Vorlesung „Kryptographie II“ (Sommersemester 2025)

Übungsblatt 3 (9.5.2025)

Aufgabe 11: Welche der Zahlen

$$5461, \quad 7957, \quad 8321, \quad 8481, \quad 8693, \quad 8881, \quad 8911$$

besteht den Fermat-Test, den Solovay-Strassen-Test, den Miller-Rabin-Test jeweils zur Basis 2? Welche der Zahlen ist eine Primzahl?

Aufgabe 12: Ein öffentlicher Goldwasser-Micali-Schlüssel wird gegeben durch $(N, 2)$ mit der 140-stelligen RSA-Zahl

```
N=184825084266490633627443597234866236073093997591323425316855225866179161230664881350490691289850785955956275335345387351230494146559518317 27.
```

Eine 4-stellige Primzahl p hat die Binärentwicklung $(a_1, \ldots, a_{11})_2$ mit $a_i \in \{0, 1\}$. Mit dem öffentlichen Goldwasser-Micali-Schlüssel $(N, 2)$ wurde die Folge $a_1, \ldots, a_{11}$ zur Zahlenfolge $b_1, \ldots, b_{11}$ Goldwasser-Micali-verschlüsselt, d.h. es wurde nach Wahl von Zufallszahlen z_i

$$b_i = \begin{cases} z_i^2 \bmod N & \text{für } a_i = 0, \\ 2z_i^2 \bmod N & \text{für } a_i = 1 \end{cases}$$

berechnet. Hier sind die Zahlen $b_1, \ldots, b_{11}$:

```
336105990496482155812519040543349947678645624383778288337278782424605459156227534132502736679385931867117758945435015577883240867436448865 8,
119047147252459431607491387801821026013936182312125344760139204817284075432955269316539666705676793396402508791758660801048698902469014810 24,
137564237261636138738425960937441555860339156305668900578024605008925881069692220146003936994529960183324249659645782053936880975727557267 67,
125318214765773534872916624280288004242103489292947042495537535627823647051071283622039183384656338240976830580256736581766465221512514895 78,
671288073019106217737646457352827233737526054744540064499141603653147872005735524575643658161475352348503754576890445755863729148979556163 6,
362673058119786303527378208419220953095977635393553960263853171870149866930890033423837537351258258040117659914414775760200353501072685 70,
123385641722938036701903356973603374931417986988579192694556771604924269229287838123966302496807237994800392547672859875931617203846174719 3,
967945679370357259259525679959825877291969834860944633250234977352859934509473455383703174373221918462707062315774017163701497931391232850 8,
747994972200676362111985288711396581996846734474859502935870794986633505487490075944594676302232689449949295885112876764619868919917159962 5,
149219560663348371951144681844412204253753664206791663223490928829518776615989620110525567958395800634047901201922388811063890600091668941 81,
180090971864814407874138369774023792230726019995608447765102610917102010055750863821369449706299323342001970227828949683449903776705199820 25.
```

Was ist p? (Hinweis: `VETRAQJBVFGRVASRUYRECNFFVREGORERPUARQVRWNPBOVFLZOBYR`)

Aufgabe 13: Für eine ungerade Primzahl p sei $\widetilde{n}(p)$ der kleinste positive quadratische Nichtrest modulo p, d.h.

$$\widetilde{n}(p) = \min\left\{ n \in \mathbb{N} : \left(\frac{n}{p}\right) = -1 \right\}.$$

(1) Zeige, dass $\widetilde{n}(p)$ eine Primzahl ist.

(2) Sei $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, ... die Folge der Primzahlen. Zeige: Ist $r \geq 2$ und p eine Primzahl mit

$$p \equiv 1 \bmod 8\, p_2 \ldots p_{r-1},$$

(Für $r = 2$ ist dies als $p \equiv 1 \bmod 8$ zu lesen.) so gilt

$$\widetilde{n}(p) \geq p_r.$$

(Aus dem Dirichletschen Primzahlsatz folgt, dass es unendlich viele Primzahlen dieser Bauart gibt.)

(3) Gibt es für jedes $r \geq 1$ ungerade Primzahlen p mit

$$\widetilde{n}(p) = p_r?$$

(4) Konstruiere eine Primzahl p mit $\widetilde{n}(p) \geq 100$. (Geht auch $\widetilde{n}(p) \geq 1000$?)

Datei: kii_u3.tex. Version vom 8.5.2025

Aufgabe 14: Sei $p = 137$. Es gilt $\left(\frac{11}{p}\right) = 1$, $\left(\frac{17}{p}\right) = 1$, $\left(\frac{59}{p}\right) = 1$, $\left(\frac{103}{p}\right) = 1$ und $\left(\frac{3}{p}\right) = -1$. Bestimme für $a = 11, 17, 59, 103$ Quadratwurzeln modulo p (unter Verwendung von $n = 3$ als Nichtquadrat modulo p). Dazu kann das Tonelli-Verfahren oder ein anderes Verfahren aus der Vorlesung benutzt werden.

Aufgabe 15: Sei p eine ungerade Primzahl und seien $a, c \in \mathbb{F}_p$. Dazu werden Matrizen im Matrizenring $\mathrm{M}_2(\mathbb{F}_p)$ durch

$$B = \begin{pmatrix} 0 & 1 \\ c^2 - a & 0 \end{pmatrix} \quad \text{und} \quad A = c \cdot \mathbf{1}_2 + B = \begin{pmatrix} c & 1 \\ c^2 - a & c \end{pmatrix}$$

definiert.

(1) Berechne B^2.

(2) Zeige, dass für jedes $n \in \mathbb{N}_0$ Elemente $u_n, v_n \in \mathbb{F}_p$ existieren mit

$$A^n = u_n \cdot \mathbf{1}_2 + v_n \cdot B.$$

(3) Zeige mit Hilfe des Ergebnisses aus (1), dass

$$B^{p-1} = \left(\frac{c^2 - a}{p}\right) \cdot \mathbf{1}_2 \quad \text{und} \quad B^p = \left(\frac{c^2 - a}{p}\right) B$$

gilt, wobei $\left(\frac{c^2-a}{p}\right)$ das Legendre-Symbol bezeichnet.

(4) Gilt für $X, Y \in \mathrm{M}_2(\mathbb{F}_p)$ die Gleichung $XY = YX$, so gilt $(X + Y)^p = X^p + Y^p$. Folgere daraus

$$A^p = c \cdot \mathbf{1}_2 + \left(\frac{c^2 - a}{p}\right) \cdot B.$$

(5) Zeige, dass im Fall $\left(\frac{c^2-a}{p}\right) = -1$ gilt

$$A^{p+1} = a \cdot \mathbf{1}_2.$$

(6) Zeige mit Hilfe von (5), dass im Fall $\left(\frac{c^2-a}{p}\right) = -1$ und $\left(\frac{a}{p}\right) = 1$

$$A^{\frac{p+1}{2}} = u_{\frac{p+1}{2}} \cdot \mathbf{1}_2$$

gilt, und folgere, dass $u_{\frac{p+1}{2}}$ eine Quadratwurzel von a in $\mathbb{F}_p$ ist.

(Mit der square-and-multiply-Methode kann man $A^{\frac{p+1}{2}}$ schnell berechnen. Daher liefert die Aufgabe eine weitere Möglichkeit, Quadratwurzeln modulo p schnell zu berechnen.)