Wolfgang K. Seiler
*Tel.* 2515

A5, C201

*26. März 2009*

# 6. Übungsblatt Zahlentheorie

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

*a)* Für welche Zahlen $a$ mit $2 \leq a \leq 14$ zeigt der gewöhnliche Primzahltest nach Fermat, daß 15 keine Primzahl ist?

*b)* Für welche Zahlen $a$ mit $2 \leq a \leq 14$ zeigt der Primzahltest nach Miller und Rabin, daß 15 keine Primzahl ist?
*Hinweis:* Mit dem chinesischen Restesatz können Sie hier viel Rechenzeit sparen!

**Aufgabe 2:** (*3 Punkte*)

Die Zahl $p = (6t+1)(12t+1)(18t+1)$ sei eine Carmichael-Zahl.

*a)* Zeigen Sie: Es gibt $1296t^3$ Zahlen $a$ zwischen 1 und $p-1$, für die $p$ den Fermat-Test besteht.

*b)* Wie verhält sich die Wahrscheinlichkeit dafür, daß $p$ für eine zufällige Basis $a$ den Fermat-Test besteht, wenn $t$ gegen unendlich geht?

**Aufgabe 3:** (*5 Punkte*)

Faktorisieren Sie $N = 72263$ nach Pollards $(p-1)$-Methode mit Suchgrenze $B = 10$ !

**Aufgabe 4:** (*3 Punkte*)

Zerlegen Sie die Zahl 1 545 013 mit dem Fermatschen Verfahren in ein Produkt zweier Faktoren!

**Aufgabe 5:** (*4 Punkte*)

Die fünfte Fermat-Zahl $F_5 = 2^{32} + 1$ soll nach dem quadratischen Sieb mit Hilfe des Polynoms

$$f(x) = (x + 2^{16})^2 - F_5$$

faktorisiert werden, allerdings nicht von Ihnen.

*a)* Geben Sie das Polynom $f(x)$ in ausmultiplizierter Form explizit an!

*b)* Finden Sie alle $x \in \mathbb{Z}$, für die $f(x)$ durch 127 teilbar ist!

*c)* Zeigen Sie, daß $f(x)$ nie durch sieben teilbar ist!
*Hinweis:* Sie können das Ergebnis von Aufgabe 3 des dritten Übungsblatts verwenden.

**Abgabe** bis zum Donnerstag, dem 2. April 2009, um 15.30 Uhr