Quadratwurzeln mod p

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

$z \to y \equiv \text{"}\sqrt{z}\text{"} \bmod p$

$\rightsquigarrow$ Punkt $(x, y) \in E$

Ziel: gegeben $z \bmod p$

finde y mit $y^2 \equiv z \bmod p$

komplexitätstheoretisch probabilistisch polynomiell

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

Ansatz $y \equiv z^{\frac{p+1}{4}} \bmod p$

Probe: $y^2 \equiv \left(z^{\frac{p+1}{4}}\right)^2 \equiv z^{\frac{p+1}{2}} \equiv z \cdot \underbrace{z^{\frac{p-1}{2}}}_{\text{1, weil } z \text{ Quadrat}}$

$\equiv z \bmod p$

Beispiel: $p = 19$, $z = 11$

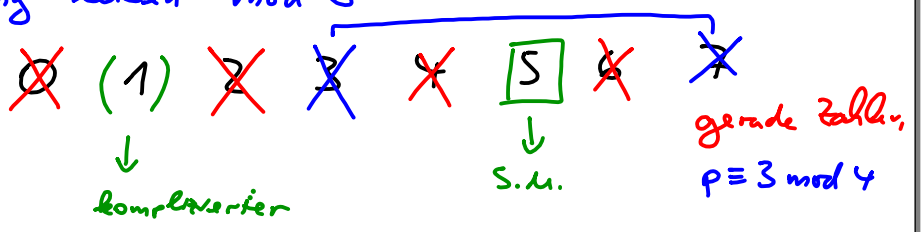
$11^{\frac{p+1}{4}} \equiv 11^{\frac{20}{4}} \equiv 11^5 \bmod 19$

$\equiv 11^2 \cdot 11^2 \cdot 11$

$\equiv 7 \cdot 7 \cdot 11$

$\equiv 11 \cdot 11 \equiv 7 \bmod 19$ ✓

übrig bleiben mod 8



Fall $p \equiv 5 \bmod 8$

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

Probe: $y^2 \equiv \left(z^{\frac{p+3}{8}}\right)^2 \equiv z^{\frac{p+3}{4}}$

$\equiv z \cdot z^{\frac{p-1}{4}}$

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

$\left(z^{\frac{p-1}{4}}\right)^2 = z^{\frac{p-1}{2}} = 1$

fertig, wenn $z^{\frac{p-1}{4}} \equiv 1 \bmod p$

Angenommen, $z^{\frac{p-1}{4}} \equiv -1 \bmod p$, dann setze statt y den Wert $y \cdot u$

$(y \cdot u)^2 \equiv \left(z^{\frac{p+3}{8}} \cdot u\right)^2 \equiv z^{\frac{p+3}{4}} \cdot u^2$

$\equiv z \cdot (-1) \cdot u^2 \bmod p$

hier wollen wir -1 haben

Teilproblem: finde u mit $u^2 \equiv -1 \bmod p$

Idee: finde ein Nichtquadrat v durch zufällige Wahl und testen von

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

$u \equiv v^{\frac{p-1}{4}} \bmod p$

Beispiel: $p = 29 \quad (\equiv 5 \bmod 8)$

a) $y^2 \equiv 20 \bmod 29$

liefert der direkte Ansatz eine Lösung?

Ja, wenn bei $z^{\frac{p-1}{4}} \equiv 1 \bmod p$ entsteht.

$$20^{\frac{29-1}{4}} = 20^7 \equiv (-9)^7 \equiv -3^{14} \equiv -(3^3)^4 \cdot 3^2$$

$$\equiv -16 \cdot 9 \equiv -144 \equiv 1 \bmod 29$$

$$\Rightarrow y \equiv z^{\frac{p+3}{8}} \equiv 20^4 \equiv (-9)^4 \equiv 3^8 \equiv 3^3 \cdot 3^3 \cdot 3^2$$

$$\equiv (-2) \cdot (-2) \cdot 9 \equiv 7 \bmod 29 \text{ ist Lösung}$$

b) $y^2 \equiv 5 \bmod 29$

teste auf direkte Lösung

$$5^{\frac{p-1}{4}} \equiv 5^7 \equiv 5^2 \cdot 5^2 \cdot 5^2 \cdot 5$$

$$\equiv \underbrace{(-4)\cdot(-4)}_{16} \cdot \underbrace{(-4)\cdot 5}_{+9}$$

$$\equiv +144 \equiv -1 \bmod 29$$

$\Rightarrow$ Nicht quadratv finden

$v = 2?$ $\quad 2^{\frac{p-1}{2}} \equiv 2^{14} \equiv 2^5 \cdot 2^5 \cdot 2^4 \equiv 3 \cdot 3 \cdot 16 \equiv -1 \bmod 29$

$\Rightarrow u$ aus v berechnen

$$u \equiv v^{\frac{p-1}{4}} \bmod p$$

$$\equiv 2^{\frac{29-1}{4}} \equiv 2^7 \equiv 2^5 \cdot 4 \equiv 3 \cdot 4 \equiv 12 \bmod 29$$

Lösung ist $y \cdot u \bmod p$ $\quad \rightarrow 12$ s.o.

$$z^{\frac{p+3}{8}} \equiv 5^{\frac{29+3}{8}} \equiv 5^4 \equiv (5^2)^2$$

$$\equiv (-4)^2 \equiv 16 \bmod 29$$

$\Rightarrow$ Lösung $16 \cdot 12 \bmod 29$

$$16 \cdot 12 = 8 \cdot (2 \cdot 12) \equiv 8 \cdot (-5) \equiv -40$$

$$\equiv -11 \equiv 18 \bmod 29$$

$18^2 \equiv 5 \bmod 29$