Übung:

$$y^2 \equiv x^3 + x + 1 \mod 7$$

teste auf gültige elliptische Kurve $[4a^3+27b^2] \not\equiv 0 \mod p$

$4\cdot 1^3 + 27\cdot 1^2 \equiv 31 \equiv 4 \mod 7$ ✓

$P_1 = (0,1)$

$P_2 = (2,2)$

Berechne $P_1 + P_1$

$P_1 + P_2$

$P_1 + (-P_1)$

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

$$m \equiv \frac{y_2 - y_1}{x_2 - x_1} \mod p \qquad P_1 = (0,1),\quad P_2 = (2,2)$$

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

$$x_3 \equiv m^2 - x_1 - x_2 \equiv 4^2 - 0 - 2 \equiv 2 - 2 \equiv 0 \mod 7$$

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

$$\Rightarrow P_1 + P_2 \equiv (0,6) \qquad [0^3 + 0 + 1 \equiv 6^2 \mod 7 \ ✓]$$

$P_1 + P_1$:

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

$$x_3 \equiv m^2 - x_1 - x_1 \equiv 4^2 - 0 - 0 \equiv 2 \mod 7$$

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

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

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

$$= \underbrace{(0,1) + (0,6)}_{y_1 \equiv -y_2 \mod p} \equiv \mathcal{O}$$

Übung:

- Arithmetik für Punkte implementieren

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

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

- Punktanzahl bestimmen (s.u.)

Anzahl der Punkte auf E

$$y^2 \equiv \underbrace{x^3 + ax + b}_{0 \le x \le p-1} \mod p$$

existiert y?

(x, y)

Beispiel: $y^2 \equiv x^3 + x + 1 \mod 7$

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
-3	4	2
-2	5	4
-1	6	1

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

$$|E| = 5$$

Kriterium für Quadrate mod p

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

Frage: $y^2 \equiv z \bmod p$ lösbar?

$$z^{\frac{p-1}{2}} \bmod p \equiv \begin{cases} 1 & \Leftarrow \text{lösbar} \\ -1 \ (\text{bzw } p-1) & \Leftrightarrow \text{unlösbar} \end{cases}$$

$n=$
100

50/50
51/49
52/48
53/47
54/46

70/30

Statistik
63% 95%

$\sqrt{n}$ / $2\cdot\sqrt{n}$

Beispiel: finde Punkt auf Kurve

$$y^2 \equiv x^3 + 2x + 3 \bmod 13$$

$$x = 0 \rightarrow y^2 \equiv 0^3 + 2\cdot 0 + 3 \equiv \underset{\underset{z}{\uparrow}}{3} \bmod 13$$

$y^2 \equiv z \bmod p$ lösbar

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

$\Rightarrow y^2 \equiv 3 \bmod 13$ 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 mod p
        if z = 0 then
            n = n+1
    else
            r ≡ z^((p-1)/2) mod p
            if r = 1 then
                n = n+2
            fi
od       fi
return n
```

$p \mid y$
$\Uparrow$
$p \mid y^2$

$y^2 \equiv 0 \bmod p$

$+1$ $(\pm y)$

$p-1$ (keine L.)

Satz von Hasse

E elliptische Kurve mod p

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

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

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

Zu vermeidende Attacken: Pohlig-Hellman, Pollard

Reduzieren auf Primteiler q von $|E|$ $\qquad$ Folge von Punkten Laufzeit $O(\sqrt{q})$

Konsequenz:

- $|E|$ muss mindestens einen großen Primteiler q haben
- $\sqrt{q} \geqslant 2^{128}$.

Spezialfälle:

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

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