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: $\sum_{i=0}^{r} a_i 10^{e_i} \equiv \sum_{i=0}^{r} a_i \bmod 9$

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

*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.)

*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?

**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?

**Aufgabe 3:** (*8 Punkte*)

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

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

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

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

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

• • • **Bitte wenden!** • • •

**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?

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

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

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

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

**Aufgabe 5:** (*7 Punkte*)

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

*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!

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

**Aufgabe 6:** (*8 Punkte*)

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

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

*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.

**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!

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

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

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

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

**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 $(\mathbb{Z}/N)^\times$ ?

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

*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!

*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.

**Abgabe** bis zum Donnerstag, dem 14. Juni 2018, um $15^{30}$ Uhr

• • • **Steht Ihr Name auf jedem Blatt?** • • •