Elliptic Curve Cryptography

DR. ODELU VANGA

COMPUTER SCIENCE AND ENGINEERING

INDIAN INSTITUTE OF INFORMATION TECHNOLOGY SRI CITY

Elliptic Curve

- Let a ∈ $\mathbb{R}$, b ∈ $\mathbb{R}$, be constants such that

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

A *non-singular elliptic curve* is the set *E* of solutions (x, y) ∈ $\mathbb{R}$ x $\mathbb{R}$ to the equation:

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

together with a special point *O* called the ***point at infinity***.

3 Cases for Solutions

Suppose P, Q ∈ *E*, where $P = (x_1,y_1)$ and $Q = (x_2,y_2)$, we must consider three cases:

1). $x_1 \neq x_2$

2). $x_1 = x_2$ and $y_1 = - y_2$

3). $x_1 = x_2$ and $y_1 = y_2$

Graphical Representation JCryptool

These cases must be considered when defining "addition" for our solution set

Defining Addition on *E*

Case 1:

For the case $x_1 \neq x_2$, addition is defined as follows:

$$\underset{P}{(x_1,y_1)} + \underset{Q}{(x_2,y_2)} = \underset{R}{(x_3,y_3)} \in E$$ where

$x_3 = \lambda^2 - x_1 - x_2$

$y_3 = \lambda(x_1 - x_3) - y_1$, and

$\boxed{\lambda = (y_2 - y_1) / (x_2 - x_1)}$

Defining Addition on E

$P = (x, y)$
$-P = (x, -y)$

Case 2:

For the case $x_1 = x_2$ and $y_1 = - y_2$, addition is defined as follows:

$P \quad + \quad Q \qquad R$

$$(x_1,y_1) + (x_2,y_2) = (x_3,y_3) \in E \text{ where}$$

$P \qquad -P \qquad O$

$(x,y) + (x,-y) = O$, the point at infinity

$P + -P = O$ - identity element.

Defining Addition on E

Case 3:

For the case $x_1 = x_2$ and $y_1 = y_2$, addition is defined as follows:

$P = Q$

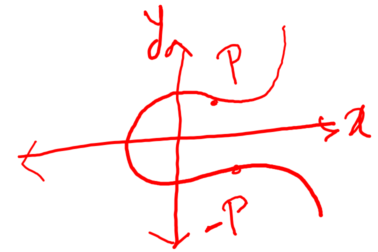
$$\overset{P}{(x_1,y_1)} + \overset{Q}{(x_2,y_2)} = \overset{R}{(x_3,y_3)} \in E, \text{ where}$$

$$x_3 = \lambda^2 - x_1 - x_2$$

$$y_3 = \lambda(x_1 - x_3) - y_1, \text{ and}$$

$$\boxed{\lambda = (3x_1^2 + a) / 2y_1}$$

Defining the Identity



- The point at infinity O, is the identity element.

  $P + O = O + P = P$, for all $P \in E$.

- From Case 2, and the Identity Element, we now have the **existence of inverses**

- Beyond the scope here to prove that we have commutativity and associativity as well

- Therefore, the set of solutions E, forms an Abelian group

Elliptic Curves modulo p

Let $p > 3$ be prime.

The elliptic curve $y^2 = x^3 + ax + b$ over $\mathbb{Z}_p$ is the set of solutions $(x,y) \in \mathbb{Z}_p \times \mathbb{Z}_p$ to the congruence:

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

where $a \in \mathbb{Z}_p$, $b \in \mathbb{Z}_p$, are constants such that

$4a^3 + 27b^2 \not\equiv 0 \pmod{p}$, together with

a special point O called the *point at infinity*.

Solutions still form an Abelian group

Example

Elliptic curve: $y^2 = x^3 + x + 6$ over $\mathbb{Z}_{11}$

X	0	1	2	3	4	5	6	7	8	9	10
$x^3 + x + 6 \bmod 11$	6	8	5	3	8	4	8	4	9	7	4
QR?	N	N	Y	Y	N	Y	N	Y	Y	N	Y
Y			4,7	5,6		2,9		2,9	3,8		2,9

Generating our group

Elliptic curve: $y^2 = x^3 + x + 6$ over $\mathbb{Z}_{11}$

- From the previous chart, and including the point at infinity *O*, we have **a group with 13 points**.
- Since the O(*E*) is prime, the group is cyclic.
- We can generate the group by choosing any point other then the point at infinity.
- Let our generator P = (2,7)

Case 1: For the case $x_1 \neq x_2$, addition is defined as follows:

$(\overset{P}{x_1,y_1}) + (\overset{Q}{x_2,y_2}) = (\overset{R}{x_3,y_3}) \in E$ where

$x_3 = \lambda^2 - x_1 - x_2$ and $y_3 = \lambda(x_1 - x_3) - y_1$ and $\lambda = (y_2 - y_1) / (x_2 - x_1)$

P = (2,7) $= (x_1, y_1)$
Q = (5,2) $= (x_2, y_2)$

R = (8,3) $= (x_3, y_3)$

Elliptic curve: $y^2 = x^3 + x + 6$ over $\mathbb{Z}_{11}$

$$\lambda = \frac{2-7}{5-2} = \frac{-5}{3} = 6 \times 3^{-1} \bmod 11$$
$$= 6 \times 4 \bmod 11$$
$$= 2$$

$$x_3 = 2^2 - 2 - 5$$
$$= 4 - 7$$
$$= -3 \bmod 11$$
$$= 8$$

$$y_3 = 2(2-8) - 7 \pmod{11}$$
$$= -12 - 7 \pmod{11}$$
$$= -19 \pmod{11}$$
$$= 3$$

$$\boxed{(2,7) + (5,2) = (8,3)}$$

Case 2: For the case $x_1 = x_2$ and $y_1 = - y_2$, addition is defined as follows:

$(x_1,y_1) + (x_2,y_2) = (x_3,y_3) \in E$ where

$(x,y) + (x,-y) = O$, the point at infinity

P = (2,7)
-P = (2, -7) = (2, 5)

$\boxed{P + (-P) = O}$

Elliptic curve: $y^2 = x^3 + x + 6$ over $\mathbb{Z}_{11}$

Case 3: For the case $x_1 = x_2$ and $y_1 = y_2$, addition is defined as follows:

P = (2,7)
2P = (5,2)

$(x_1,y_1) + (x_2,y_2) = (x_3,y_3) \in E$, where

$x_3 = \lambda^2 - x_1 - x_2$ and $y_3 = \lambda(x_1 - x_3) - y_1$, and $\lambda = (3x_1^2 + a) / 2y_1$

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

Elliptic curve: $y^2 = x^3 + x + 6$ over $\mathbb{Z}_{11}$

$P = (2,7)$, $Q = (2,7)$, $P + Q = P + P = 2P$

$\lambda = (3 \times 2^2 + 1) / (2 \times 7)$

$= (13) \times (14)^{-1} \bmod 11$

$= 2 \times 3^{-1} \bmod 11$

$= 2 \times 4 \bmod 11$

$= 8$

$x_3 = 8^2 - 2 - 2$

$= 60 \bmod 11 = 5$

$y_3 = 8(2-5) - 7 \bmod 11$

$= 8(-3) - 7 \bmod 11$

$= 8(8) + 4 \bmod 11$

$= 68 \bmod 11$

$= 2$

$\boxed{P + P = 2P = (2,7) + (2,7) = (5,2)}$

Double-and-Add

Choose a large random secret : K

$K = 10$, $KP \Leftarrow$ Scalar point multiplication.

Given $K, P \Rightarrow KP$ is easy.

ECDLP : Given KP, P

finding $\underline{\underline{K}}$

$$\left.\begin{array}{l}\underbrace{P + P + P + \cdots + P}_{KP-}\end{array}\right\} O(\log K)$$

$\log K$

$(10) = 1010$

$$\left.\begin{array}{l}2P = P + P \\ 4P = 2P + 2P \\ 8P = 4P + 4P\end{array}\right\}$$

$10P = 2P + 8P$

$\underline{1 \times 2^3} + 0 \times 2^2 + \underline{1 \times 2^1} + 0 \times 2^0$

EC Group

Hasse's theorem on elliptic curves gives us, including the point at infinity, where E defined over $K = F_q$

$$|\#E(K) - (q+1)| \le 2\sqrt{q}$$

We can generate this by using the rules of addition we defined earlier where 2P = P + P

O

P = (2,7)	2P = (5,2)	3P = (8,3)
4P = (10,2)	5P = (3,6)	6P = (7,9)
7P = (7,2)	8P = (3,5)	9P = (10,9)
10P = (8,8)	11P = (5,9)	12P = (2,4)

Home work:

$y^2 = x^3 + 10x + 15$ over Z_{23}.

$P = (5,12)$

$\Rightarrow ?$ $2P = P + P$

$\Rightarrow ?$ $17P = ?$

Sources Used

"Recommended Elliptic Curves For Federal Government Use" July 1999

Cryptography Theory and Practice. Douglas Stinson, 3rd ed

A Friendly Introduction to Number Theory. Joseph Silverman, 3rd ed

Elements of Modern Algebra. Gilbert and Gilbert, 6th edition