

Übung :

$$y^2 \equiv x^3 + x + 1 \pmod{7}$$

teste auf gültige elliptische kurve $[4a^3 + 27b^2]$

$$P_1 = (0, 1)$$

$$P_2 = (2, 2)$$

Berechne $P_1 + P_1$

$$P_1 + P_2$$

$$P_1 + (-P_1)$$

$$\neq 0 \pmod{p}$$

$$P_1 + P_2 : P_1 \neq P_2$$

$$m \equiv \frac{y_2 - y_1}{x_2 - x_1} \pmod{p} \quad P_1 = (0, 1)$$

$$P_2 = (2, 2)$$

$$\equiv \frac{2 - 1}{2 - 0} \equiv \frac{1}{2} \equiv 4 \pmod{7}$$

$$x_3 \equiv m^2 - x_1 - x_2 \equiv 4^2 - 0 - 2 \equiv 2 - 2 \equiv 0 \pmod{7}$$

$$y_3 \equiv m(x_1 - x_3) - y_1 \equiv 4 \cdot (0 - 0) - 1 \equiv 6 \pmod{7}$$

$$\Rightarrow P_1 + P_2 \equiv (0, 6) \quad [0^3 + 0 + 1 \equiv 6^2 \pmod{7} \checkmark]$$

$$P_1 + P_1 :$$

$$m \equiv \frac{3x^2 + a}{2y} \equiv \frac{3 \cdot 0^2 + 1}{2 \cdot 1} \equiv \frac{1}{2} \equiv 4 \pmod{7}$$

$$x_3 \equiv m^2 - x_1 - x_1 \equiv 4^2 - 0 - 0 \equiv 2 \pmod{7}$$

$$y_3 \equiv m(x_1 - x_3) - y_1 \equiv 4 \cdot (0 - 2) - 1 \equiv 5 \pmod{7}$$

$$\Rightarrow P_1 + P_1 = (2, 5)$$

$$P_1 + (-P_1) = (0, 1) + (0, -1)$$

$$= (0, 1) + (0, 6) \equiv \mathcal{O}$$

$$\left. \begin{array}{l} y_1 \equiv -y_2 \\ \pmod{p} \end{array} \right\}$$

$$\begin{aligned} &= 3 \cdot 1 \equiv 4 \pmod{7} \\ &4 \cdot 1 + 2 \cdot 1^2 \\ &= 4 + 2 = 6 \end{aligned}$$

Übung:

- Arithmetik für Punkte implementieren

$$\frac{3x^2+a}{2y}, \frac{y_2-y_1}{x_2-x_1} \pmod{p} \rightarrow \text{Inverse über}$$

$$\frac{1}{x} \equiv x^{p-2} \pmod{p}$$

- Punktzahl bestimmen (s.u.)

Anzahl der Punkte auf E

$$y^2 \equiv \underbrace{x^3 + ax + b}_{\text{mod } p}$$

(x, y) \uparrow existiert y ? $0 \leq x \leq p-1$

Beispiel: $y^2 \equiv x^3 + x + 1 \pmod{7}$

x	0	1	2	3	4	5	6
y^2	1	3	4	3	6	5	6
y	± 1	—	± 2	—	—	—	—

y	y^2
0	0
1	1
2	4
3	2
4	2
5	4
6	1

-3
-2
-1

$$E = \{ (0, 1), (0, 6), (2, 2), (2, 5), \emptyset \}$$

$$|E| = 5$$

Kriterium für Quadrate mod p

p Primzahl, $1 \leq z \leq p-1$ gegeben

Frage: $y^2 \equiv z \pmod p$ lösbar?

$$z \pmod p \equiv \begin{cases} 1 & \Leftrightarrow \text{lösbar} \\ -1 \text{ (bzw } p-1) & \Leftrightarrow \text{unlösbar} \end{cases}$$

n=		
100	50/50	
	51/49	
	52/48	statistik
	53/47	63% 95%
	54/46	
	<u>70/30</u>	$\sqrt{n} / 2 \cdot \sqrt{n}$

Beispiel: finde Punkt auf Kurve

$$y^2 \equiv x^3 + 2x + 3 \pmod{13}$$

$$x=0 \rightarrow y^2 \equiv 0^3 + 2 \cdot 0 + 3 \equiv 3 \pmod{13}$$

$$y^2 \equiv z \pmod p \text{ lösbar}$$

$$\boxed{\frac{p-1}{2}} \equiv \frac{13-1}{2} \equiv 6 \equiv 3 \equiv 3^3 \equiv 3 \cdot 3 \equiv 1 \cdot 1 \equiv \boxed{1} \pmod{13}$$

$\Rightarrow y^2 \equiv 3 \pmod{13}$ lösbar $\Rightarrow y$ berechnen (?)

$(0, y)$ und $(0, -y)$ sind Punkte auf E

Punktezählalgorithmus:

n = 0 // Anzahl Punkte

for x = 0 to p-1 do

$$z = x^3 + ax + b \pmod p$$

if z = 0 then

$$n = n + 1$$

else

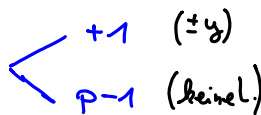
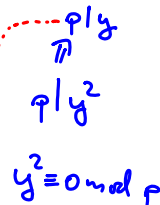
$$r \equiv z^{\frac{p-1}{2}} \pmod p$$

if r = 1 then

$$n = n + 2$$

fi

od
return n



Satz von Hasse

E elliptische Kurve mod p

$$(\sqrt{p} - 1)^2 \leq |E| \leq (\sqrt{p} + 1)^2$$

$$p - 2\sqrt{p} + 1$$

$$p + 2\sqrt{p} + 1$$

\Rightarrow Größenordnung von $|E|$ hängt nur von p ab

Zu vermeidende Attacken: Pohlig-Hellman, Pollard

\downarrow
Reduzieren auf
Primteiler q von $|E|$

\downarrow
Folge von Kurzen
Laufzeit $O(\sqrt{q})$

Konsequenz:

- $|E|$ muss mindestens einen großen Primteiler q haben

- $\sqrt{q} \geq 2^{128}$

Spezialfälle:

- $|E| = p \Rightarrow$ es gibt einen polynomiellen Algorithmus

- $|E| = p-1$ bzw. $q \mid p-1, k \leq 6 \Rightarrow$ subexp. Algorithmus