Anzahl der Punkte auf E

Beispiele:

$p = 7$, $y^2 \equiv x^3 + x + 4 \bmod 7$, $|E| = 10$

$p = 101$, $y^2 \equiv x^3 + x + 1 \bmod 101$, $|E| = 105$

$y^2 \equiv x^3 + 3x + 7 \bmod 101$, $|E| = 91$

$p = 997$, $y^2 \equiv x^3 + 2x + 2 \bmod 997$, $|E| = 973$

$x^3 + 2x + 4 \bmod 997$, $|E| = 1048$

Satz von Hasse:

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

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

Quadratwurzeln mod p

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

zu lösen sind Gleichungen

$$y^2 \equiv z \bmod p \qquad (*)$$

für vorgegebene z.

Test, ob $(*)$ lösbar:

$$z^{\frac{p-1}{2}} \equiv \left\{ \begin{array}{c} 1 \\ 0 \\ -1 \end{array} \right\} \bmod p \Leftrightarrow \left\{ \begin{array}{l} \text{2 Lösungen} \pm y \\ \text{nur 0 ist Lösung} \\ \text{keine Lösung} \end{array} \right.$$

Beispiel:

- $y^2 \equiv 2 \bmod 7$, Test $2^{\frac{7-1}{2}} \equiv 2^3 \equiv 1 \bmod 7$
  $\Rightarrow$ 2 Lösungen
- $y^2 \equiv 3 \bmod 7$, Test $3^{\frac{7-1}{2}} \equiv 3^3 \equiv 6 \equiv -1 \bmod 7$
  $\Rightarrow$ keine Lösung

Berechnung der Quadratwurzeln

$y^2 \equiv z \bmod p$ $\qquad$ $z^{\frac{p-1}{2}} \equiv 1 \bmod p$

- einfacher Fall: $p \equiv 3 \bmod 4$

$y \equiv z^{\frac{p+1}{4}} \bmod p$ ist eine Lösung, denn

$$y^2 \equiv \left(z^{\frac{p+1}{4}}\right)^2 \equiv z^{\frac{p+1}{2}} \equiv \underbrace{z^{\frac{p-1}{2}}}_{1} \cdot \underbrace{z^{\frac{2}{2}}}_{z} \equiv z \bmod p$$

- nächst komplizierterer Fall

$p \equiv 5 \bmod 8$ $\qquad$ $z^{\frac{p-1}{2}} \equiv 1 \bmod p$

$\hookrightarrow z^{\frac{p-1}{4}} \equiv \pm 1 \bmod p$

$y \equiv z^{\frac{p+3}{8}} \bmod p$

$$y^2 \equiv \left(z^{\frac{p+3}{8}}\right)^2 \equiv z^{\frac{p+3}{4}} \equiv \underbrace{z^{\frac{p-1}{4}}}_{\pm 1} \cdot \underbrace{z^{\frac{4}{4}}}_{z} \equiv \pm z \bmod p$$

falls $z^{\frac{p-1}{4}} \equiv 1 \bmod p$, dann $y^{\frac{p+3}{8}} \bmod p$ eine Lösung

falls $z^{\frac{p-1}{4}} \equiv -1 \bmod p$, dann tue folgendes

erzwinge eine zusätzliche "-1", indem eine Variable u mit $u^2 \equiv -1 \bmod p$ eingebracht wird. Hierzu wähle so lange zufällige Werte r, bis $r^{\frac{p-1}{4}} \equiv u \bmod p$ diese Bedingung erfüllt.

gelöste Fälle

~~0~~ 1 ~~2~~ [3] ~~4~~ [5] ~~6~~ [7] (mod 8)

↑ Erweiterung des 5 mod 8 Verfahrens

≡3 mod 4

S.O.

≡3 mod 4

Beispiele:

- $p \equiv 3 \bmod 4$

  $p = 19$, $y^2 \equiv 6 \bmod 19$

  $z = 6 \rightsquigarrow y \equiv z^{\frac{p+1}{4}} \equiv 6^{\frac{19+1}{4}} \equiv 6^5 \bmod 19$

$$6^5 \equiv 6^2 \cdot 6^2 \cdot 6 \equiv (-2) \cdot (-2) \cdot 6 \equiv 24 \equiv 5 \bmod 19$$

- $p \equiv 5 \bmod 8$

  $p = 29$, $y^2 \equiv 7 \bmod 29$

$$y \equiv 7^{\frac{29+3}{8}} \equiv 7^4 \equiv 7^2 \cdot 7^2 \equiv 20 \cdot 20 \equiv (-9) \cdot (-9)$$
$$= 81 \equiv -6 \equiv 23 \bmod 29 \quad \checkmark$$

- $p = 29$

  $y^2 \equiv 5 \bmod 29$

(führt auf den Fall $z^{\frac{p-1}{4}} \equiv -1 \bmod p$)