Wolfgang K. Seiler
Tel. 2515

A5, C201

6. Juni 2011

13. Übungsblatt Zahlentheorie

Aufgabe 1:

a) Erklären Sie, warum der Euklidische Algorithmus den größten gemeinsamen Teiler zweier ganzer Zahlen berechnet!

b) Welche Rolle spielt er beim Beweis der eindeutigen Primzerlegung für natürliche Zahlen?

c) In welchen anderen Ringen gibt es ebenfalls einen erweiterten Euklidischen Algorithmus?

d) Was können Sie daraus für diese Ringe folgern?

Aufgabe 2:

a) Für welche $n \in \mathbb{N}$ bilden die Restklassen modulo n einen Körper?

b) Was ist $4/3$ im Körper $\mathbb{F}_{17}$?

c) Für ein vom Nullelement verschiedenes Element a aus diesem Körper und zwei natürliche Zahlen n, m sei $a^n = a^m$. Was können Sie daraus für n und m folgern?

d) Wie ist die Ordnung eines Element von $(\mathbb{Z}/n)^\times$ definiert, und welche Werte kann sie im Fall $n = 23$ annehmen?

e) Wie viele Elemente hat die prime Restklassengruppe modulo 35?

Aufgabe 3:

a) Wie und warum funktionieren elektronische Unterschriften nach RSA?

b) Der private Exponent d der RSA-Bank hat 700 Dezimalstellen. Von den sechs Direktoren kennt jeder nur die Restklasse von d modulo einer jeweils anderen 250-stelligen Primzahl p. Wie viele Direktoren müssen ihre Restklasse eingeben, damit der Computer (der nur die Primzahlen der Direktoren kennt) eine Unterschrift berechnen kann?

c) Welcher Satz wird dabei verwendet?

d) Erklären Sie in groben Zügen den Algorithmus, nach dem der Computer hier vorgeht!

Aufgabe 4:

a) Nennen Sie einige Anwendungen von Kettenbrüchen!

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

c) Welche reelle Zahlen lassen sich durch einen endlichen Kettenbruch darstellen?

Aufgabe 5:

a) Wie ist die Norm eines Elements eines quadratischen Zahlkörpers definiert?

b) Welche Norm hat das Element $2 + \sqrt{2} \in \mathbb{Q}[\sqrt{-2}]$?

c) Welche Norm hat das Element $\frac{1}{11} + \frac{9}{11}\sqrt{3} \in \mathbb{Q}[\sqrt{3}]$?

d) Das Element $x \in \mathbb{Q}[\sqrt{d}]$ habe ganzzahlige Norm. Welche Eigenschaft muß es noch haben um in der Hauptordnung zu liegen?

e) Zeigen Sie: Ein Element eines imaginärquadratischen Zahlkörpers ist genau dann eine Einheit, wenn es Norm eins hat.

f) Gilt dies auch für reellquadratische Zahlkörper?

g) Was ist die Hauptordnung eines quadratischen Zahlkörpers?

Aufgabe 6:

a) Eine natürliche Zahl soll als Summe von Quadraten ganzer Zahlen dargestellt werden. Wie viele Summanden braucht man mindestens, damit dies immer funktioniert?

b) Für welche natürlichen Zahlen reichen bereits zwei Summanden?

c) Warum kann man sich beim Beweis der entsprechenden Aussagen (im wesentlichen) auf Primzahlen beschränken?

Aufgabe 7:

a) Zeigen Sie: Die Kongruenz $x^2 \equiv a \bmod 103$ ist genau dann lösbar (in $\mathbb{Z}$), wenn a^{26} eine Lösung ist!

b) Ist die Kongruenz $x^2 \equiv 5 \bmod 257$ lösbar?

c) Zeigen Sie: Ist p eine Primzahl und sind $a, b \in \mathbb{Z}$ keine Vielfachen von p, so gilt für das LEGENDRE-Symbol die Gleichung $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$!

d) Wie ist das JACOBI-Symbol $\left(\frac{n}{m}\right)$ definiert?

e) Folgt aus $\left(\frac{n}{m}\right) = -1$, daß die Kongruenz $x^2 \equiv n \bmod m$ unlösbar ist?

Keine Abgabe — Frohe Ferien!