Wiederholung

Erzeugerkriterium

teste ob g ein Erzeuger mod p ist:

$p-1 = q_1^{e_1} \cdot q_2^{e_2} \cdots q_r^{e_r}$ Primfaktorzerlegung

falls $g^{\frac{p-1}{q_i}} \not\equiv 1 \bmod p$

für $1 \leq i \leq r$, dann g Erzeuger mod p

Beispiel: $p = 31$, $p-1 = 2 \cdot 3 \cdot 5$ ($q_1 = 2$, $q_2 = 3$, $q_3 = 5$)

teste $g=2$:

$2^{\frac{31-1}{2}} \equiv 2^{15} \equiv (2^5)^3 \equiv 1^3 \equiv 1 \bmod 31 \rightarrow$ kein E.

teste $g=3$:

$3^{\frac{31-1}{2}} \equiv 3^{15} \equiv (3^3)^5 \equiv (-4)^5 \equiv (-2^2)^5 \equiv -2^{10} \equiv -1 \bmod 31$

$3^{\frac{31-1}{3}} \equiv 3^{10} \equiv (3^3)^3 \cdot 3 \equiv (-4)^3 \cdot 3 \equiv -2 \cdot 3 \equiv -6 \bmod 31$

$3^{\frac{31-1}{5}} \equiv 3^6 \equiv (3^3)^2 \equiv (-4)^2 \equiv 16 \bmod 31$

Chinesischer Restsatz mit mehreren Teilergebnissen
(Anwendung bei diskreten Logarithmen)

DL-Problem:

$$3^x \equiv 24 \mod 31, \quad p-1 = 2 \cdot 3 \cdot 5$$

Reduktion auf Untergruppen-Größe 2

$$\left(3^x\right)^{\frac{31-1}{2}} \equiv 24^{\frac{31-1}{2}} \mod 31$$

$$(-1)^x \equiv 24^{15} \equiv 2^{15} \cdot 2^{15} \cdot 2^{15} \cdot 3^{15} \equiv 1 \cdot 1 \cdot 1 \cdot (-1)$$

$$(-1)^x \equiv -1 \mod 31 \rightarrow x \equiv 1 \mod 2$$

UG Größe 3:

$$\left(3^x\right)^{\frac{31-1}{3}} \equiv 24^{\frac{31-1}{3}} \mod 31$$

$$\left(3^{10}\right)^x \equiv 24^{10} \mod 31$$

$$25^x \equiv \left(2^{10}\right)^3 \cdot 3^{10} \equiv 1^3 \cdot 3^{10} \equiv 25 \mod 31$$

$$\rightarrow x \equiv 1 \mod 3$$

UG Größe 5:

$$\left(3^x\right)^{\frac{31-1}{5}} \equiv 24^{\frac{31-1}{5}} \mod 31$$

$$16^x \equiv 24^6 \equiv \left(2^6\right)^3 \cdot 3^6 \equiv 2^3 \cdot 16 \equiv 2 \cdot 2 \cdot (7 \cdot 16) \equiv 4 \mod 31$$

$$16^x \equiv 4 \mod 31$$

$$\rightarrow x \equiv 3 \mod 5$$

$x=0$ —
$x=1$ —
$x=2$ $16^2 \equiv (2^4)^2 \equiv 2^8 \equiv 8 \mod 31$
$x=3$ $16^3 \equiv 16^2 \cdot 16 \equiv 8 \cdot 16 \equiv 4 \mod 31$

Chinesischer Restsatz

$$\left.\begin{aligned} x &\equiv 1 \bmod 2 \\ x &\equiv 1 \bmod 3 \\ x &\equiv 3 \bmod 5 \end{aligned}\right] \rightarrow \text{Eng mod } 2 \cdot 3$$

$m_1 = 2 \quad m_2 = 3$

$a_1 = 1 \quad a_2 = 1$

$m_1' \equiv \frac{1}{m_1} \bmod m_2 \qquad m_2' \equiv \frac{1}{m_2} \bmod m_1$

$m_1' \equiv \frac{1}{2} \bmod 3 \qquad m_2' \equiv \frac{1}{3} \bmod 2$

$m_1' \equiv 2 \bmod 3 \qquad m_2' \equiv 1 \bmod 2$

$x = a_1 \cdot m_2 \cdot m_2' + a_2 \cdot m_1 \cdot m_1' = 1 \cdot 3 \cdot 1 + 1 \cdot 2 \cdot 2 = 7$

$x \equiv 7 \equiv 1 \bmod 6$

$\left.\begin{aligned} x &\equiv 1 \bmod 6 \\ x &\equiv 3 \bmod 5 \end{aligned}\right]$ Chin. Restsatz $\longrightarrow$ $x \equiv 13 \bmod 30$

Quadratwurzeln mod p

Löse $y^2 \equiv z \bmod p$

→ prüfe $z^{\frac{p-1}{2}} \equiv 1 \bmod p$

Fälle:

$p \equiv 1 \bmod 8$ in Vorlesung nicht behandelt

$p \equiv 3 \bmod 8, \equiv 7 \bmod 8 \Rightarrow p \equiv 3 \bmod 4 \Rightarrow z^{\frac{p+1}{4}}$ ist Lösung

$p \equiv 5 \bmod 8$

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

Falls $z^{\frac{p-1}{4}} \equiv 1 \bmod p \rightarrow z^{\frac{p+3}{8}}$ ist Lösung

sonst brauchen wir eine Variable u mit $u^2 \equiv -1 \bmod p$

$$\rightarrow \left(u \cdot z^{\frac{p+3}{8}}\right)^2 \equiv u^2 \cdot (-z) \equiv (-1)\cdot(-z) \equiv z \bmod p$$

u ist eine Quadratwurzel von -1

rate ein Nichtquadrat r $\left(\rightarrow r^{\frac{p-1}{2}} \equiv -1 \bmod p\right)$

$$\left(r^{\frac{p-1}{4}}\right)^2 \equiv -1 \bmod p$$

u

wähle r zufällig bis Nichtquadrat gefunden

Beispiel:

$p = 13 \quad (\equiv 5 \bmod 8)$

$z = 10$ ist Quadrat wg. $10^{\frac{13-1}{2}} \equiv 1 \bmod 13$

$\Rightarrow y^2 \equiv 10 \bmod 13$ lösbar $(*)$

Ansatz: $y \equiv z^{\frac{p+3}{8}} \equiv 10^{\frac{13+3}{8}} \equiv 10^2 \equiv 9 \bmod 13$

aber $z^{\frac{p-1}{4}} \equiv 10^{\frac{13-1}{4}} \equiv 10^3 \equiv (-3)^3 \equiv -27 \equiv -1 \bmod 13$

$\rightarrow$ r zufällig wählen

$r = 2$ (Frage: Nichtquadrat)

$\boxed{2^{\frac{p-1}{2}}} \equiv 2^6 \equiv 2^4 \cdot 2^2 \equiv 3 \cdot 2^2 \equiv 12 \equiv \boxed{-1} \bmod 13$

$\Rightarrow \underbrace{y \cdot 2^{\frac{p-1}{4}}}$ ist Lösung der Gleichung $(*)$

$9 \cdot 2^{\frac{13-1}{4}} \equiv 9 \cdot 2^3 \equiv \underbrace{9 \cdot 2}_{5} \cdot 2 \cdot 2 \equiv 7 \bmod 13$

Probe: $7^2 \equiv 10 \bmod 13$ ✓

Elliptische Kurven

$y^2 \equiv x^3 + ax + b$ unbekannt

$P_1 = (x_1, y_1) \Rightarrow y_1^2 \equiv x_1^3 + ax_1 + b$

$P_2 = (x_2, y_2) \Rightarrow y_2^2 \equiv x_2^3 + ax_2 + b$

Signaturen

m Nachricht

$h(m)$ Hashwert ($e = h(m)$ in ECDSA)

mit $h(m)$ wird Signatur s berechnet ((r,s) in ECDSA, DSA)

Empfänger hat m, Signatur s

↳ $h(m)$ berechnen → Signaturverfahren