Institut für Informatik
Prof. Dr. J. Rothe

Wintersemester 2023/24
Übungsblatt 7

Lösungsvorschläge

Kryptokomplexität 1

Bearbeitungszeit: 21. November bis 29. November - 1. Dezember
Verantwortlich: Roman Zorn

Aufgabe 1 : Fermat-Test

Führen Sie für folgende Zahlen den Fermat-Test durch. Wählen Sie jeweils $a = 3$ und verwenden Sie dabei Square-and-Multiply. Geben Sie alle Rechenschritte an. In welchem Fall/in welchen Fällen gibt der Test ein richtiges Ergebnis an?

(a) ▶ $n = 375$,

(b) ▶ $n = 419$,

(c) ▶ $n = 1105$.

Lösungsvorschlag: ▶
Wir betrachten alle Aufgabeteilen gleichzeitig: Es muss jeweils getestet werden, ob $a^{n-1} \equiv 1 \mod n$ gilt. Dazu berechnen wir die Potenz jeweils mit Square-and-Multiply. Es gilt $374 = 2 + 4 + 16 + 32 + 64 + 256 = 2^1 + 2^2 + 2^4 + 2^5 + 2^6 + 2^8$, $418 = 2 + 32 + 128 + 256 = 2^1 + 2^5 + 2^7 + 2^8$ und $1104 = 16 + 64 + 1024 = 2^4 + 2^6 + 2^{10}$ und

2^0	2^1	2^2	2^3	2^4	2^5	2^6	2^7	2^8	2^9	2^{10}	
3	**9**	**81**	186	**96**	**216**	**156**	336	**21**			mod 375
3	**9**	81	276	337	**20**	400	**361**	**12**			mod 419
3	9	81	1036	**341**	256	**341**	256	341	256	**341**	mod 1105

Nun gilt

$$3^{374} \equiv 9 \cdot 81 \cdot 96 \cdot 216 \cdot 156 \cdot 21 \equiv 144 \not\equiv 1 \mod 375.$$

Also ist 3 ein Fermat-Zeuge dafür, dass 375 keine Primzahl ist.
Ebenso gilt

$$3^{418} \equiv 9 \cdot 20 \cdot 361 \cdot 12 \equiv 1 \mod 419.$$

Also ist 419 möglicherweise eine Primzahl; und tatsächlich ist 419 eine Primzahl.
Außerdem gilt

$$3^{1104} \equiv 341^3 \equiv 1 \mod 1105.$$

Also ist 1105 möglicherweise eine Primzahl; allerdings ist 1105 die zweitkleinste Carmichael-Zahl (nach 561) und somit zusammengesetzt. Der Primfaktor 5 ist zum Beispiel offensichtlich. Demnach ist 3 ein Fermat-Lügner für 1105.

Aufgabe 2 : Miller-Rabin-Test

Führen Sie für folgende Zahlen den Miller-Rabin-Test durch. Wählen Sie jeweils $a = 3$ und verwenden Sie dabei Square-and-Multiply. In welchem Fall/in welchen Fällen gibt der Test ein richtiges Ergebnis an?

(a) ► $n = 375$,

(b) ► $n = 419$,

(c) ► $n = 1105$.

Lösungsvorschlag: ►
Wir betrachten alle Aufgabeteile gleichzeitig: Zunächst berechnen wir für jede Zahl n, wie oft $n-1$ den Teiler 2 enthält. Es gilt $374 = 2 \cdot 187$, $418 = 2 \cdot 209$ und $1104 = 2^4 \cdot 69$. Nun führen wir den ersten Teil des Tests durch, wobei die Berechnungen mit Square-and-Multiply durchgeführt werden. Es gilt $187 = 1 + 2 + 8 + 16 + 32 + 128 = 2^0 + 2^1 + 2^3 + 2^4 + 2^5 + 2^7$, $209 = 1 + 16 + 64 + 128 = 2^0 + 2^4 + 2^6 + 2^7$ bzw. $69 = 1 + 4 + 64 = 2^0 + 2^2 + 2^6$ und

2^0	2^1	2^2	2^3	2^4	2^5	2^6	2^7	
3	**9**	81	**186**	**96**	**216**	156	**336**	mod 375
3	9	81	276	**337**	20	**400**	**361**	mod 419
3	9	**81**	1036	341	256	**341**		mod 1105

(Wir verwenden hier die gleichen n und a wie in Aufgabe 1. Somit ist diese Tabelle ein Ausschnitt aus der vorherigen Tabelle).
Nun gilt

$$3^{187} \equiv 3 \cdot 9 \cdot 186 \cdot 96 \cdot 216 \cdot 336 \equiv 12 \not\equiv 1 \mod 375.$$

Also besteht 3 den ersten Teil des Tests für 375.
Ebenso gilt

$$3^{209} \equiv 3 \cdot 337 \cdot 400 \cdot 361 \equiv 1 \mod 419.$$

Also ist 419 möglicherweise eine Primzahl; und tatsächlich ist 419 eine Primzahl.
Außerdem gilt

$$3^{69} \equiv 3 \cdot 81 \cdot 341 \equiv 1093 \mod 1105.$$

Also besteht 3 den ersten Teil des Tests für 1105.
Jetzt führen wir den zweiten Teil des Tests durch. Dies müssen wir nicht mehr für 419 machen, da schon der erste Teil des Tests es nicht mehr ermöglicht, dass 3 ein Miller-Rabin-Zeuge für 419 sein kann.

Da $k = 1$ für 375, müssen wir die Gleichung nur für $j = 0$ überprüfen. Somit gilt

$$3^{187} \equiv 12 \not\equiv 374 \equiv -1 \mod 375.$$

Also besteht 3 auch den zweiten Teil des Tests für 375 und somit ist 3 ein Miller-Rabin-Zeuge dafür, dass 375 keine Primzahl ist.
Für 1105 ist $k = 4$ und es gilt

$$\begin{aligned} 3^{69} &\equiv 1093 \not\equiv 1104 \equiv -1 \mod 1105 \\ 3^{2\cdot 69} &\equiv 1093^2 \equiv 144 \not\equiv 1104 \equiv -1 \mod 1105 \\ 3^{2^2\cdot 69} &\equiv 144^2 \equiv 846 \not\equiv 1104 \equiv -1 \mod 1105 \\ 3^{2^3\cdot 69} &\equiv 846^2 \equiv 781 \not\equiv 1104 \equiv -1 \mod 1105. \end{aligned}$$

Also besteht 3 auch den zweiten Teil des Tests für 1105 und somit ist 3 ein Miller-Rabin-Zeuge dafür, dass 1105 keine Primzahl ist.

Aufgabe 3 : Ordnung von Gruppenelementen

(a) Betrachten Sie, für eine Primzahl p, die Gruppe $(\mathbb{Z}_p^*, \cdot)$ aus der Vorlesung und sei $a \in \mathbb{Z}_p^*$.

► Zeigen Sie, dass für jedes $i, j \in \mathbb{Z}$ mit $j > i \geq 0$

$$a^i \equiv a^j \mod p \iff i \equiv j \mod \text{ord}(a)$$

gilt, wobei wir mit $\text{ord}(a)$ die Ordnung von a in $\mathbb{Z}_p^*$ bezeichnen.

Hinweis: Betrachten Sie gegebenenfalls noch einmal die Lösung von Blatt 5, Aufgabe 4.

Lösungsvorschlag: ► Angenommen, es gilt $a^i \equiv a^j \mod p$ für beliebige $i, j \in \mathbb{Z}$ mit $j > i \geq 0$. Dann gilt für $k = j - i > 0$

$$a^k = a^{j-i} = a^j \cdot a^{-i} = a^j \cdot (a^i)^{-1} \equiv a^j \cdot (a^j)^{-1} \equiv 1 \mod p, \tag{1}$$

wie im Beweis von Aufgabe 4(a) von Blatt 5.

Weiterhin wissen wir, dass wir jedes $k \in \mathbb{Z}$ schreiben können als $k = l \cdot \text{ord}(a) + r$, für $0 \leq r < \text{ord}(a)$. Somit gilt nun durch (1)

$$1 \equiv a^k = a^{l\cdot \text{ord}(a)+r} = (a^{\text{ord}(a)})^l \cdot a^r \equiv 1^l \cdot a^r \equiv a^r \mod p.$$

Nun gilt, dass alle $a^0, \ldots, a^{ord(a)}$ paarweise verschieden sein müssen (nach Aufgabe 4(b) von Blatt 5). Aus $r < \text{ord}(a)$ können wir nun folgern, dass $r = 0$ gilt und somit teilt $\text{ord}(a)$ die Differenz $j - i$, was zu zeigen war.

Für die Rückrichtung nehmen wir an, dass $\text{ord}(a)$ die Differenz $j - i$ teilt, d.h.

es gilt $j - i = l \cdot \text{ord}(a)$, dann folgt

$$a^i = a^i \cdot 1^l \equiv a^i \cdot (a^{\text{ord}(a)})^l = a^i \cdot a^{l \cdot \text{ord}(a)} = a^{i + l \cdot \text{ord}(a)} \equiv a^j \mod p.$$

(b) Es sei $n = p \cdot q$ für Primzahlen p und q und γ mit $\text{ord}(\gamma) = p - 1$ in $\mathbb{Z}_p^*$.

► Folgern Sie aus (a), dass nun

$$\gamma^{n-1} \equiv 1 \mod p \Longrightarrow p - 1 \text{ teilt } n - 1$$

gilt.

Lösungsvorschlag: ► Man sieht sofort, dass die gewünschte Aussage gilt, wenn man in (a) $a = \gamma$, $j = n - 1$ und $i = 0$ einsetzt, denn dann besagt (a)

$$\gamma^0 \equiv \gamma^{n-1} \mod p \Longleftrightarrow 0 \equiv n - 1 \mod p - 1,$$

was insbesondere die gewünschten Aussage zeigt.

Aufgabe 4 : Quadratwurzel von 1 modulo n

(a) ► Zeigen Sie, dass die Kongruenz

$$n^2 \equiv 1 \bmod 8$$

für alle ungeraden natürlichen Zahlen n gilt.

Lösungsvorschlag: ► Ungerade natürliche Zahlen sind von der Form $n = 2k + 1$ mit $k \in \mathbb{N}$.

$$n^2 = (2k + 1)^2 = 4k(k + 1) + 1$$

Da entweder k oder $k + 1$ durch 2 teilbar ist, ist $k(k + 1)$ durch 2 teilbar und $4 \cdot k(k + 1)$ durch 8 teilbar. Also ist

$$n^2 = 4k(k + 1) + 1 \equiv 1 \bmod 8.$$

(b) ► Gilt diese Aussage für alle natürlichen Zahlen? Begründen Sie Ihre Antwort.

Lösungsvorschlag: ► Nein, zum Beispiel gezeigt durch $n = 4$, denn

$$n^2 = 16 \equiv 0 \bmod 8.$$

(c) Sei $n = 5 \cdot 17 = 85$.

► Wie viele Quadratwurzel von 1 modulo n gibt es? Geben Sie sie an und zeigen Sie ohne zu quadrieren, dass es sich tatsächlich um Quadratwurzeln von 1 modulo n handelt.

Lösungsvorschlag: ► Eine aus k ungeraden Primzahlen zusammengesetzte Zahl n hat 2^k Quadratwurzeln von 1 modulo n. Somit gibt es 4 Quadratwurzeln von 1 modulo 85. Die Quadratwurzeln von 1 modulo 85 sind $1, 16, 69, 84$, da für jede dieser Zahlen $a \in \{1, 16, 69, 84\}$ gilt, dass für jedes $p_i \in \{5, 17\}$ entweder $a \equiv 1 \mod p_i$ oder $a \equiv p_i - 1 \mod p_i$. Neben den trivialen Quadratwurzeln 1 und 84, gilt:

$$16 \equiv 1 \mod 5 \quad \text{und} \quad 16 \equiv 17 - 1 \mod 17$$
$$69 \equiv 5 - 1 \mod 5 \quad \text{und} \quad 69 \equiv 1 \mod 17$$