Wolfgang K. Seiler
*Tel.* 2515

A5, C201

*25. August 2014*

# Modulklausur Zahlentheorie

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

**Aufgabe 1:** (*5 Punkte*)

Die *alternierende Quersumme* einer natürlichen Zahl $n$ wird berechnet, indem man ihre Dezimalziffern, ausgehend von der niedrigsten, abwechselnd positiv und negativ nimmt und diese Zahlen aufaddiert; die alternierende Quersumme von 12345 ist demnach also $5-4+3-2+1=3$.

*a)* Zeigen Sie, daß eine natürliche Zahl $n$ genau dann durch elf teilbar ist, wenn ihre alternierende Quersumme durch elf teilbar ist!

*b)* Ist jede natürliche Zahl $n$ modulo elf kongruent zu ihrer alternierenden Quersumme?

*c)* Wie verhält es sich mit *a)* und *b)*, wenn man bei der Berechnung der *alternierenden Quersumme* mit der höchsten Dezimalziffer anfängt?

*d)* Welchen Rest hat die Zahl $n = 3141592654$ bei der Division durch elf?

**Aufgabe 2:** (*6 Punkte*)

*a)* Wie viele Elemente hat die prime Restklassengruppe $(\mathbb{Z}/19800)^\times$ ?
*(Hinweis: Die alternierende Quersumme von 19800 ist null.)*

*b)* $n = 4704977$ ist ein Produkt zweier Primzahlen, und $\varphi(n) = 4700160$. Bestimmen Sie die Primzerlegung von $n$ ausgehend von diesen Informationen!

*c)* Bestimmen Sie den kleinsten Exponenten $r$, für den $a^r \equiv 1 \bmod n$ gilt für alle zu $n$ teilerfremden ganzen Zahlen $a$!

**Aufgabe 3:** (*9 Punkte*)

*a)* Berechnen Sie im Körper $\mathbb{F}_{31}$ die Elemente

$$x_1 = 5 - 3^2, \qquad x_2 = 2^5, \qquad x_3 = 2^{2014}, \qquad x_4 = \frac{3}{25} \quad \text{und} \quad x_5 = 29! = \prod_{i=1}^{29} i$$

*b)* Bestimmen Sie die kleinste natürliche Zahl, die eine primitive Wurzel modulo 31 ist!

*c)* Geben Sie zu jeder möglichen Ordnung eines Elements von $\mathbb{F}_{31}^\times$ ein Element an, das exakt diese Ordnung hat!

**Aufgabe 4:** (*4 Punkte*)

*a)* Der (wenn auch vielleicht nicht unter Bachelorstudenten) bekannte Mathematiker Maxim Kontsevich feiert heute seinen fünfzigsten Geburtstag. An welchem Wochentag wurde er geboren?

*b)* Der ehemalige indische Premierminister Moraji Desai wurde am 29. Februar 1896 geboren und starb am 10. April 1995. Wie oft konnte er seinen Geburtstag an einem 29. Februar feiern? (1896 war er natürlich noch zu jung zum Feiern.)

• • • **Bitte wenden!** • • •

**Aufgabe 5:** (*8 Punkte*)

*a)* Die Zahl $N = 98587$ hat keinen Primteiler, der wesentlich kleiner ist als ihre Quadratwurzel. Bestimmen Sie ihre Primzerlegung!

*b)* Welche Zahlen $1 < e < 10$ kommen als öffentliche Exponenten für ein RSA-System mit Modul $N$ in Frage?

*c)* Bestimmen Sie für den öffentlichen Exponenten $e = 19$ einen möglichst kleinen privaten Exponenten!

*d)* Wie viele Multiplikationen modulo $N$ sind notwendig, um eine Nachricht in diesem System mit $e = 19$ zu verschlüsseln?

**Aufgabe 6:** (*10 Punkte*)

*a)* Bestimmen Sie die Kettenbruchentwicklung von $\sqrt{5}$!

*b)* Finden Sie einen Näherungsbruch für $\sqrt{5}$ mit möglichst kleinem Nenner, der sich höchstens um $10^{-2}$ von $\sqrt{5}$ unterscheidet!

*c)* Finden Sie eine ganzzahlige Lösung der Gleichung $x^2 - 5y^2 = 1$!

*d)* In der Kettenbruchentwicklung der reellen Zahl $x$ seien alle Koeffizienten gleich der natürlichen Zahl $a$, d.h.

$$x = [\overline{a}] = a + \cfrac{1}{a + \cfrac{1}{a + \ddots}}\,.$$

Bestimmen Sie $x$!

*e)* Was erhalten Sie speziell für $a = 4$?

**Aufgabe 7:** (*8 Punkte*)

*a)* Zeigen Sie, ausgehend von der Kongruenz $20206^2 \equiv 1 \bmod 54329$, daß $p = 54329$ keine Primzahl sein kann!

*b)* Wie lassen sich aus obiger Gleichung zwei nichttriviale Faktoren von $p$ bestimmen? (Die Faktoren müssen nicht berechnet werden.)

*c)* Führen Sie für $p$ sowohl den FERMAT-Test als auch den Test von MILLER und RABIN für die Basis $a = 20206$ durch! Sie können dabei neben der Kongruenz aus *a)* auch noch benutzen, daß $p - 1 = 8 \times 6791$ ist und $a^{6791} \equiv a \bmod p$.

**Aufgabe 8:** (*10 Punkte*)

Untersuchen Sie, welche der folgenden Kongruenzen lösbar sind, und bestimmen Sie gegebenenfalls eine Lösung:

*a)* $x^2 \equiv 7 \bmod 31$

*b)* $x^2 \equiv 11 \bmod 35$

*c)* $x^2 \equiv 13 \bmod 37$

*d)* Die natürliche Zahl $n$ sei kongruent sieben modulo acht. Zeigen sie, daß $n$ nicht als Summe dreier Quadratzahlen geschrieben werden kann! *(Hinweis: Betrachten Sie die Quadrate modulo acht!)*

**Abgabe** bis zum Montag, dem 25. August 2014, um $10^{30}$ Uhr

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