Elliptic Curves over Reals

Note Title 4/24/2012

Let $a, b \in \mathbb{R}$ be const. s.t. $4a^3 + 27b^2 \neq 0$

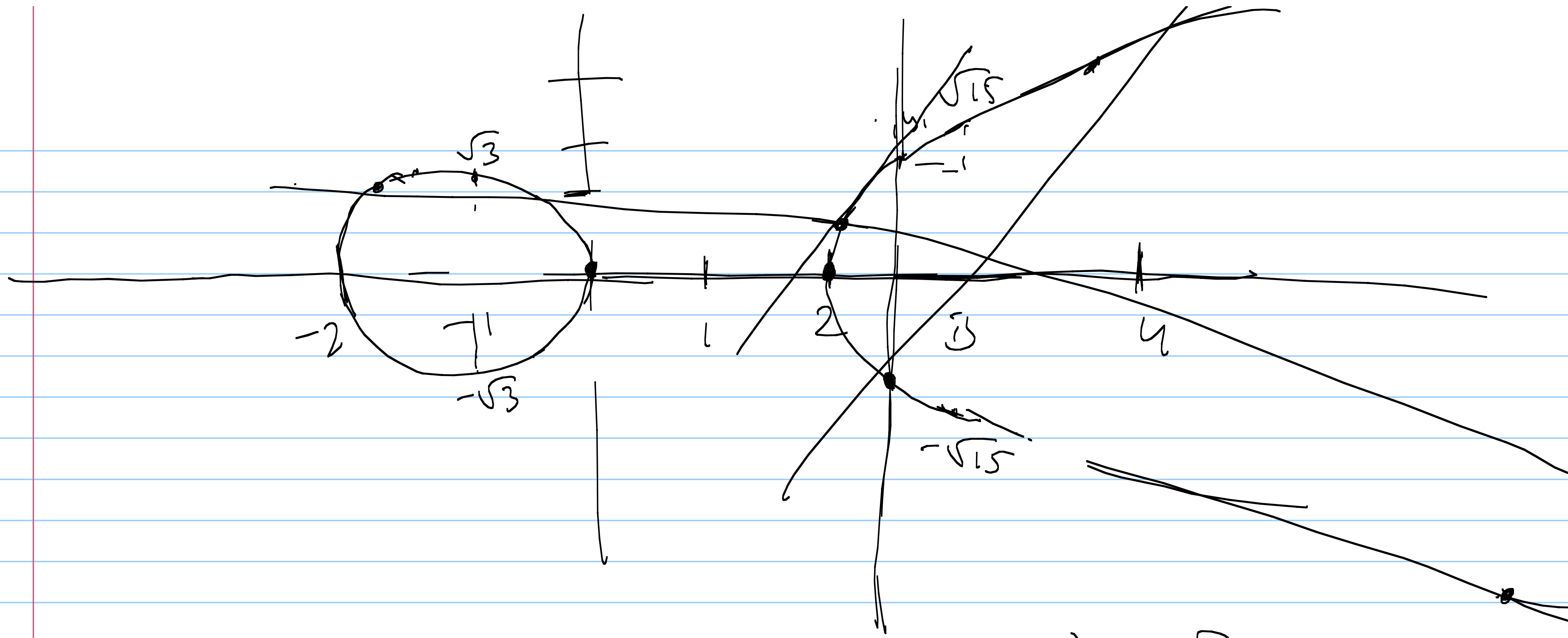
A non-singular E.C. is the set E of solutions $(x, y) \in \mathbb{R} \times \mathbb{R}$ to the equation

$$\boxed{y^2 = x^3 + ax + b}$$

plus special point $\mathcal{O}$ called the point at infinity.

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

$(x, y) \in E \Rightarrow (x, -y) \in E$ $\quad (2, 0) \in E$



$$(x,y) \in E \Rightarrow (x,-y) \in E$$

Define binary op. '$+$' to make $(E, +)$ Abelian group. We will assume that 'O' is the identity element of the group.

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

cases to consider:

1) $x_1 \neq x_2$
2) $x_1 = x_2$ & $y_1 = -y_2$
3) $x_1 = x_2$ & $y_1 = y_2$

Case 1: $P, Q \in E$

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

$(x_1, y_1) + (x_2, y_2) = (x_3, y_3)$

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

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

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

Case 2: $(x_1, y_1) + (x_1, -y_1) = \mathcal{O}$

case 3: $(x_1, y_1) + (x_1, y_2) = (x_3, y_3)$

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

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

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

1) Addition is closed on the set E.

2) 〃 is commutative

3) '0' is an identity element for '+'

4) Every point on E has an inverse

5) $(+)$ satisfies associativity.

$y_1 = \lambda x_1 + v$

$y_2 = \lambda x_2 + v$

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

$y_1^2 = x_1^3 + ax + 6$

$y_2^2 = x_2^3 + ax + 6$

$v = y_1 - \lambda x_1 = y_2 - \lambda x_2$

$$y_3 = \lambda x_3 + v \qquad y_3 = \lambda x_3 + v$$

$$y_3^2 = x_3^3 + ax + b \qquad \lambda($$

$$(\lambda x_3 + v)^2 = x_3^3 + ax + b$$

$$\lambda^2 x_3^2 + 2\lambda v x_3 + v^2 = x_3^3 + ax + b$$

$$\Rightarrow \quad x_3^3 - \lambda^2 x_3^2 - 2\lambda v x_3 - v^2 + ax + b = 0$$

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

Let $p>3$ be prime. E.C. $y^2 = x^3 + ax + b$ over $\mathbb{Z}_p$ is the set of solutions

$$(x, y) \in \mathbb{Z}_p \times \mathbb{Z}_p$$

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

where $a, b \in \mathbb{Z}_p$ s.t. $4a^3 + 27b^2 \neq 0 \bmod p$

plus a special point 'O' called the point at infinity.

For $P, Q \in E$ where $P = (x_1, y_1)$, $Q = (x_2, y_2)$

add(P, Q)
{ If $x_1 = x_2$ and $y_1 = -y_2$ then

return '$\mathcal{O}$'

$(x_1, y_1) + (x_1, -y_1) = \mathcal{O}$

else

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

$y_3 = \lambda(x_1 - x_3) - y_1 \pmod p$

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

return (x_3, y_3)

}

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

$\downarrow$

5rx

x	$x^3+x+6 \bmod 11$	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)

E has total 13 points including $\mathcal{O}$.

$\overline{p \equiv 3 \bmod 4}$

$x^2 \equiv a \bmod p$ if a is QR

than $x = \pm\, a^{\frac{p+1}{4}} \bmod p$

$\alpha = (2,7)$

$\alpha + \alpha = 2\alpha = (2,7) + (2,7)$

$\lambda = (3 \times 4 + 1) \cdot (2 \times 7)^{-1} = 8 \mod 1$

$x_3 = 5, \quad y_3 = 2$

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

$\alpha = (2,7)$

$2\alpha = (5,2)$

$3\alpha = (8,3)$ ..

$12\alpha = (2,4) =$

An elliptic curve E defined over $\mathbb{Z}_p$ will have 'roughly' p points,

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

Remember El-Gamal over $\mathbb{Z}_p$

choose secret α, publish $\beta = g^{\alpha}$ where g is generator of $\mathbb{Z}_p^*$

$C = E(m) =$ choose random k

$(g^k, M \cdot \beta^k)$

$Dec(c_1, c_2) = ((c_1)^{\alpha})^{-1} \cdot c_2 = m$

Analog of D.L over EC

Given α a generator of large subgroup of EC

and given z element of that subgroup

find intergor k s.t $k.\alpha = z$

Analog of El-Gamal over EC

Given E over Z_p s.t B is a generator of a large subgroup. Choose random $a \in Z_p$

and publish $a.B$ where a is secret.

$$E(P_m) = (kB,\ P_m + k(a.B))$$

$$D(C_1, C_2) = C_2 - a.C_1 = P_m$$

Example : $B = (2,7)$ $\quad a = 7$

$$\beta = 7.B = (7,2)$$

$$E(x,k) = \big(k.(2,7),\ x + k.(7,2)\big)$$

if $x = (10,9)$, $k = 3$

$$c_1 = 3.(2,7) = (8,3)$$

$$c_2 = (10,9) + 3\cdot(7,2) - (10,2)$$

$$(E, t)$$

$$(2, t)$$