Wolfgang K. Seiler
Tel. 2515

A5, C201

14. Juni 2018

Modulklausur Zahlentheorie

• • • **Schreiben Sie bitte auf jedes Blatt Ihren Namen!** • • •

Aufgabe 1: *(7 Punkte)*

a) $a_0, \ldots, a_r$ seien ganze Zahlen und $e_0, \ldots, e_r \in \mathbb{N}_0$. Zeigen Sie: $\sum_{i=0}^{r} a_i 10^{e_i} \equiv \sum_{i=0}^{r} a_i \bmod 9$

Lösung: Wegen $10 \equiv 1 \bmod 9$ ist auch $10^e \equiv 1 \bmod 9$ für alle $e \in \mathbb{N}_0$.

b) Eine natürliche Zahl n ist genau dann durch neun teilbar, wenn die Summe ihrer Dezimalziffern (ihre Quersumme) durch neun teilbar ist.

Lösung: Das ist der Spezialfall von *a)* bei dem alle $e_i = i$ sind und $a_i \in \{0, 1, \ldots, 9\}$.

c) $n \in \mathbb{N}$ sei die Dezimalzahl, die entsteht, wenn man die Zahlen von eins bis 100 ohne Zwischenräume hintereinander schreibt, also

$$n = 12345678910111213 \ldots 96979899100\,.$$

Bestimmen Sie die Reste von n bei der Division durch $a = 2, 3, 4, 5, 6, 72, 8, 9, 10$! (Die 72 an Stelle von 7 ist **kein** Druckfehler: Der Rest modulo 7 wäre nur mit großem Aufwand zu bestimmen; der modulo 72 läßt sich einfach aus den anderen berechnen.)

Lösung: n ist durch hundert teilbar, also erst recht durch $2, 4, 5$ und 10. Setzen wir $a_i = i$ läßt sich n mit geeigneten e_i in der Form aus *a)* schreiben; somit ist

$$n \equiv \sum_{i=1}^{100} a_i = \sum_{i=1}^{100} i = \frac{100 \cdot 101}{2} = 5050 \equiv 5 + 5 = 10 \equiv 1 \bmod 9\,,$$

und damit ist auch $n \equiv 1 \bmod 3$.

Da $n \equiv 1 \bmod 3$, ist $n \equiv 1 \bmod 6$ oder $n \equiv 4 \bmod 6$. Da n gerade ist, kommt nur die zweite Möglichkeit in Betracht.

Da 1000 und jedes Vielfache davon durch acht teilbar sind, ist $n \equiv 100 \equiv 4 \bmod 8$.

$72 = 8 \cdot 9$; wie wir bereits wissen, ist $n \equiv 4 \bmod 8$ und $n \equiv 1 \bmod 9$. Da acht und neun teilerfremd sind, können wir den chinesischen Restesatz anwenden, um $n \bmod 72$ zu bestimmen:

$$9 \equiv \begin{cases} 1 & \bmod 8 \\ 0 & \bmod 9 \end{cases} \quad \text{und} \quad -8 \equiv \begin{cases} 0 & \bmod 8 \\ 1 & \bmod 9 \end{cases};$$

somit ist $n \equiv -8 \cdot 1 + 9 \cdot 4 = 28 \bmod 72$. Der gesuchte Divisionsrest ist also 28.

d) Als gerade Zahl kann n natürlich nicht prim sein. Wenn wir hinten noch die Zahl 101 anhängen, erhalten wir eine ungerade Zahl m. Ist m eine Primzahl?

Lösung: Nach *a)* ist $m \equiv \sum_{i=1}^{101} i = \frac{1}{2} \cdot 101 \cdot 102 \bmod 9$. Da 102 durch drei teilbar ist, gilt dasselbe für m, so daß auch m keine Primzahl ist.

Aufgabe 2: *(6 Punkte)*

Bei der Fußballweltmeisterschaft feiern in einem Restaurant einige Fußballspieler sowie bayrische und russische Fans. Um unsere Vorurteile zu respektieren, bestellt jeder bayrische Fan eine Maß Bier und jeder russische Fan hundert Gramm Wodka. Die Fußballspieler sind in Gruppen von jeweils elf Freunden gekommen, und eingedenk der Ermahnungen seines Trainers bestellt jeder von ihnen ein Glas Mineralwasser. Eine Maß Bier kostet 300 Rubel, hundert Gramm Wodka hundert Rubel und ein Glas Mineralwasser 600 Rubel. Der Kellner serviert siebzig Getränke und kassiert (ohne Trinkgeld) 21 400 Rubel. Wie viele Fußballspieler und wie viele bayrische *bzw.* russische Fans sind anwesend?

Lösung: x sei die Anzahl der Fußballspieler, y die der bayrischen Fans und z die der russischen. Wenn wir die Preise der Einfachheit halber in hundert Rubel ausdrücken, erhalten wir die beiden Gleichungen

$$x + y + z = 70 \quad \text{und} \quad 6x + 3y + z = 214\,.$$

Außerdem ist x durch elf teilbar.

Substituieren wir $z = 70 - x - y$ in der zweiten Gleichung, erhalten wir

$$5x + 2y = 214 - 70 = 144\,.$$

Der ggT eins von fünf und zwei läßt sich als $1 = 5 \cdot 1 - 2 \cdot 2$ darstellen; also ist

$$144 = 5 \cdot 144 - 2 \cdot 288\,.$$

Von dieser Gleichung können wir noch Vielfache von $0 = 5 \cdot 2 - 2 \cdot 5$ subtrahieren; die allgemeine ganzzahlige Lösung ist also

$$x = 144 - 2k, \quad y = -288 + 5k \quad \text{und} \quad z = 70 - x - y = 214 - 3k\,.$$

Da x, y, z positiv sein müssen, ist $k < 72$, $k > 288/5 > 57$ und $k < 214/3 < 72$, d.h. $58 \le k \le 71$. Damit liegt x zwischen $154 - 2 \cdot 71 = 12$ und $154 - 2 \cdot 58 = 38$ und ist eine gerade, durch elf teilbare Zahl. Somit ist $x = 22$ und $k = 61$, also $y = 5 \cdot 61 - 288 = 17$ und $z = 70 - 22 - 17 = 31$.

Anwesend sind somit 22 Spieler, 17 bayrische und 31 russische Fans.

Aufgabe 3: *(8 Punkte)*

a) Berechnen Sie im Körper $\mathbb{F}_{101}$ die Elemente

$$x_1 = 9^2 + 10^2 + 12^2, \qquad x_2 = 25 \cdot 40 \quad \text{und} \quad x_3 = \frac{5}{33}$$

Lösung: In $\mathbb{F}_{101}$ ist $9^2 = 81 = -20$, $10^2 = 100 = -1$ und $12^2 = 144 = 43$, also $x_1 = -20 - 1 - 43 = 22$.

$x_2 = 25 \cdot 40 = 1000$; wegen $100 = -1$ ist $x_2 = -10 = 91$.

Zur Berechnung von x_3 müssen wir zunächst über den erweiterten EUKLIDischen Algorithmus das multiplikative Inverse von 33 bestimmen:

$$\begin{aligned} 101 : 33 = 3 \text{ Rest } 2 &\Longrightarrow 2 = 101 - 3 \cdot 33 \\ 33 : 2 = 16 \text{ Rest } 1 &\Longrightarrow 1 = 33 - 16 \cdot (101 - 3 \cdot 33) = 49 \cdot 33 - 16 \cdot 101 \end{aligned}$$

Somit ist $49 \cdot 33 \equiv 1 \bmod 101$; im Körper $\mathbb{F}_{101}$ ist also $x_3 = 5/33 = 5 \cdot 49 = 245 = 43$. Zur Probe können wir noch nachrechnen, daß in der Tat $43 \cdot 33 = 1419 = 14 \cdot 101 + 5$ ist.

b) Zeigen Sie, daß in $\mathbb{F}_{101}$ gilt $\prod_{i=1}^{99} i = 1$!

Lösung: Nach der WILSONschen Kongruenz ist $100! = \prod_{i=1}^{100} i \equiv -1 \bmod 101$; wegen $100 \equiv -1 \bmod 101$ ist das Produkt also kongruent zu $+1$, wenn man den Faktor 100 wegläßt.

c) Zeigen Sie, daß zwei eine primitive Wurzel modulo 101 ist!

Lösung: $101-1 = 100 = 2^2 \cdot 5^2$; ein Element a ist also genau dann eine primitive Wurzel, wenn $a^{100} \equiv 1 \bmod 101$ ist, aber a^{20} und a^{50} modulo 101 beide von eins verschieden sind.
$2^{10} = 1024 \equiv 14 \bmod 101$; also ist $2^{20} \equiv 14^2 = 196 \equiv -6 \bmod 101$ offensichtlich von eins verschieden.
$2^{50} = 2^{20} \cdot 2^{20} \cdot 2^{10} \equiv (-6)^2 \cdot 14 = 504 \equiv -1 \bmod 101$ ist ebenfalls von eins verschieden, aber das Quadrat 2^{100} ist kongruent eins. Somit ist zwei in der Tat eine primitive Wurzel.

d) Finden Sie alle Lösungen der Gleichung $x^2 + 1 = 0$ in $\mathbb{F}_{101}$!

Lösung: Die Gleichung ist äquivalent zu $x^2 = -1 = 100$, hat also offensichtlich ± 10 als Lösungen. Da wir in einem Körper sind, kann es nicht mehr als zwei Lösungen geben; somit sind $x = 10$ und $x = 101 - 10 = 91$ die einzigen Lösungen.

Aufgabe 4: *(8 Punkte)*
$2018 = 2 \cdot 1009$, und 1009 ist eine Primzahl.

a) Welche Zahlen zwischen null und 2017 sind invertierbar modulo 2018, und wie viele sind das?

Lösung: Das sind alle, die teilerfremd zu 2018 sind, also weder durch zwei noch durch 1009 teilbar. Im angegebenen Bereich sind das alle ungeraden Zahlen außer 1009, also 1008 Stück.

b) Wie viele Elemente hat die prime Restklassengruppe modulo $2 \cdot 2018 = 4036$?

Lösung: Die Primzerlegung von 4036 ist $2^2 \cdot 1009$, also ist

$$\varphi(4036) = \varphi(2^2) \cdot \varphi(1009) = (2^2 - 2) \cdot (1009 - 1) = 2016\,.$$

(Alternativ kann man natürlich auch wie bei *a)* argumentieren.)

c) Hat die Kongruenz $x^2 \equiv 7 \bmod 1009$ ganzzahlige Lösungen?

Lösung: Da 1009 eine Primzahl ist, gilt dies genau dann, wenn das LEGENDRE-Symbol $\left(\frac{7}{1019}\right) = 1$ ist. Da $1019 \equiv 1 \bmod 4$ ist und $1009 : 7 = 144$ Rest 1, gilt nach dem quadratischen Reziprozitätsgesetz

$$\left(\frac{7}{1009}\right) = \left(\frac{1009}{7}\right) = \left(\frac{1}{7}\right) = 1\,,$$

denn eins ist natürlich ein quadratischer Rest modulo sieben. Somit ist die Kongruenz lösbar.

d) Hat die Kongruenz $x^2 \equiv 7 \bmod 2018$ ganzzahlige Lösungen?

Lösung: Wie wir gerade gesehen haben, gibt es $x \in \mathbb{Z}$ mit $x^2 \equiv 7 \bmod 1009$. Außerdem gibt es $y \in \mathbb{Z}$ mit $y^2 \equiv 7 \bmod 2$, beispielsweise $y = 1$. Nach dem chinesischen Restesatz lassen sich aus x und y Zahlen z bestimmen, mit $z^2 \equiv 7 \bmod 2018$. Die Kongruenz ist daher lösbar.

e) Auf welchen Wochentag fällt der 1. März 4036 ?

Lösung: Die Nummer des Wochentags ist modulo sieben kongruent zu

$$4035+\left[\frac{4035}{4}\right]-\left[\frac{4035}{100}\right]+\left[\frac{4035}{400}\right]+31+29+1 = 4035+1008-40+10+61 = 5074 \equiv 6 \bmod 7\,.$$

Der 1. März 4036 ist also ein Samstag.

Aufgabe 5: (*7 Punkte)*

a) Die Zahl $N = 21\,040\,553$ ist Produkt zweier ungefähr gleich großer Primzahlen. Bestimmen Sie diese!

Lösung: In dieser Situation bietet sich das Verfahren von FERMAT an, d.h. wir suchen ein i, für das $N + i^2$ eine Quadratzahl ist. Für $i = 0, 1, 2, 3$ ist $\sqrt{N + i^2}$ keine ganze Zahl, aber

$$N + 4^2 = 21\,040\,569 = 4587^2\,.$$

Somit ist $N = 4587^2 - 4^2 = (4587 - 4)(4587 + 4) = 4583 \cdot 4591$

b) Wenn wir alle Empfehlungen bezüglich der Größe der Parameter ignorieren, können wir N als RSA-Modul verwenden. Bestimmen Sie den kleinstmöglichen Exponenten, mit dem das funktioniert!

Lösung: e muß teilerfremd sein zu $p - 1 = 4582$ und zu $q - 1 = 4590$. Damit muß e insbesondere ungerade sein. 4590 ist sowohl durch drei als auch durch fünf teilbar, also kommen diese Zahlen nicht in Frage. Bei Division durch sieben hat 4582 den Rest vier und 4590 Rest fünf, also ist $e = 7$ der kleinstmögliche öffentliche Exponent.

c) Finden Sie dazu einen möglichst kleinen privaten Exponenten d !

Lösung: $q - 1$ ist offensichtlich durch zwei, fünf und neun teilbar; Division durch deren Produkt 90 ergibt den Quotienten $51 = 3 \cdot 17$. Somit ist $4590 = 2 \cdot 3^3 \cdot 5 \cdot 17$. Wäre $p-1$ durch drei, fünf oder siebzehn teilbar, so auch die Differenz $q - p = 8$, und das ist offensichtlich nicht der Fall. Das kleinste gemeinsame Vielfache von $p - 1$ und $q - 1$ ist daher

$$\lambda = \frac{(p-1)(q-1)}{2} = \frac{4582 \cdot 4590}{2} = 10\,515\,690\,.$$

Wir müssen eins als Linearkombination aus dieser Zahl und sieben ausdrücken, also den erweiterten EUKLIDischen Algorithmus anwenden:

$$10\,515\,690 : 7 = 1\,502\,241 \text{ Rest } 3 \Longrightarrow 3 = 10\,515\,690 - 7 \cdot 1\,502\,241$$
$$7 : 3 = 2 \text{ Rest } 1 \Longrightarrow 1 = 7 - 2 \cdot (10\,515\,690 - 7 \cdot 1\,502\,241) = 3\,004\,483 \cdot 7 - 2 \cdot 10\,515\,690\,.$$

Somit können wir $d = 3\,004\,483$ wählen.

Aufgabe 6: (*8 Punkte)*

a) Bestimmen Sie die Kettenbruchentwicklung von $\sqrt{12} = 2\sqrt{3}$!

Lösung: Da $3^2 < 12 < 4^2$, ist der ganzzahlige Anteil drei; der Kehrwert der Differenz ist

$$\frac{1}{\sqrt{12} - 3} = \frac{\sqrt{12} + 3}{12 - 3^2} = 1 + \frac{\sqrt{12}}{3}$$

und hat ganzzahligen Anteil zwei. Bilden wir wieder den Kehrwert der Differenz

$$\frac{1}{\frac{1}{3}\sqrt{12}-1} = \frac{3}{\sqrt{12}-3} = \frac{3(\sqrt{12}+3)}{3} = \sqrt{12}+3\,,$$

so ist dessen ganzahliger Anteil sechs. Die Differenz ist $\sqrt{12}-3$, was wir schon oben hatten, d.h. ab hier wir alles periodisch und

$$\sqrt{12} = 3 + \cfrac{1}{2+\cfrac{1}{6+\cfrac{1}{2+\cfrac{1}{6+\cdots}}}}\,.$$

b) Finden Sie eine ganzzahlige Lösung der Gleichung $x^2 - 12y^2 = 1$!

Lösung: Aus $x^2 - 12y^2 = 1$ folgt

$$\left(\frac{x}{y}\right)^2 - 12 = \left(\frac{x}{y} - \sqrt{12}\right)\left(\frac{x}{y} + \sqrt{12}\right) = \frac{1}{y^2} \Longrightarrow \frac{x}{y} - \sqrt{12} = \frac{1}{y^2\left(\frac{x}{y} + \sqrt{12}\right)}\,.$$

Wegen $\left(\frac{x}{y}\right)^2 > 1$ ist $\frac{x}{y} > \sqrt{12}$, also ist der Nenner rechts insbesondere größer als $2y^2$, und damit muß x/y nach LEGENDRE eine Konvergente der Kettenbruchentwicklung von $\sqrt{12}$ sein.
Wir müssen also die Nenner und Zähler der Konvergenten der Kettenbruchentwicklung durchprobieren. $3 = \frac{3}{1}$ liefert $3^2 - 12\cdot 1^2 = -3$. Die nächste Konvergente ist $3\frac{1}{2} = \frac{7}{2}$, und $7^2 - 12\cdot 2^2 = 1$. Somit ist $x = 7, y = 2$ eine Lösung.

c) Finden Sie einen Näherungsbruch mit möglichst kleinem Nenner, der sich höchstens um 10^{-3} von $611/576$ unterscheidet! Beweisen Sie diese Schranke, ohne die Dezimaldarstellung der relevanten Brüche zu berechnen.

Lösung: Die besten Näherungen sind die Konvergenten der Kettenbruchentwicklung; ist p/q eine solche Konvergente, so ist der Betrag der Abweichung kleiner als $1/q^2$.

$$\frac{611}{576} = 1 + \frac{35}{576} \quad \text{und} \quad \frac{576}{35} = 16 + \frac{16}{35}\,;$$

der erste Näherungsbruch ist also $1\frac{1}{16}$. Da $16^2 = 2^8 = 256$ kleiner als Tausend ist, reicht das noch nicht.
$\frac{35}{16} = 2 + \frac{3}{16}$, der nächste Näherungsbruch ist also

$$1 + \frac{1}{16 + \frac{1}{2}} = 1\frac{2}{33} = \frac{35}{33}\,.$$

Da $33^2 = 1089 > 1000$ ist, unterscheidet sich dieser Bruch um höchstens ein Tausendstel von $611/576$.

Aufgabe 7: *(8 Punkte)*

a) Zeigen Sie, das $2i$ im Ring $\mathbb{Z} \oplus \mathbb{Z}i$ der GAUSSschen Zahlen als Quadrat eines irreduziblen Elements geschrieben werden kann!

Lösung: Bekanntlich ist $2 = (1+i)(1-i)$, also ist

$$2i = (1+i) \cdot \big(i(1-i)\big) = (1+i)(i+1) = (1+i)^2 .$$

$1+i$ ist irreduzibel, da seine Norm zwei eine Primzahl ist.

b) Zerlegen Sie $34i$ in $\mathbb{Z} \oplus \mathbb{Z}i$ in ein Produkt von Potenzen nicht assoziierter irreduzibler Elemente!

Lösung: $34 = 2 \cdot 17$. Da $17 \equiv 1 \bmod 4$ und prim ist, läßt sich diese Zahl als Summe zweier Quadrate schreiben; in der Tat ist $17 = 4^2 + 1^2$. Somit ist $17 = (4+i)(4-i)$. Beide Faktoren sind irreduzibel, da ihre Norm die Primzahl 17 ist, und sie sind nicht assoziiert, da es in $\mathbb{Z} \oplus \mathbb{Z}i$ nur die vier Einheiten ± 1 und $\pm i$ gibt und der Quotient der beiden Zahlen mit keiner davon übereinstimmt. Zusammen mit *a)* folgt, daß

$$34i = (1+i)^2(4+i)(4-i)$$

die gesuchte Zerlegung ist.

c) Finden Sie, ausgehend von *a)* und *b),* alle Darstellungen von 34 als Summe zweier Quadrate!

Lösung: Da $34 = 2 \cdot 17$ nur einen Primteiler kongruent eins modulo vier hat, gibt es bis auf Reihenfolge nur eine solche Darstellung.

$$34 = 2{\cdot}17 = (1{+}I)(1{-}I)(4{+}i)(4{-}1) = \big((1{+}i)(4{+}i)\big)\big((1{-}i)(4{-}i)\big) = (3{+}5i)(3{-}5i) = 3^2{+}5^2 .$$

d) Bestimmen Sie alle Elemente der Norm 34 in $\mathbb{Z} \oplus \mathbb{Z}i$!

Lösung: Die Norm von $a+bi$ ist a^2+b^2; nach *c)* ist das nur für die Zahlen $\pm 3 \pm 5i$ und $\pm 5 \pm 3i$ gleich 34.

e) Berechnen Sie in $\mathbb{Z} \oplus \mathbb{Z}i$ den ggT von $7+19i$ und 10!

Lösung: $\frac{7+19i}{10} = \frac{7}{10} + \frac{19}{10}i$ hat $1+2i$ als nächstgelegene Zahl aus $\mathbb{Z} \oplus \mathbb{Z}i$; wir können also setzen

$$(7+19i) : 10 = 1+2i \text{ Rest } -3-i .$$

Im nächsten Schritt ist

$$\frac{10}{-3-i} = \frac{-30+10i}{(-3-i)(-3+i)} = -\frac{30+10i}{10} = -3+i ;$$

Die Division geht also auf ohne Rest; somit ist der ggT gleich $-3-i$. Da ein ggT nur bis auf Einheiten eindeutig bestimmt ist, können wir noch beispielsweise mit der Einheit -1 multiplizieren, um das etwas schönere Ergebnis $3+i$ zu bekommen; wir könnten auch mit $-i$ multiplizieren und „den“ ggT als $1+3i$ darzustellen.

Aufgabe 8: *(8 Punkte)*

$p_1, \ldots, p_r$ seien verschiedene Primzahlen, und N sei ihr Produkt.

a) Wie viele Elemente hat die prime Restklassengruppe $(\mathbb{Z}/N)^\times$?

Lösung: Die Ordnung der primen Restklassengruppe ist

$$\varphi(N) = \varphi(p_1) \cdots \varphi(p_r) = (p_1 - 1) \cdots (p_r - 1)\,.$$

b) λ sei ein gemeinsames Vielfaches aller Zahlen $p_i - 1$. Zeigen Sie, daß $a^{\lambda+1} \equiv a \bmod N$ für **alle** $a \in \mathbb{Z}$.

Lösung: Ist a teilerfremd zu p_i, so ist $a^{p_i-1} \equiv 1 \bmod p_i$ nach dem kleinen Satz von FERMAT. Da λ ein Vielfaches von $p_i - 1$ ist, folgt, daß dann auch $a^\lambda \equiv 1 \bmod p_i$ ist und damit $a^{\lambda+1} \equiv 1 \bmod p_i$.

Eine nicht zu p_i teilerfremde Zahl a ist durch p_i teilbar, und dasselbe gilt natürlich auch für $a^{\lambda+1}$, d.h. $a^{\lambda+1} \equiv 0 \equiv a \bmod p_i$.

Somit ist $a^{\lambda+1} \equiv a \bmod p_i$ für alle $a \in \mathbb{Z}$. Da dies für alle i gilt, folgt $a^{\lambda+1} \equiv a \bmod N$ für alle $a \in \mathbb{Z}$.

c) e sei teilerfremd zu allen Zahlen $p_i - 1$. Zeigen Sie, daß die Abbildung

$$\begin{cases} \mathbb{Z}/N \to \mathbb{Z}/N \\ \quad x \mapsto x^e \end{cases}$$

bijektiv ist!

Lösung: λ sei das kleinste gemeinsame Vielfache der Zahlen $p_i - 1$. (Man könnte auch das Produkt nehmen.) Nach *b)* ist dann $a^{\lambda+1} \equiv a \bmod N$ für alle $a \in \mathbb{Z}$.

Da e teilerfremd zu allen $p_i - 1$ ist, ist es auch teilerfremd zu λ; der erweiterte EUKLIDische Algorithmus liefert also Zahlen d, k mit $de - k\lambda = 1$. Durch Addition eines Vielfachen der Gleichung $e\lambda - \lambda e = 0$ können wir gegebenenfalls erreichen, daß d und k beide positiv sind.

Dann ist $a^{de} = a^{1+k\lambda} \equiv a \bmod N$ für alle $a \in \mathbb{Z}$, denn mit λ ist auch $k\lambda$ ein gemeinsames Vielfaches aller $p_i - 1$, so daß wir *b)* anwenden können.

Dies zeigt, daß die Abbildung

$$\begin{cases} \mathbb{Z}/N \to \mathbb{Z}/N \\ \quad x \mapsto x^d \end{cases}$$

invers zur obigen Abbildung ist, so daß beide bijektiv sein müssen.

d) Folgern Sie, daß man beim RSA-Verfahren auch einen Modul N benutzen kann, der Produkt von mehr als zwei (paarweise verschiedenen) Primzahlen ist, und begründen Sie, warum man das nicht tut.

Lösung: Wie die Lösung von *c)* zeigt, kann jemand, der die Faktorisierung von N kennt eine Umkehrabbildung zur Potenzierung mit e bestimmen, und alles funktioniert genauso wie bei RSA. Bei einer vorgegebenen Größe von N wird allerdings mit steigender Anzahl die Größe des kleinsten Faktors immer kleiner, was die Faktorisierung von N erleichtert. RSA mit mehr als zwei Faktoren wäre somit unsicherer als das klassische Verfahren mit nur zwei Primzahlen.