Wolfgang K. Seiler
Tel. 2515

A5, C201

31. August 2018

Modulklausur Zahlentheorie

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

Aufgabe 1: (*5 Punkte*)

a) a und b seien beliebige ganze Zahlen. Zeigen Sie, daß $10a + b$ genau dann durch sieben teilbar ist, wenn $a - 2b$ durch sieben teilbar ist.

b) Gilt auch allgemeiner, daß $10a + b \equiv a - 2b \bmod 7$ für alle $a, b \in \mathbb{Z}$?

c) Wenden Sie *a)* mehrfach an um ohne Divisionen zu entscheiden, ob 12345 durch sieben teilbar ist!

Aufgabe 2: (*7 Punkte*)

a) Im August 2345 werden an der Rhineckar School of Commerce die Klausuren für den Studiengang Wirtschaftsmathematik geschrieben. Alle Studenten des dritten Studienjahrs sind pflichtangemeldet für die Klausuren Wirtschaftsalgebra, Wirtschaftsgeometrie und Wirtschaftszahlentheorie. Im Hörsaal werden die Studenten jeweils in der Reihenfolge ihres Eintreffens auf die zur Verfügung stehenden Plätze verteilt, so daß alle Reihen außer der letzten voll besetzt sind. In der letzten Reihe sitzt bei jeder Klausur genau ein Student.

Wirtschaftsalgebra wird in einem Hörsaal geschrieben, in dem unter Klausurbedingungen sieben Studenten in eine Reihe passen; elf Studenten sind nicht erschienen.

Wirtschaftsgeometrie wird in einem Hörsaal geschrieben, in dem neun Studenten in eine Reihe passen; zehn Studenten sind nicht erschienen.

Im Hörsaal für die Wirtschaftszahlentheorie passen nur fünf Studenten in eine Reihe; hier sind neun Studenten nicht erschienen.

Insgesamt sind 444 Studenten im Studiengang Wirtschaftsmathematik eingeschrieben, von denen natürlich weniger als die Hälfte im dritten Studienjahr sind. Wie viele Studenten sind im dritten Studienjahr?

b) Die Klausur in Wirtschaftszahlentheorie wird am letzten Freitag im August geschrieben. Welches Datum ist das?

Aufgabe 3: (*6 Punkte*)

Bestimmen Sie alle ganzzahligen Lösungen des linearen Gleichungssystems

$$x + 2y + 3z = 101 \quad \text{und} \quad 2x - 7y + 8z = 102\,!$$

b) Bestimmen Sie alle Lösungen mit $x, y, z \in \mathbb{N}$!

• • • **Bitte wenden!** • • •

Aufgabe 4: (*8 Punkte*)

a) Berechnen Sie im Körper $\mathbb{F}_{97}$ die Elemente

$$x_1 = 10^2 + 11^2 + 12^2, \qquad x_2 = 31 \cdot 32 \quad \text{und} \quad x_3 = \frac{20}{33}$$

b) Im Körper $\mathbb{F}_{103}$ hat die Zwei die Ordnung 51. (Das müssen Sie nicht beweisen.) Zeigen Sie: Wenn es ein Element $x \in \mathbb{F}_{103}$ gibt mit $x^2 = 2$, so ist entweder x oder $-x$ eine primitive Wurzel.

c) Geben Sie eine Formel an, mit der man ein x mit $x^2 = 2$ in $\mathbb{F}_{103}$ bestimmen kann – sofern ein solches x existiert.

d) Nun sei p eine beliebige Primzahl. Bestimmen Sie in Abhängigkeit von p die drei Elemente

$$S = \sum_{x \in \mathbb{F}_p} x, \qquad P_1 = \prod_{x \in \mathbb{F}_p} x \quad \text{und} \quad P_2 = \prod_{x \in \mathbb{F}_p^\times} x\,!$$

Aufgabe 5: (*11 Punkte*)

a) Zerlegen Sie die Zahl $N = 37!$ in ihre Primfaktoren!

b) Zeigen Sie: Ist $N + i$ eine Primzahl, so muß $\mathrm{ggT}(i, N) = 1$ sein.

c) Man kann zeigen, daß $P = N + 1$ prim ist. Q sei die nächstgrößere Primzahl. Geben Sie eine möglichst gute untere Schranke für $Q - P$ an!

d) Entscheiden Sie für jede der drei Zahlen $r = 31, 41, 64$, ob es in $(\mathbb{Z}/P)^\times$ Elemente der Ordnung r gibt, und bestimmen Sie gegebenenfalls deren Anzahl!

e) Hat die Kongruenz $x^2 \equiv 3 \bmod 37$ ganzzahlige Lösungen?

f) Hat die Kongruenz $x^2 \equiv 3 \bmod 185$ ganzzahlige Lösungen? ($185 = 5 \cdot 37$.)

Aufgabe 6: (*7 Punkte*)

a) Die Zahl $N = 17\,690\,411$ 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 7: (*6 Punkte*)

a) Bestimmen Sie die Kettenbruchentwicklung von $\sqrt{26}$!

b) Finden Sie eine ganzzahlige Lösung der Gleichung $x^2 - 26y^2 = 1$ sowie eine der Gleichung $x^2 - 26y^2 = -1$!

c) Finden Sie einen Näherungsbruch mit möglichst kleinem Nenner, der sich höchstens um 10^{-4} von $\sqrt{26}$ unterscheidet! Beweisen Sie diese Schranke, ohne die Dezimaldarstellung von $\sqrt{26}$ zu verwenden!

Aufgabe 8: (*10 Punkte*)

a) Zeigen Sie: Jedes Element $x \in \mathbb{Z} \oplus \mathbb{Z}i$, dem Ring der GAUSSschen Zahlen, mit primer Norm ist irreduzibel.

b) Zerlegen Sie $85i$ im Ring $\mathbb{Z} \oplus \mathbb{Z}i$ in ein Produkt irreduzibler Element!

c) Finden Sie, ausgehend von *b)*, alle Darstellungen von 85 als Summe zweier Quadrate!

d) Bestimmen Sie alle Elemente der Norm 85 in $\mathbb{Z} \oplus \mathbb{Z}i$!

e) Leiten Sie aus dem Ergebnis von *d)* eine Darstellung von π als Linearkombination geeigneter Arkustangenswerte ab!

Abgabe bis zum Freitag, dem 31. August 2018, um 9^{00} Uhr

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