Elliptic Curves in Crypto, part I

The discrete logarithm problem in $\mathbb{Z}_p$

Problem Instance $I = (p, \alpha, \beta)$, where p is prime, $\alpha \in \mathbb{Z}_p$ is a primitive element, and $\beta \in \mathbb{Z}_p^*$.
Objective Find the unique integer a, $0 \leq a \leq p-2$, such that $$\alpha^a \equiv \beta \pmod{p}.$$
We will denote this integer a by $\log_\alpha \beta$.

ECDL analog

$I = (E, P, Q)$

E elliptic curve

$P, Q \in E$, points

Find k such that $Q = kP$

k integer

The Generalized Discrete Logarithm Problem

- Given is a finite cyclic group G with the group operation $\circ$ and cardinality n.
- We consider a primitive element $\alpha \in G$ and another element $\beta \in G$.
- The discrete logarithm problem is finding the integer x, where $1 \leq x \leq n$, such that:

$$\beta = \underbrace{\alpha \circ \alpha \circ \alpha \circ \ldots \circ \alpha}_{x \text{ times}} = \alpha^x$$

or, in additive notation
x int, $\alpha, \beta \in G$

$$\beta = \alpha + \alpha + \ldots + \alpha$$
$$= x\alpha$$

$x, \alpha \longrightarrow x\alpha, \beta$ easy

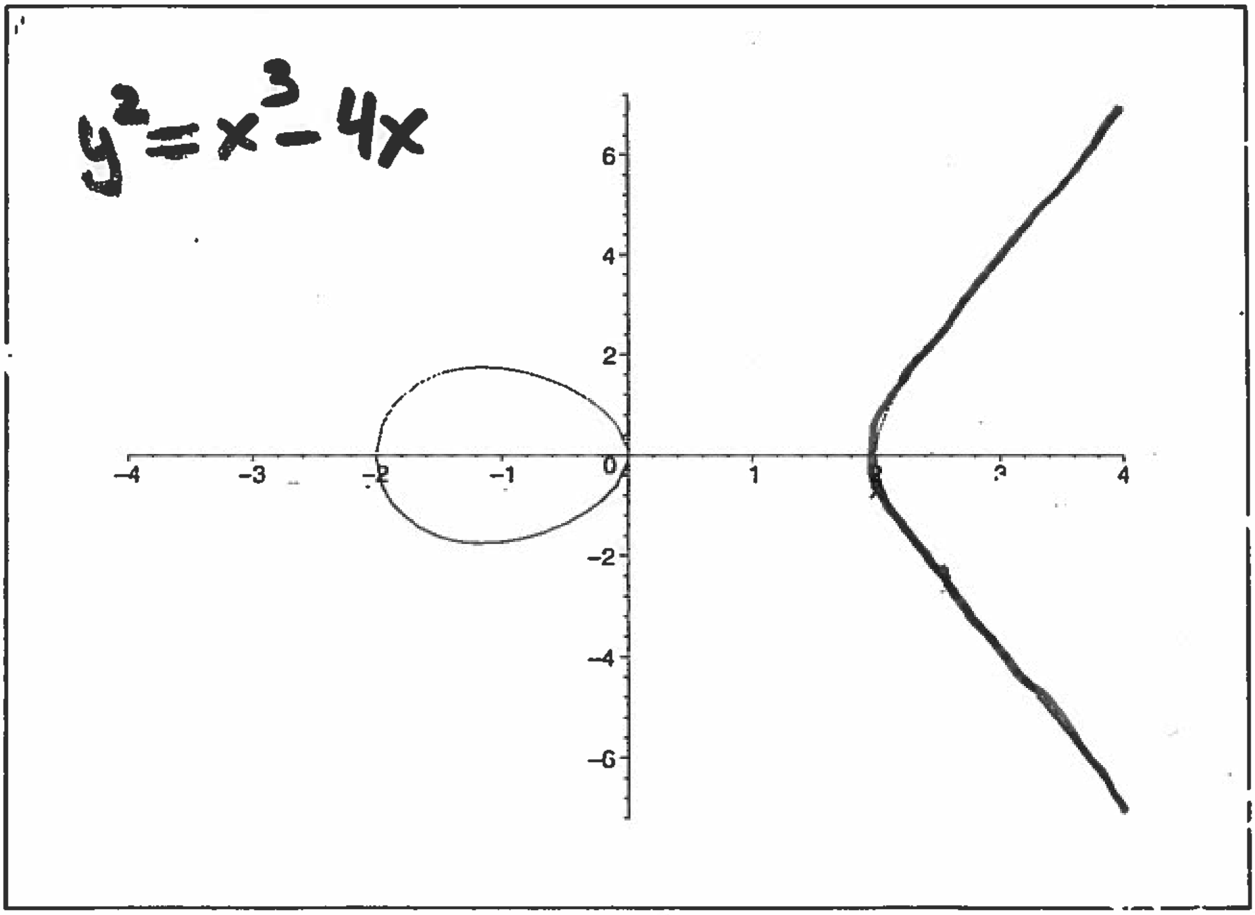
$\alpha, \beta \longrightarrow x$ infeasible to compute

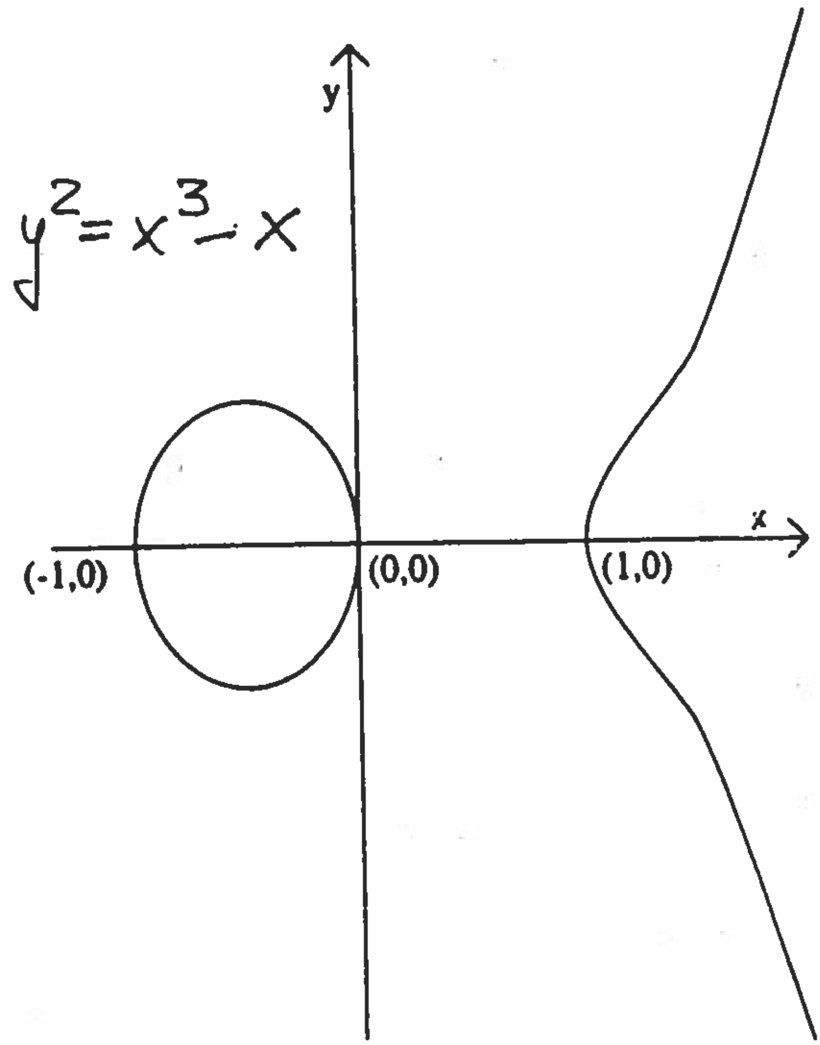
Elliptic Curves over the Reals

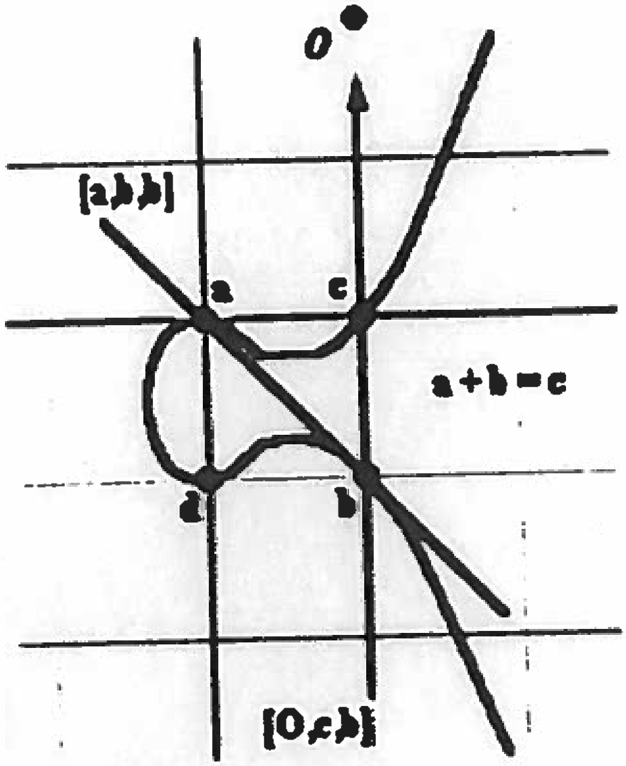
Definition 6.3: Let $a, b \in \mathbb{R}$ be constants such that $4a^3 + 27b^2 \neq 0$. A *non-singular elliptic curve* is the set E of solutions $(x, y) \in \mathbb{R} \times \mathbb{R}$ to the equation

$$y^2 = x^3 + ax + b, \tag{6.4}$$

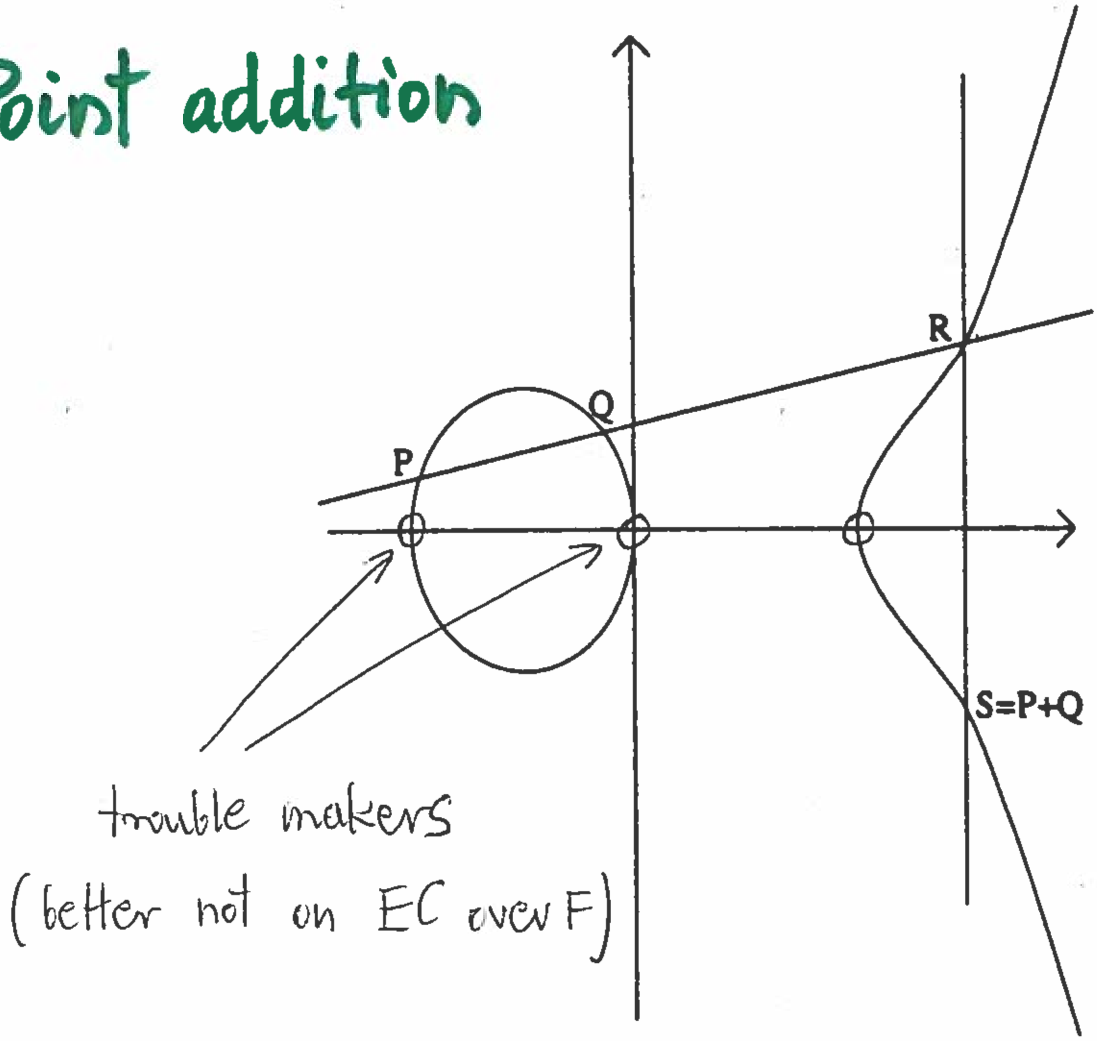
together with a special point $\mathcal{O}$ called the *point at infinity*.




$y^2 = x^3 - x$
y
x
(-1,0)
(0,0)
(1,0)


O
[a,b,b]
a
c
a+b=c
d
b
[O,c,b]

Point addition



Elliptic Curves Modulo a Prime

Definition 6.4: 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

$$y^2 \equiv x^3 + ax + b \pmod{p}, \tag{6.6}$$

where $a, b \in \mathbb{Z}_p$ are constants such that $4a^3 + 27b^2 \not\equiv 0 \pmod{p}$, together with a special point $\mathcal{O}$ called the *point at infinity*.

$P = (x_1, y_1)$ $\qquad$ $Q = (x_2, y_2)$

If $x_2 = x_1$ and $y_2 = -y_1$, then $P + Q = \mathcal{O}$;

$P + Q = (x_3, y_3)$, where

$$x_3 = \lambda^2 - x_1 - x_2$$
$$y_3 = \lambda(x_1 - x_3) - y_1,$$

$$\lambda = \begin{cases} (y_2 - y_1)(x_2 - x_1)^{-1}, & \text{if } P \neq Q \\ (3{x_1}^2 + a)(2y_1)^{-1}, & \text{if } P = Q. \end{cases}$$

$$P + \mathcal{O} = \mathcal{O} + P = P$$

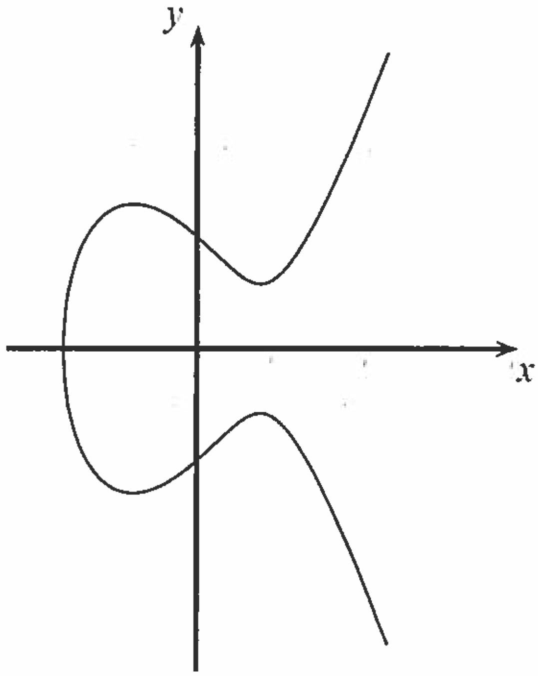
Computations on Elliptic Curves (ctd.)

- In cryptography, we are interested in elliptic curves module a prime p:

> ***Definition: Elliptic Curves over prime fields***
>
> *The elliptic curve over Z_p, $p>3$ is the set of all pairs $(x,y) \in Z_p$ which fulfill*
>
> $$y^2 = x^3 + ax + b \bmod p$$
>
> *together with an imaginary point of infinity θ, where $a,b \in Z_p$ and the condition*
>
> $$4a^3+27b^2 \neq 0 \bmod p.$$

- Note that $Z_p = \{0,1,\ldots, p-1\}$ is a set of integers with modulo p arithmetic

∈



$$
\begin{tikzcd}
4a^3 + 27b^2 \arrow[r, "=0"] \arrow[d, "\neq 0"] & \text{singular EC} \\
\text{6.4 has 3 differcnt rots in } \mathbb{C} &
\end{tikzcd}
$$

Defining $P+Q$

Suppose $P, Q \in E$, where $P = (x_1, y_1)$ and $Q = (x_2, y_2)$. We 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 $y_1 = y_2$

In case 1, we define L to be the line through P and Q. L intersects E in the two points P and Q, and it is easy to see that L will intersect E in one further point, which we call R'. If we reflect R' in the x-axis, then we get a point which we name R. We define $P + Q = R$.

O – infinity, $P + O = O + P = P$

Let's work out an algebraic formula to compute R. First, the equation of L is $y = \lambda x + \nu$, where the slope of L is

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

and

$$\nu = y_1 - \lambda x_1 = y_2 - \lambda x_2.$$

In order to find the points in $E \cap L$, we substitute $y = \lambda x + \nu$ into the equation for E, obtaining the following:

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

which is the same as

$$x^3 - \lambda^2 x^2 + (a - 2\lambda\nu)x + b - \nu^2 = 0. \tag{6.5}$$

The roots of equation (6.5) are the x-co-ordinates of the points in $E \cap L$. We already know two points in $E \cap L$, namely, P and Q. Hence x_1 and x_2 are two roots of equation (6.5).

Since equation (6.5) is a cubic equation over the reals having two real roots, the third root, say x_3, must also be real. The sum of the three roots must be the negative of the coefficient of the quadratic term, or λ^2. Therefore

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

x_3 is the x-co-ordinate of the point R'. We will denote the y-co-ordinate of R' by $-y_3$, so the y-co-ordinate of R will be y_3. An easy way to compute y_3 is to use the fact that the slope of L, namely λ, is determined by any two points on L. If we use the points (x_1, y_1) and $(x_3, -y_3)$ to compute this slope, we get

$$\lambda = \frac{-y_3 - y_1}{x_3 - x_1},$$

or

$$y_3 = \lambda(x_1 - x_3) - y_1.$$

Therefore we have derived a formula for $P + Q$ in case 1: if $x_1 \neq x_2$, then $(x_1, y_1) + (x_2, y_2) = (x_3, y_3)$, where

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

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

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

Vieta's Formulas

Wolfram

DOWNLOAD *Mathematica* Notebook   CONTRIBUTE To this Entry

Let s_i be the sum of the products of distinct polynomial roots r_j of the polynomial equation of degree n

$$a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0 = 0, \qquad (1)$$

where the roots are taken i at a time (i.e., s_i is defined as the symmetric polynomial $\Pi_i(r_1, \ldots, r_n)$) s_i is defined for $i = 1, \ldots, n$. For example, the first few values of s_i are

$$s_1 = r_1 + r_2 + r_3 + r_4 + \ldots \qquad (2)$$

$$s_2 = r_1 r_2 + r_1 r_3 + r_1 r_4 + r_2 r_3 + \ldots \qquad (3)$$

$$s_3 = r_1 r_2 r_3 + r_1 r_2 r_4 + r_2 r_3 r_4 + \ldots, \qquad (4)$$

and so on. Then Vieta's formulas states that

$$s_i = (-1)^i \frac{a_{n-i}}{a_n}. \qquad (5)$$

The theorem was proved by Viète (also known as Vieta, 1579) for positive roots only, and the general theorem was proved by Girard.

Case 2, where $x_1 = x_2$ and $y_1 = -y_2$, is simple: we define $(x, y) + (x, -y) = \mathcal{O}$ for all $(x, y) \in E$. Therefore (x, y) and $(x, -y)$ are inverses with respect to the elliptic curve addition operation.

Case 3 remains to be considered. Here we are adding a point $P = (x_1, y_1)$ to itself. We can assume that $y_1 \neq 0$, for then we would be in case 2. Case 3 is handled much like case 1, except that we define L to be the tangent to E at the point P. A little bit of calculus makes the computation quite simple. The slope of L can be computed using implicit differentiation of the equation of E:

$$2y\frac{dy}{dx} = 3x^2 + a.$$

Substituting $x = x_1, y = y_1$, we see that the slope of the tangent is

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

The rest of the analysis in this case is the same as in case 1. The formula obtained is identical, except that λ is computed differently.

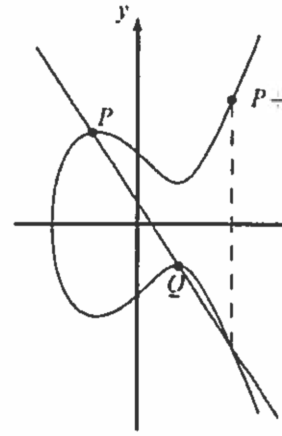
Computations on Elliptic Curves (ctd.)

- Generating a *group of points* on elliptic curves based on point addition operation *P+Q = R, i.e.,* $(x_P,y_P)+(x_Q,y_Q) = (x_R,y_R)$
- Geometric Interpretation of point addition operation
  - *Draw straight line through P and Q; if P=Q use tangent line instead*
  - *Mirror third intersection point of drawn line with the elliptic curve along the x-axis*
- Elliptic Curve Point Addition and Doubling Formulas

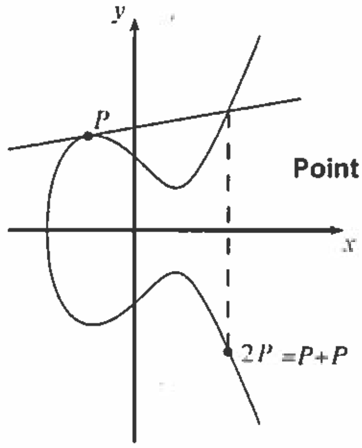
$$x_3 = s^2 - x_1 - x_2 \bmod p \quad \text{and} \quad y_3 = s(x_1 - x_3) - y_1 \bmod p$$

where

$$s = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1} \bmod p & ; \text{if } P \neq Q \text{ (point addition)} \\ \dfrac{3x_1^2 + a}{2y_1} \bmod p & ; \text{if } P = Q \text{ (point doubling)} \end{cases}$$



Point Addition



Point Doubling

$\mathbb{Z}_{11}$

Example 6.7 Let E be the elliptic curve $y^2 = x^3 + x + 6$ over $\mathbb{Z}_{11}$.

$11 \equiv 3 \bmod 4$

$$\pm z^{(11+1)/4} \bmod 11 = \pm z^3 \bmod 11. = \sqrt{z} \bmod 11$$

in action in secp256k1

x	$x^3 + x + 6 \bmod 11$	quadratic residue?	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

$$\begin{array}{lll lll lll}
\alpha &=& (2,7) & 2\alpha &=& (5,2) & 3\alpha &=& (8,3) \\
4\alpha &=& (10,2) & 5\alpha &=& (3,6) & 6\alpha &=& (7,9) \\
7\alpha &=& (7,2) & 8\alpha &=& (3,5) & 9\alpha &=& (10,9) \\
10\alpha &=& (8,8) & 11\alpha &=& (5,9) & 12\alpha &=& (2,4)
\end{array}$$

Example: Let E be the elliptic curve $y^2 = x^3 + x + 1$ over Z_{17}. Lets find the points on E.

x	$x^3 + x + 1$	quad. residue?	y
0	1	yes	1,16
1	3	no	
2	11	no	
3	14	no	
4	1	yes	1,16
5	12	no	
6	2	yes	6,11
7	11	no	
8	11	no	
9	8	yes	5,12
10	8	yes	5,12
11	0	DNA	0
12	7	no	
13	1	yes	1,16
14	5	no	
15	8	yes	5,12
16	16	yes	4,13

Thus E has 18 points on it. They are { (0, 1), (0, 16), (4, 1), (4, 16), (6, 6), (6, 11), (9, 5), (9, 12), (10, 5), (10, 12), (11, 0), (13, 1), (13, 16), (15, 5), (15, 12), (16, 4), (16, 13), O }.

infinity

Is E cyclic?

18 elements

Elliptic curve $y^2 = x^3 + x + 1$ example cont'd:

Let α =(0, 1). We compute the multiples of α.

$\alpha = (0, 1)$	$10\alpha = (15, 5)$
$2\alpha = (13, 1)$	$11\alpha = (6, 11)$
$3\alpha = (4, 16)$	$12\alpha = (10, 5)$
$4\alpha = (9, 12)$	$13\alpha = (16, 13)$
$5\alpha = (16, 4)$	$14\alpha = (9, 5)$
$6\alpha = (10, 12)$	$15\alpha = (4, 1)$
$7\alpha = (6, 6)$	$16\alpha = (13, 16)$
$8\alpha = (15, 12)$	$17\alpha = (0, 16)$
$9\alpha = (11, 0)$	$18\alpha = \mathcal{O}$

We can now compute an example of the ElGamal encryption using this elliptic curve:

Suppose that $\alpha = (0, 1)$ and Bob's secret exponent is $a = 5$, so

$$\beta = 5\alpha = (16, 4).$$

Encryption is

$$e_K(x, k) = (k(0, 1), x + k(16, 4))$$

where $x \in E$ and $0 \leq k \leq 17$.

Decryption is

$$d_K(y_1, y_2) = y_2 - 5y_1$$

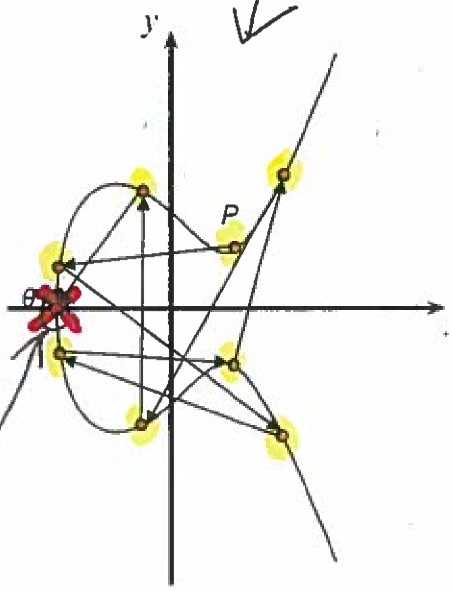
Try encrypting and decrypting the message (15, 12).

Computations on Elliptic Curves (ctd.)

$y^2 = x^3 + 2x + 2$ over $\mathbb{Z}_{17}$

- The points on an elliptic curve and the point at infinity θ form cyclic subgroups

$2P = (5,1)+(5,1) = (6,3)$
$3P = 2P+P = (10,6)$
$4P = (3,1)$
$5P = (9,16)$
$6P = (16,13)$
$7P = (0,6)$
$8P = (13,7)$
$9P = (7,6)$
$10P = (7,11)$
$11P = (13,10)$
$12P = (0,11)$
$13P = (16,4)$
$14P = (9,1)$
$15P = (3,16)$
$16P = (10,11)$
$17P = (6,14)$
$18P = (5,16)$
$19P = \theta$



This elliptic curve has order #E = |E| = 19 since it contains 19 points in its cyclic group.

$P = (5,1)$

better draw it at ∞

another example

$$\text{POINTCOMPRESS}(P) = (x, y \bmod 2), \text{ where } P = (x, y) \in E.$$

$$\text{POINTCOMPRESS} : E \backslash \{O\} \to \mathbb{Z}_p \times \mathbb{Z}_2,$$

$$p \equiv 3 \bmod 4 \implies y = z^{(p+1)/4} \bmod p$$

Algorithm 6.4: POINTDECOMPRESS(x, i)

$z \leftarrow x^3 + ax + b \bmod p$
if z is a quadratic non-residue modulo p
  then return ("failure")
  else $\begin{cases} y \leftarrow \sqrt{z} \bmod p \\ \textbf{if } y \equiv i \pmod 2 \\ \quad \textbf{then return } (x, y) \\ \quad \textbf{else return } (x, p - y) \end{cases}$

HP: US patent 6252960 B1 1998
expires in 2018

130+ crypto and EC patents:
NSA, Certicom, RSA Security, HP, Harris