Wolfgang K. Seiler
Tel. 2515

A5, C201

13. Juni 2014

Modulklausur Zahlentheorie

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

Aufgabe 1: (*5 Punkte*)

Die *Paarquersumme* einer natürlichen Zahl n wird berechnet, indem man die Zahl von rechts her in Gruppen aus zwei Ziffern aufteilt und die entstehenden zweistelligen Zahlen addiert; die Paarquersumme von 12345 ist also $45 + 23 + 1 = 68$.

a) Zeigen Sie, daß n genau dann durch elf teilbar ist, wenn seine Paarquersumme durch elf teilbar ist.

b) Ist jede natürliche Zahl n modulo elf kongruent zu ihrer Paarquersumme?

c) Welchen Rest hat die Zahl 2718281828459045 bei der Division durch elf?

Aufgabe 2: (*6 Punkte*)

Für ein *public viewing* zur Fußballweltmeisterschaft möchte ein Choreograph zum Auftakt Statisten in Fußballtrikots in die Arena einmarschieren lassen. Wenn er sie in Elferreihen marschieren läßt, bleiben in der letzten Reihe acht übrig, allerdings ist der Zug dann zu lang. Deshalb ordnet er sie in Fünfundzwanzigerreihen an; jetzt bleiben in der letzten Reihe sieben übrig.

a) Finden Sie eine untere Schranke für die Anzahl der Statisten!

b) Welche anderen Anzahlen wären auch noch möglich?

Aufgabe 3: (*8 Punkte*)

a) Berechnen Sie im Körper $\mathbb{F}_{29}$ die Elemente

$$x_1 = 2 - 5^2, \qquad x_2 = 26 \cdot 27, \qquad x_3 = \frac{5}{27} \quad \text{und} \quad x_4 = 28! = \prod_{i=1}^{28} i$$

b) Zeigen Sie, daß die Zwei und die Drei primitive Wurzeln modulo 29 sind, nicht aber die Sechs.

c) Geben Sie zu jeder möglichen Ordnung eines Elements von $\mathbb{F}_{29}^{\times}$ ein Element an, das exakt diese Ordnung hat!

• • • **Bitte wenden!** • • •

Aufgabe 4: (*8 Punkte*)

J sei eine Jahreszahl und $1900 < J < 2072$.

a) Zeigen Sie: Im Jahr $J+4$ hat sich der Wochentag, auf den der 1. Januar fällt, gegenüber dem Jahr J um fünf verschoben.

b) J' sei das erste Jahr nach J, in dem jedes Datum auf den gleichen Wochentag fällt wie im Jahr J. Zeigen Sie;

$$J' = \begin{cases} J+28 & \text{falls } J \equiv 0 \bmod 4 \\ J+6 & \text{falls } J \equiv 1 \bmod 4 \\ J+11 & \text{sonst} \end{cases}$$

c) Warum sind diese Formeln falsch für $J = 1900$ und $J = 2072$?

Aufgabe 5: (*6 Punkte*)

a) Wie läßt sich bei RSA mit öffentlichem Exponenten $e = 5$ und Modul $N = pq$ ein privater Exponent d ohne EUKLIDischen Algorithmus aus e und einem gemeinsamen Vielfachen m von $p-1$ und $q-1$ berechnen?

b) Finden Sie für das RSA-System mit $p = 409$, $q = 523$ und $e = 5$ einen möglichst kleinen privaten Exponenten d !

c) Warum ist es hier nicht möglich, den öffentlichen Exponenten $e = 3$ zu nehmen?

Aufgabe 6: (*10 Punkte*)

a) Bestimmen Sie die Kettenbruchentwicklung von $\sqrt{10}$!

b) Finden Sie einen Näherungsbruch für $\sqrt{10}$ mit möglichst kleinem Nenner, der sich höchstens um 10^{-3} von $\sqrt{10}$ unterscheidet!

c) Finden Sie eine ganzzahlige Lösung der Gleichung $x^2 - 10y^2 = 1$!

d) Konstruieren Sie aus der Lösung von *c)* ein Element der Norm eins aus $\mathbb{Q}[\sqrt{10}]$!

e) Konstruieren Sie über das Quadrat dieses Elements eine weitere Lösung der Gleichung $x^2 - 10y^2 = 1$!

Aufgabe 7: (*8 Punkte*)

a) Bestimmen Sie im Ring $\mathbb{Z} \oplus \mathbb{Z}i$ der GAUSSschen Zahlen die Primzerlegung der Zahl $15i$!

b) Finden Sie alle ganzzahligen Lösungen der Gleichung $x^2 + y^2 = 15$!

c) Berechnen Sie in $\mathbb{Z} \oplus \mathbb{Z}i$ den ggT von $1+5i$ und $2+8i$!

d) Zeigen Sie: $\text{ggT}(a+ib, a-ib) = \text{ggT}(a,b)$ für alle $a+ib \in \mathbb{Z} \oplus \mathbb{Z}i$

Aufgabe 8: (*8 Punkte*)

Welche der folgenden Kongruenzen sind lösbar:

a) $x^2 \equiv 4 \bmod 12345$

b) $x^2 \equiv 5 \bmod 23$

c) $x^2 \equiv 5 \bmod 21$

d) Finden Sie die kleinste ungerade Primzahl p, für die die Kongruenz $x^2 \equiv p \bmod 127$ lösbar ist! (127 ist prim.)

Abgabe bis zum Freitag, dem 13. Juni 2014, um 13^{00} Uhr

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