decipher the message.*
4. *Using the repeated nonce, decipher the ciphered message* $(Y_{1,2} = (6, -3), Y_{2,2} = (2, 1))$

Exercise 5

Solution

[1]

$$B = 7A = 2^3A - A = 2^2(4,3) - (3,3) =$$
$$= 2(8,7) + (3,-3) = (11,9) + (3,-3) = (11,4)$$

[2] Bob computes:

$$Y_1 = kA = 3(3,3) = 2(3,3) + (3,3) = (4,3) + (3,3) = (6,-3)$$
$$Y_2 = P_m + kB = (8,6) + 3(11,4) = (8,6) + (3,-3) + (11,4) = (4,3)$$

[3] Alice deciphers:

$$P_m = Y_2 - aY_1 = (4,3) - 7(6,-3) = (4,3) + 8(6,3) + (6,-3) =$$
$$= 4(2,1) + (12,8) = (2,12) + (12,8) = (8,6)$$

Exercise 5

Solution

[4] We have

$$
\begin{aligned}
Y_{2,1} - P_{m,1} = kB = Y_{2,2} - P_{m,2} \\
P_{m,2} = Y_{2,2} - Y_{2,1} + P_{m,1} \\
= (2,1) - (4,3) - (8,6) = (6,10)
\end{aligned}
$$

ECDHKE

Alice and Bob want to agree on a common key that they can use for exchanging data via a symmetric encryption scheme. One way to establish a secret key is the following method:

1. Alice and Bob agree on public parameters: the curve E, over the finte field, the prime p, the basepoint P, and the points $A = N_A P$ and $B = N_B P$.
2. While they keep secret the parameters: the integers N_A (Alice's), and N_B (Bob's).
3. Alice gets the key as follows: $k_A = B \cdot N_A$.
4. Bob gets the key as follows: $k_B = A \cdot N_B$. Notice that they have the same key, namely $k_A = k_B$.

Exercise 6

Exercise

Your task is to a compute a session key in the DHKE protocol based on elliptic curves. Your private key is $a = 6$. *You receive Bob's public key* $B = (5, 9)$. *The elliptic curve being used is defined by*

$$y^2 \equiv x^3 + x + 6 \bmod 11$$

Solution

$k = aB = 6(5, 9)$

$$\begin{array}{c|r} 1 & B = (5,9) \\ 1 & 2B + B = 2(5,9) + (5,9) = (7,2) \\ 0 & 3B + 3B = 2(7,2) = (2,7) \end{array}$$

Exercise 7

Exercise

Alice and Bob exchange a session key using the Diffie-Hellman protocol. They publish an elliptic curve $E : y^2 \equiv x^3 + 3x + 5 \pmod{11}$*. This curve has* $N = 9$ *points. They also publish* $P = (1, 3)$*.*
Alice sends the message $A = aP = (0, 7)$ *and receives the message* $B = bP = (0, 4)$*.*

1. *Verify that* P *is a primitive generator.*
2. *Enumerate the points of the curve.*
3. *Compute* b *using the Baby Step, Giant Step algorithm.*
4. *Compute the session key.*

Exercise 7

Solution

[1] The number of points $N = 9 = 3^2$ *is not prime. If* P *is primitive, it has order 9, which implies that* $(9/3)P = 3P \neq \infty$ *Here we have:*

$$2P = 2(1,3) = (10,10)$$
$$3P = 2P + P = (4,2)$$

P *is primitive.*

Exercise 7

Solution

[2]

x	$y^2 \equiv a \pmod{11}$	$a^{\frac{p-1}{2}} \pmod{11}$	$y \equiv a^{\frac{p+1}{4}} \pmod{11}$
0	5	1	± 4
1	9	1	± 3
2	8	-1	$-$
3	8	-1	$-$
4	4	1	± 9
5	2	-1	$-$
6	8	-1	$-$
7	6	-1	$-$
8	2	-1	$-$
9	2	-1	$-$
10	1	1	± 1
∞	$-$	$-$	∞

Exercise 7

Solution

The points are:

$$(0,4),(0,7),(1,3),(1,8),(4,2),(4,9),(10,1),(10,10),\infty$$

[3] We use the baby step, giant step algorithm. We choose $M = \lceil \sqrt{9} \rceil = 3$*. We compute*

$$-MP = 3(-P) = 3(1,8) = (4,9)$$

and build the table:

i,j	iP	$B - jMP = B + j(-MP)$
0	∞	$(0,4)$
1	$(1,3)$	$(0,4)+(4,9)=(1,3)$
2	$(10,10)$	$\dots$
3	$(4,2)$	$\dots$

Exercise 7

Solution

We find out that $iP = Q - jMP \rightarrow P = B - 1 \cdot 3P$*, therefore* $B = (1+3)P = 4P$ *and* $b = 4$*.*

[4] The session key is the point $K = bA = 4(0,7) = (10,10)$*.*

Exercise 8

Exercise

Consider the elliptic curve E:

$$E : y^2 \equiv x^3 + x + 1 \pmod{11}$$

where we choose the point $P = (4, 5)$. *The curve has 14 points.*
Alice and Bob use the ECDHKE. Alice chooses the secret number $a = 3$ *e receives from Bob the point* $B = bP = (2, 0)$. *At the end of the protocol, Alice and Bob have a secret,* S*, with coordinates* (x_S, y_S). *From that point they obtain a secret key,* k*, computed as follows:*

$$k = 2x_S + (y_S \bmod 2)$$

if $S = \infty$*, then* $k = 22$.

Exercise 8

Exercise

1. *Find, if there exist, the points with coordinate $x = 5$ and $x = 8$. Use the square root formula.*
2. *Compute the order of P.*
3. *Compute the point A sent by Alice.*
4. *Compute the key at the end of the exchange.*
5. *Using Pohlig–Hellman algorithm, compute b.*
6. *Given the point B from Bob, how many keys is it possible to obtain? Specify which are they.*

Exercise 8

Solution

1 *For* $x = 5$*, we have* $y^2 = 10$*. Since* $10^5 \bmod 11 = -1$*, there aren't square roots.*
For $x = 8$*, we have* $y^2 = 4$*. Since* $4^5 \bmod 11 = 1$*, there are two points with coordinate* $y = 4^3 \bmod 11 = \pm 2$*.*

2 *The order of* P *could be 2, 7, 14.*

$$2P = (6, 5)$$
$$7P = (2, 0)$$

So the order is 14.

3 $A = aP = 3(4, 5) = (1, 6)$

4 $S = aB = 3(2, 0) = (2, 0)$ *from that* $k = 4$

Exercise 8

Solution

5 $O = 2 \cdot 7 = 14$

$$O_i = O/q_i^{e_i} \rightarrow O_1 = 14/2 = 7, \quad O_2 = 14/7 = 2$$

$$y_i = O_i^{-1} \bmod q_i^{e_i} \rightarrow y_1 = 7^{-1} \bmod 2 = 1, \quad y_2 = 2^{-1} \bmod 7 = 4$$

$$O_1 B = a_1 O_1 P \rightarrow 7B = a_1 \cdot 7P \rightarrow (2,0) = a_1(2,0) \rightarrow a_1 = 1$$

$$O_2 B = a_2 O_2 P \rightarrow 2B = a_2 \cdot 2P \rightarrow \infty = a_2(6,5) \rightarrow a_2 = 0$$

$$b = \sum_i a_i O_i y_i \bmod O \rightarrow b = 1 \cdot 7 \cdot 1 + 0 \cdot 2 \cdot 4 \bmod 14 = 7$$

6 *The order of B is 2, so there are two possible keys.*

ECIES

Alice wants to send a message m to Bob. First, Bob establishes his public key. He chooses an Elliptic Curve E over a finite field $\mathcal{F}_q$ and a point A on E of large prime order N. He then chooses a secret integer s and computes $B = sA$. The public key is (q, E, N, A, B). The private key is s. The algorithm also needs two cryptographic hash functions, H_1 and H_2, and a symmetric encryption function E_k that are publicly agreed upon.

To encrypt and send her message, Alice does the following:

1. Downloads Bob's public key.
2. Chooses a random integer k with $1 \leq k \leq N - 1$.
3. Computes $R = kA$ and $Z = kB$.
4. Writes the output of $H_1(R, Z)$ as $k_1 \| k_2$, where k_1 and k_2 have specified lengths.
5. Computes $C = E_{k_1}(m)$ and $t = H_2(C, k_2)$.
6. Sends (R, C, t) to Bob.

ECIES

To decrypt, Bob does the following:

1. Computes $Z = sR$, using his knowledge of the secret key s.
2. Computes $H_1(R, Z)$ and writes the output as $k_1 \| k_2$.
3. Computes $H_2(C, k_2)$. If it does not equal t, Bob stops and rejects the ciphertext. Otherwise, he continues.
4. Computes $m = D_{k_1}(C)$, where D_{k_1} is the decryption function for E_{k_1}.

Exercise 9

Exercise

Alice uses the ECIES cryptosystem. She publishes the elliptic curve E:

$$E : y^2 = x^3 + 3x - 1 \pmod{23}$$

which has $N = 33$ points, and the base point $A = (2, 6)$. Alice chooses the secret number $a = 4$ and publishes the point $B = aA = (14, 5)$.
To compute the session key, Bob chooses a nonce k and computes $R = kA = (21, 13)$ and $S = kB$. The point S si the session key. Bob sends to Alice the point R and the message m, ciphered with the session key.

1. *Compute the curve points corresponding to $x = 4, 9, 16$.*
2. *Compute the order of A.*
3. *Write the formulas used by Alice to compute the session key and then find it.*
4. *Compute k by using PH.*

Exercise 9

Solution

[1]

x	$y^2 \equiv a \pmod{23}$	$a^{\frac{p-1}{2}} \pmod{23}$	$y \equiv a^{\frac{p+1}{4}} \pmod{23}$
4	6	1	± 11
9	19	-1	$-$
16	3	1	± 7

[2] The order of A could be 3, 11 or 33.
Thus, $3(2,6) = (8,12)$, $11(2,6) = (1,7)$. *Then, the order is 33.*

[3] $S = kB = kaA = aR = 4(21,13) = (20,3)$.

Exercise 9

Solution

[4] $O = 3 \cdot 11 = 33,$

$$O_i = O/q_i^{e_i} \rightarrow O_1 = 33/3 = 11, \quad O_2 = 33/11 = 3$$

$$y_i = O_i^{-1} \bmod q_i^{e_i} \rightarrow y_1 = 11^{-1} \bmod 3 = 2, \quad y_2 = 3^{-1} \bmod 11 = 4$$

$$O_1 S = a_1 O_1 B \rightarrow 11S = a_1 \cdot 11B \rightarrow \infty = a_1(1,7) \rightarrow a_1 = 0$$

$$O_2 S = a_2 O_2 B \rightarrow 3S = a_2 \cdot 3B \rightarrow (21,13) = a_2(21,13) \rightarrow a_2 = 1$$

$$k = \sum_i a_i O_i y_i \bmod O \rightarrow k = 0 \cdot 11 \cdot 2 + 1 \cdot 3 \cdot 4 \bmod 33 = 12$$