Wolfgang K. Seiler
Tel. 2515

A5, C201

31. März 2011

7. Übungsblatt Zahlentheorie

Aufgabe 1: *(6 Punkte)*
Faktorisieren Sie $N = 72263$ nach Pollards $(p-1)$-Methode mit Suchgrenze $B = 10$!

Aufgabe 2: *(5 Punkte)*
Zerlegen Sie die Zahl 1 545 013 mit dem Fermatschen Verfahren in ein Produkt zweier Faktoren!

Aufgabe 3: *(6 Punkte)*
Die fünfte Fermat-Zahl $F_5 = 2^{32} + 1$ soll nach dem quadratischen Sieb mit Hilfe des Polynoms

$$f(x) = \left(x - \left[\sqrt{F_5}\right]\right)^2 - F_5$$

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 4 des dritten Übungsblatts verwenden.

Aufgabe 4: *(3 Punkte)*

a) Bis vor knapp zehn Jahren wurde für die Wahl von RSA-Moduln $N = pq$ geraten, für p und q Primzahlen der Form $p = 2p' + 1$ und $q = 2q' + 1$ zu wählen mit Primzahlen p', q'. Welchen Grund hatte diese Empfehlung?

b) Warum findet man sie heute nicht mehr in den Richtlinien von Regulierungsbehörden und Sicherheitsberatern?

Bitte beachten Sie:

Ab April ist die Vorlesung montags und donnerstags!

Abgabe bis zum Donnerstag, dem 7. April 2011, um 17.15 Uhr