9. Musterlösung zu Mathematik für Informatiker I, WS 2003/04

KATHRIN TOFALL, MICHAEL NÜSKEN

Die mit * gekennzeichneten Aufgabenteile und Aufgaben sind freiwillig. Die dort erworbenen Punkte werden als Weihnachtszusatzpunkte gutgeschrieben.

Aufgabe 9.1 (Modulares Rechnen). (4+3 Punkte)

(i) Finde alle Lösungen x von $3(x+3) = 7$ in $\mathbb{Z}_{13}$. 1

Lösung. Zuerst müssen wir $3 \bmod 13$ invertieren; mit dem EEA erhalten wir 9 als Inverse. Damit wissen wir, daß $x + 3 \equiv 11 \bmod 13$ ist, somit $x \equiv 8 \bmod 13$. Alle Lösungen in $\mathbb{Z}$ sind von der Form $8+13y$, wobei $y \in \mathbb{Z}$. Die Lösungen suchen wir aber in $\mathbb{Z}_{13}$ und erhalten also $x = 8 = -5$ als einzige Lösung in $\mathbb{Z}_{13}$. ◯

(ii) Finde alle Lösungen x von $17(2-x)x = 4x^2 - x + 7$ in $\mathbb{Z}_{21}$. 1

Lösung. Wir bringen zuerst alles auf eine Seite und fassen zusammen:

$$0 = 4x^2 - x + 7 - 17(2-x)x = 21x^2 - 35x + 7 = 7x + 7 \quad \text{in } \mathbb{Z}_{21}.$$

Nun betrachten wir diese Gleichung modulo 3 und modulo 7:

$$\begin{aligned} 0 &= x + 1 \quad \text{in } \mathbb{Z}_3, \\ 0 &= 0 \quad \text{in } \mathbb{Z}_7. \end{aligned}$$

Die erste Gleichung hat genau die Lösung $x = 2$ in $\mathbb{Z}_3$, die zweite Gleichung hat in $\mathbb{Z}_7$ jede Zahl als Lösung. Damit sind alle $x \in \mathbb{Z}_{21}$ Lösung, die modulo 3 den Rest 2 ergeben, die Lösungsmenge ist

$$\{2, 5, 8, 11, 14, 17, 20\} \subset \mathbb{Z}_{21}.$$

Bemerkung: In $\mathbb{Z}$ gelesen gibt es natürlich noch mehr Lösungen, aber deren Reste modulo 21 waren gefragt und die stehen alle da. ◯

(iii) Finde alle Lösungen x von $x + 1/x = 1 - 5x$ in $\mathbb{Z}_6$. 1

Lösung. Die Gleichung ist äquivalent zu

$$6x + 1/x - 1 \equiv 1/x - 1 \equiv 0 \bmod 6.$$

Also ist $x = 1$ die einzige Lösung in $\mathbb{Z}_6$, wobei wir darauf aufmerksam machen, dass 1 auch invertierbar ist, sich also in die ursprüngliche Gleichung einsetzen lässt. ◯

(iv) Finde alle Lösungen x von $3x = 9$ in $\mathbb{Z}_{105}$. *Tipp*: Verwende den Chinesischen Restsatz. [1]

Lösung. Da $105 = 3 \cdot 5 \cdot 7$ ist, können wir die Gleichung wegen des chinesischen Restsatzes nach jedem Faktor getrennt betrachten.

$$\begin{aligned} 0 &= 0 \quad \text{in } \mathbb{Z}_3, \\ 3x &= 9 \quad \text{in } \mathbb{Z}_5 \text{ und in } \mathbb{Z}_7. \end{aligned}$$

Die erste Gleichung hat offenbar jede Zahl in $\mathbb{Z}_3$ als Lösung, die zweite Gleichung hat $x = 3$ in $\mathbb{Z}_5$ und $\mathbb{Z}_7$ und damit auch in $\mathbb{Z}_{35}$ als Lösung. Nach dem chinesischen Restsatz sind damit die Lösungen der ursprünglichen Gleichung alle die Zahlen in $\mathbb{Z}_{105}$ die modulo 35 den Rest 3 ergeben, also ist die Lösungsmenge in $\mathbb{Z}_{105}$

$$\{3, 38, 73\}.$$ ◯

Lösung (Etwas näher an der älteren Betrachtungsweise). Die Gleichung entspricht $3x - 9 \equiv 0 \bmod 105$. Also gilt

$$105 \mid (3(x - 3)).$$

Die 3 können wir kürzen und erhalten

$$35 \mid (x - 3).$$

Also entspricht x der 3 modulo 35. Alle Lösungen in $\mathbb{Z}$ sind von der Form $3 + 35y$, wobei $y \in \mathbb{Z}$. Damit ist die Lösungsmenge in $\mathbb{Z}_{105}$

$$\{3, 38, 73\}.$$ ◯

2* (v*) Finde alle Lösungen von $x^2 + x + 4 = 0$ in $\mathbb{Z}_{19}$. *Tipp*: Eine Gleichung der Form $u^2 = c$ hat höchstens zwei Lösungen modulo einer Primzahl.

Lösung. Diese Aufgabe können wir mit quadratischer Ergänzung lösen. Wir können dabei erstmal wie in $\mathbb{Q}$ vorgehen, da modulo 19 alle

Zahlen (bis auf die 0) invertierbar sind. Bei dieser Aufgabe wäre die quadratische Ergänzung $\left(\frac{1}{2}\right)^2$ und die ganze Gleichung könnte man so umstellen:

$$-4 + \left(\frac{1}{2}\right)^2 = x^2 + x + \left(\frac{1}{2}\right)^2 = \left(x + \frac{1}{2}\right)^2.$$

Mit dem EEA können wir das Inverse von 2 berechnen. Es gilt $2 \cdot 10 = 1$ in $\mathbb{Z}_{19}$. Wenn wir diese Ergebnisse in die Umformung einsetzen, folgt:

$$(x+10)^2 = -4 + 10^2 = 1 \quad \text{in } \mathbb{Z}_{19}.$$

Die Gleichung $u^2 = 1$ in $\mathbb{Z}_{19}$ hat sicher die beiden Lösungen $u = \pm 1$ und nach dem Tipp (vergleiche *Aufgabe 9.4(iii*)) kann es nicht mehr geben, da ja 19 prim ist. Also hat die Gleichung die Lösungen

$$x = 9 \pm 1 \quad \text{in } \mathbb{Z}_{19}.$$

Und die Lösungsmenge ist $\{8, 10\} = \{8, -9\} \subset \mathbb{Z}_{19}$. ◯

(vi*) Finde alle Lösungen x von $x \equiv 2 \bmod 7$ und $x^2 \equiv 1 \bmod 11$. 1*

Lösung. Wir lösen zuerst die zweite Gleichung. Offenbar sind $x \equiv 1 \bmod 11$ und $x \equiv -1 \bmod 11$ Lösungen. Nach *Aufgabe 9.4(iii*) kann es auch keine weiteren geben. Wir müssen nun also die beiden Systeme

$$x \equiv 2 \bmod 7, \qquad x \equiv 1 \bmod 11$$

und

$$x \equiv 2 \bmod 7, \qquad x \equiv -1 \bmod 11$$

lösen. Dazu berechnen wir zuerst mit dem EEA passende s und t:

i	r_i	q_i	s_i	t_i	Kommentar
0	11		1	0	
1	7	1	0	1	$4 = 1 \cdot 7 + 11$
2	4	1	1	-1	$3 = 1 \cdot 4 + 7$
3	3	1	-1	2	$1 = 1 \cdot 3 + 4$
4	1	3	2	-3	$0 = 3 \cdot 1 + 3$
5	0		-7	11	

Wir erhalten als den ggT $1 = 2 \cdot 11 + -3 \cdot 7$. Setzen wir nun $u = 2 \cdot 11$ und $v = -3 \cdot 7$, so ist offenbar

$$u \equiv 1 \bmod 7, \qquad v \equiv 0 \bmod 7,$$
$$u \equiv 0 \bmod 11, \qquad v \equiv 1 \bmod 11.$$

Das erste System ist also äquivalent zu $x \equiv 2u + 1v \bmod 77$ und das zweite zu $x \equiv 2u - 1v \bmod 77$. Wir erhalten die Lösungsmenge $\{23, 65\} = \{23, -12\} \subset \mathbb{Z}_{77}$. ◯

Aufgabe 9.2 (RSA durchführen). (4+1 Punkte)

Wir wollen einmal das RSA Verfahren an Zahlen durchführen.

1 (i) Sei $p = 251$ und $q = 263$. Bestimme den Modul N sowie $\varphi(N)$.

Lösung. $N = 251 \cdot 263 = 66013$ und $\varphi(N) = (p-1) \cdot (q-1) = 250 \cdot 262 = 65500$. ◯

1 (ii) Sei $e = 17$. Bestimme den Entschlüsselungsexponenten d.

Lösung. Wir benutzen den EEA, um das Inverse von $17 \bmod 65500$ zu bestimmen:

i	r_i	q_i	s_i	t_i
0	65 500	–	1	0
1	17	3 852	0	1
2	16	1	1	−3 852
3	1	16	−1	3 853
4	0	–	17	−65 500

Also gilt $1 = -1 \cdot 65500 + 3853 \cdot 17$. Somit ist das gesuchte $d = 3853$. ◯

1 (iii) Sei x die geheime Nachricht, die dem ASCII-Zeichenpaar „Ok“ entspricht. Berechne deren Verschlüsselung y.

Lösung. Wenn wir das Wort Ok so in eine Dezimalzahl umwandeln, wie in Aufgabe 5.3, dann erhalten wir $x = 20331$. Deren Verschlüsselung ist dann $20331^{17} \bmod 66013$:

$$\begin{aligned} 20331^2 &\equiv 42168 \bmod 66013, \\ 20331^4 &\equiv 42168^2 \equiv 14056 \bmod 66013, \\ 20331^8 &\equiv 14056^2 \equiv 60240 \bmod 66013, \\ 20331^{16} &\equiv 60240^2 \equiv 56977 \bmod 66013. \end{aligned}$$

Also berechnen wir wie folgt:

$$20331^{17} = 20331^{16} \cdot 20331 \equiv 3263 \bmod 66013.$$

Zur Basis 256 wäre das dann das Zahlenpaar $[12, 191]$. ◯

1 (iv) Sei $y = 3263$ die verschlüsselte Nachricht. Berechne deren Entschlüsselung z.

Lösung. Die Entschlüsselung von y ist 3263^{3853}:

$$\begin{aligned}
3263^{(10)_2} &\equiv 19076 \bmod 66013,\\
3263^{(100)_2} &\equiv 30120 \bmod 66013,\\
3263^{(1000)_2} &\equiv 63754 \bmod 66013,\\
3263^{(10000)_2} &\equiv 20080 \bmod 66013,\\
3263^{(100000)_2} &\equiv 65009 \bmod 66013,\\
3263^{(1000000)_2} &\equiv 17821 \bmod 66013,\\
3263^{(10000000)_2} &\equiv 65511 \bmod 66013,\\
3263^{(100000000)_2} &\equiv 53965 \bmod 66013,\\
3263^{(1000000000)_2} &\equiv 57730 \bmod 66013,\\
3263^{(10000000000)_2} &\equiv 20582 \bmod 66013,\\
3263^{(100000000000)_2} &\equiv 13303 \bmod 66013.
\end{aligned}$$

Weil $3853 = (1,1,1,1,0,0,0,0,1,1,0,1)_2$ berechnen wir also:

$$\begin{aligned}
3263^{3853} &\equiv 3263^{2048} \cdot 3263^{1024} \cdot 3263^{512} \cdot 3263^{256} \cdot 3263^{8} \cdot 3263^{4} \cdot 3263\\
&\equiv 13303 \cdot 20582 \cdot 57730 \cdot 53965 \cdot 63754 \cdot 30120 \cdot 3263\\
&\equiv 20331 \bmod 66013.
\end{aligned}$$

Alternativ hätten wir auch so vorgehen können:

$$\begin{aligned}
3263^{(1)_2} &\equiv 3263 \bmod 66013, & 3263^{(1111000)_2} &\equiv 28112 \bmod 66013,\\
3263^{(10)_2} &\equiv 19076 \bmod 66013, & 3263^{(11110000)_2} &\equiv 42921 \bmod 66013,\\
3263^{(11)_2} &\equiv 60742 \bmod 66013, & 3263^{(111100000)_2} &\equiv 53463 \bmod 66013,\\
3263^{(110)_2} &\equiv 57981 \bmod 66013, & 3263^{(111100001)_2} &\equiv 43423 \bmod 66013,\\
3263^{(111)_2} &\equiv 64758 \bmod 66013, & 3263^{(1111000010)_2} &\equiv 27610 \bmod 66013,\\
3263^{(1110)_2} &\equiv 56726 \bmod 66013, & 3263^{(1111000011)_2} &\equiv 49698 \bmod 66013,\\
3263^{(1111)_2} &\equiv 62499 \bmod 66013, & 3263^{(11110000110)_2} &\equiv 14809 \bmod 66013,\\
3263^{(11110)_2} &\equiv 3765 \bmod 66013, & 3263^{(111100001100)_2} &\equiv 11295 \bmod 66013,\\
3263^{(111100)_2} &\equiv 48443 \bmod 66013, & 3263^{(111100001101)_2} &\equiv 20331 \bmod 66013.
\end{aligned}$$

(v*) Programmiere RSA in MAPLE. *Tipp*: Verwende die Hilfe, um mehr über `mod` sowie `nextprime` zu erfahren. 1*

Lösung. Ein RSA-Mapleworksheet wird auf der Vorlesungsseite verfügbar sein. ◯

Aufgabe 9.3 (Ansatz für einen Primtest). (4+2 Punkte)

Sei n ungerade.

1 (i) Berechne 2^{n-1} rem n für alle ungeraden n mit $3 \leq n \leq 20$ sowie für $n = 1105$.

Lösung. Für $n \in \{3, 5, 7, 11, 13, 17, 19\}$, also n prim und kleiner 20, gilt:

$$2^{n-1} \equiv 1 \bmod n.$$

Für $n = 9$ ist $\varphi(9) = 3^{2-1} \cdot (3-1) = 3 \cdot 2 = 6$, da 9 Primpotenz. Also gilt $2^6 \equiv 1 \bmod 9$ und dann insgesamt:

$$2^{9-1} = 2^8 = 2^6 \cdot 2^2 \equiv 1 \cdot 4 = 4 \bmod 9.$$

Bleibt noch $n = 15 = 3 \cdot 5$ (also weder prim noch Primpotenz). Also $\varphi(15) = (3-1) \cdot (5-1) = 2 \cdot 4 = 8$. Wir wissen dann $2^8 \equiv 1 \bmod 15$. Insgesamt wieder:

$$2^{15-1} = 2^{14} = 2^8 \cdot 2^6 \equiv 1 \cdot \frac{2^8}{4} \equiv \frac{1}{4} \equiv 4 \bmod 15.$$

Für $n = 1105$ berechnen wir $2^{(10001010000)_2}$:

$$\begin{aligned}
2^{(10)_2} &\equiv 4 \bmod 1105, & 2^{(1000100)_2} &\equiv 1036 \bmod 1105,\\
2^{(100)_2} &\equiv 16 \bmod 1105, & 2^{(1000101)_2} &\equiv 967 \bmod 1105,\\
2^{(1000)_2} &\equiv 256 \bmod 1105, & 2^{(10001010)_2} &\equiv 259 \bmod 1105,\\
2^{(10000)_2} &\equiv 341 \bmod 1105, & 2^{(100010100)_2} &\equiv 781 \bmod 1105,\\
2^{(10001)_2} &\equiv 682 \bmod 1105, & 2^{(1000101000)_2} &\equiv 1 \bmod 1105,\\
2^{(100010)_2} &\equiv 1024 \bmod 1105, & 2^{(10001010000)_2} &\equiv 1 \bmod 1105.
\end{aligned}$$

Wir erhalten also folgende Tabelle

n	3	5	7	9	11	13	15	17	19	1105
2^{n-1} rem n	1	1	1	4	1	1	4	1	1	1

. ○

1 (ii) Prüfe, für welche dieser n

(a) die Gleichung $2^{n-1} \equiv 1 \bmod n$ gilt.

(b) die Zahl n prim ist.

Vergleiche.

Lösung. Wir erhalten folgende Tabelle

n	3	5	7	9	11	13	15	17	19	1105
2^{n-1} rem n	1	1	1	4	1	1	4	1	1	1
n prim?	t	t	t	f	t	t	f	t	t	f

.

Das Ergebnis 1 für 2^{n-1} rem n ist meist (aber nicht immer!) gleichbedeutend mit Primheit. ◯

(iii) Gilt „n prim $\implies$ $2^{n-1} \equiv 1 \bmod n$“? Begründe. 1

Lösung. Diese Richtung gilt. Wenn n prim ist, dann ist $\varphi(n) = n - 1$ und dann gilt mit dem Satz von Lagrange: $2^{\varphi(n)} = 2^{n-1} \equiv 1 \bmod n$. ◯

(iv) Gilt „$2^{n-1} \equiv 1 \bmod n$ $\implies$ n prim“? Begründe. 1

Lösung. Nein. Das gilt nicht. Das Gegenbeispiel $1105 = 3 \cdot 5 \cdot 17$ haben wir in (i) schon gesehen. Dort gilt 2^{1104} rem $1105 = 1$, obwohl 1105 nicht prim ist. ◯

(v*) Verwende beispielsweise MuPAD oder MAPLE, um alle Zahlen n zwischen 3 und 1000 zu finden, für die Primheit und $2^{n-1} \equiv 1 \bmod n$ nicht äquivalent sind. Gib außer der Lösung auch Dein Mapleprogramm an. *Hilfe*: Schleifen und Bedingungen in Maple gibt man wie im folgenden Beispiel ein: 2*

```
> for n from 3 to 100 do
    A:=(n mod 10=1);
    B:=isprime(2*n+1);
    if A and B then print( n, A, B ); end if;
  end do:
```

Erläuterung des MAPLE*-Codes*: Die Schleife läuft hier von 3 bis 100. Es wird jeweils geprüft, ob die Schleifenvariable n der 1 modulo 10 entspricht (A) und danach, ob $2n + 1$ prim ist (B). Wenn beides zutrifft, werden n, A und B ausgegeben.

Der Doppelpunkt anstelle eines Semikolons am Ende verhindert, dass jedes Zwischenergebnis ausgegeben wird. Mit `print(...)` kann man trotzdem etwas ausgeben; MAPLEs Hilfe dazu erhält man mit `?print`. MAPLE kennt den logischen Operator `xor` und das Prädikat `isprime`. Möchtest Du `A` ein wenig anders sehen, schlag doch mal unter `evalb` nach.

Lösung. Folgende Prozedur liefert die gewünschten Ergebnisse:

```
> for n from 3 to 1000 by 2 do
    A:= (2&^(n-1) mod n = 1);
    B:= isprime(n);
    if A xor B
    then
      print( n, A, B );
    end if;
  end do:
```

Als Ausgaben erhält man dann:

```
341, 1 = 1, false
561, 1 = 1, false
645, 1 = 1, false
```

Auch diese drei Zahlen sind also Gegenbeispiele für (iv). ◯

***Aufgabe 9.4** (Modulare quadratische Gleichung). (0+6 Punkte)

Wir betrachten hier die Gleichung

$$x^2 \equiv 1 \bmod m.$$

Die entsprechende Gleichung über den reellen (oder komplexen) Zahlen hat genau zwei Lösungen, und jede Gleichung der Form $ax^2 + bx + c = 0$ hat jedenfalls höchstens zwei reelle (komplexe) Lösungen. Wir wollen untersuchen, was modulo einer Zahl m passiert.

Wir beginnen mit dem Fall, dass $m = p$ eine Primzahl ist.

1 (i*) Sei $ab \equiv 0 \bmod p$. Zeige, dass dann $a \equiv 0 \bmod p$ oder $b \equiv 0 \bmod p$ ist. *Bemerkung*: Über den reellen (oder komplexen) Zahlen gilt das: Ist $ab = 0$ für zwei reelle (oder komplexe) Zahlen, dann ist $a = 0$ oder $b = 0$.

Lösung. Sei $ab \equiv 0 \bmod p$, das heißt $p \mid ab$. Es gibt also ein t mit $pt = ab$. Die Zahlen t, a und b haben jeweils eine Primfaktorzerlegung und Zusammensetzen liefert zwei Primfaktorzerlegungen der Zahl $pt = ab$. Da Primfaktorzerlegung nach dem Hauptsatz der Zahlentheorie eindeutig ist, müssen diese (bis auf die Reihenfolge der Faktoren) übereinstimmen. Insbesondere muss p auch rechts vorkommen. Damit muss p in a oder in b auftreten. Das heißt $p \mid a$ oder $p \mid b$. ◯

1 (ii*) Gib zwei Lösungen der Gleichung $x^2 \equiv 1 \bmod p$ an.

Lösung. Da $(\pm 1)^2 \equiv 1 \bmod p$ ist, sind $x \equiv 1 \bmod p$ und $x \equiv -1 \bmod p$ Lösungen. Ausser im Fall $p = 2$ sind diese auch modulo p verschieden. (Im Fall $p = 2$ zählt die eine Lösung doppelt.) ◯

(iii*) Zeige, dass es keine weiteren Lösungen gibt. *Tipp*: Schreibe $x^2 - 1$ als Produkt und verwende (i*). 1

Lösung. Sei x ein Rest mit $x^2 \equiv 1 \bmod p$. Dann ist $x^2 - 1 = (x-1)(x+1) \equiv 0 \bmod p$. Nach (i*) folgt $x - 1 \equiv 0 \bmod p$ oder $x + 1 \equiv 0 \bmod p$, das heißt $x \equiv 1 \bmod p$ oder $x \equiv -1 \bmod p$. Damit sind die unter (ii*) angegebenen Lösungen tatsächlich alle, die es gibt. ◯

Nun wollen wir untersuchen, was für ein Produkt $m = pq$ zweier unterschiedlicher Primzahlen p, q geschieht.

(iv*) Seien $s, t \in \mathbb{Z}$ mit $1 = sp + tq$. Zeige, dass $\pm sp \pm tq$ Lösungen von $x^2 \equiv 1 \bmod pq$ sind. 1

Lösung. Nach dem Chinesischen Restsatz genügt es zu zeigen, dass jedes $c = \pm sp \pm tq$ die Gleichung modulo p und modulo q erfüllt (unabhängig von der Vorzeichenwahl). Aber $c \equiv \pm 1 \bmod p$, also ist c Lösung von $x^2 \equiv 1 \bmod p$. Genauso $c \equiv \pm 1 \bmod q$, also ist c Lösung von $x^2 \equiv 1 \bmod q$. Damit ist jeder der vier Werte c eine Lösung der Gleichung $x^2 \equiv 1 \bmod pq$. ◯

(v*) Zeige, dass es modulo m höchstens vier Lösungen gibt. *Tipp*: Kombiniere den chinesischen Restsatz und (iii*). 1*

Lösung. Nach dem Chinesischen Restsatz ist jede Lösung von $x^2 \equiv 1 \bmod pq$ eine Lösung des Systems $x^2 \equiv 1 \bmod p$, $x^2 \equiv 1 \bmod q$ und umgekehrt. Jede Lösung der Gleichung liefert ein Paar (x_p, x_q) von Lösungen des Systems. Jede der Gleichungen des Systems hat nach (iii*) höchstens zwei Lösungen, also hat das System höchstens $2 \cdot 2$ Lösungen, für jedes Paar von Lösungen eine. Und damit hat auch die Gleichung modulo pq höchstens vier Lösungen. ◯

Faktorisierungsalgorithmen versuchen zu einer natürlichen Zahl m ihre Primfaktorzerlegung zu berechnen. Einige beruhen darauf, dass sie (mehr oder minder geschickt) zwei Zahlen finden mit

$$u^2 \equiv v^2 \bmod m, \qquad u \not\equiv \pm v \bmod m.$$

(vi*) Zeige, dass (und wie) man für $m = pq$ aus solchen u und v ganz leicht p und q berechnen kann. [1*]

Lösung. Wenn u und v so gegeben sind, ist $(u+v)(u-v) = u^2 - v^2 \equiv 0 \bmod m$, das heißt $m \mid (u+v)(u-v)$. Aber wegen $u \not\equiv \pm v \bmod p$ ist weder $u+v$ noch $u-v$ durch m teilbar. Die Faktoren von m müssen sich daher echt auf $u+v$ und $u-v$ verteilen. Daher sind $\mathrm{ggT}(m, u+v)$ und $\mathrm{ggT}(m, u-v)$ echte Teiler von m. Im Falle, dass m ein Produkt von zwei Primzahlen ist, erhalten wir so diese beiden Primzahlen. ◯

***Aufgabe 9.5** (Rabin Entschlüsselung). (0+5 Punkte)

Das Rabin-Verfahren arbeitet mit einem Produkt N zweier Primzahlen p und q, die beide kongruent 3 modulo 4 sind. Die zu verschlüsselnde Zahl wird dann modulo N quadriert. Wir wollen hier sehen, wie man diesen Quadrierungsschritt modulo der Primzahl p rückgängig machen kann.

(i*) Zeige, dass $\frac{p+1}{4}$ eine ganze Zahl ist. [1]

Lösung. Weil $p \equiv 3 \bmod 4$ ist, erhalten wir $p+1 \equiv 0 \bmod 4$, also $4 \mid (p+1)$. Das heißt $\frac{p+1}{4} \in \mathbb{Z}$. ◯

(ii*) Zeige $a^{p+1} \equiv a^2 \bmod p$. [1]

Lösung. Nach dem kleinen Satz von Fermat gilt $a^p \equiv a \bmod p$. Daraus folgt die Behauptung durch Multiplikation mit a. ◯

(iii*) Schließe, $a^{\frac{p+1}{2}} \equiv \pm a \bmod p$. *Tipp*: Verwende (ii*) und *Aufgabe 9.4(iii*). [1]

Lösung. Für $a \equiv 0 \bmod p$ ist die Behauptung klar. Sei also $a \not\equiv 0 \bmod p$ und damit a invertierbar modulo p. Wir haben $\left(a^{\frac{p+1}{2}}\right)^2 \equiv a^{p+1} \equiv a^2 \bmod p$, also $\left(\frac{a^{\frac{p+1}{2}}}{a}\right)^2 \equiv 1 \bmod p$. Weil eine Gleichung der Form $x^2 \equiv 1 \bmod p$ höchstens zwei Lösungen modulo p haben kann und diese ± 1 sind, muss $\frac{a^{\frac{p+1}{2}}}{a}$ eine davon sein. Also folgt

$$a^{\frac{p+1}{2}} \equiv \pm a \bmod p.$$ ◯

(iv*) Sei $b = a^2$ und $w = b^{\frac{p+1}{4}}$. Zeige $a \equiv \pm w \bmod p$. Mit anderen Worten: w ist eine Wurzel aus b. [1]

Lösung. Es gilt $w = b^{\frac{p+1}{4}} = \left(a^2\right)^{\frac{p+1}{4}} = a^{2 \cdot \frac{p+1}{4}} = a^{\frac{p+1}{2}}$. Nach (iii*) ist dann $w \equiv \pm a \bmod p$. ◯

Damit können wir also modulo einer Primzahl, die kongruent 3 modulo 4 ist, Wurzeln ziehen aus einer Zahl, die ein Quadrat ist.

Mit Hilfe des chinesischen Restsatzes lassen sich Wurzeln auch modulo N ziehen. Sei $b \equiv a^2 \bmod N$.

(v*) Seien $s, t \in \mathbb{Z}$ mit $1 = sp + tq$ und $c = \pm spb^{\frac{q+1}{4}} \pm tqb^{\frac{p+1}{4}}$. Zeige, dass in jedem der vier Fälle $c^2 \equiv b \bmod N$ gilt. 1*

Lösung. Nach dem Chinesischen Restsatz (Eindeutigkeit, Aufgabe 8.6) genügt es $c^2 \equiv b \bmod p$ und $c^2 \equiv b \bmod q$ zu prüfen. Aber $c \equiv b^{\frac{p+1}{4}} \bmod p$, also ist nach (iv*) $c \equiv \pm a \bmod p$. Ebenso ist $c \equiv b^{\frac{q+1}{4}} \bmod q$ und mit (iv*) $c \equiv \pm a \bmod q$. Damit ist $c^2 \equiv b \bmod p$ und $c^2 \equiv b \bmod q$, also $c^2 \equiv b \bmod pq$. ◯

Nach *Aufgabe 9.4(v*) kann es nicht mehr Lösungen geben, wir haben also alle gefunden. Aus diesen vier Lösungen muss man zur Rabin-Entschlüsselung die richtige raten, was leicht möglich ist, wenn natürlicher Text verschlüsselt wurde wie in Aufgabe 5.3. (Beachte, dass $N = 66013$ den oben genannten Anforderungen genügt.)

Lösung. Wir bemerken zusätzlich, dass die Rechnung in (v*) so nur durchführbar ist, wenn p und q bekannt sind. Man kann sogar beweisen, dass ein Angreifer, der $c^2 \equiv b \bmod N$ lösen kann, auch in der Lage ist, N zu zerlegen. Da das aber als schwierig gilt, ist ein Angriff mindestens gleich schwierig. ◯