Wolfgang K. Seiler
Tel. 2515

A5, C201

12. April 2013

7. Übungsblatt Kryptologie

Aufgabe 1: *(3 Punkte)*
Faktorisieren Sie die Zahl 990 675 589 nach der Methode von Fermat!

Aufgabe 2: *(7 Punkte)*
Bereits 1931 entwickelten D.H. Lehmer und R.E. Powers folgende Methode zur Faktorisierung ganzer Zahlen: Ist a/b eine Konvergente der Kettenbruchentwicklung von $\sqrt{N}$; so ist $q = a^2 - Nb^2$ eine relativ kleine Zahl; falls $q = x^2$ eine Quadratzahl sein sollte, haben wir eine Relation der Form $a^2 \equiv x^2 \bmod N$, die uns vielleicht zu einer Faktorisierung von N führt.

a) Warum verwenden D.H. Lehmer und R.E. Powers Kettenbrüche und nicht irgendwelche rationalen Approximationen von $\sqrt{N}$?

b) Berechnen Sie die ersten fünf Konvergenten a_i/b_i der Kettenbruchentwicklung von $\sqrt{15}$!

c) Welche davon liefern direkt eine Relation der Form $a_i^2 \equiv x_i^2 \bmod 15$, und wann führt diese Relation zu einer Faktorisierung?

d) Was ändert sich, wenn Sie anstelle der Relation $a_i^2 - 15b_i^2 = q_i$ die Relation

$$a_i^2 \equiv (q_i \bmod 15) \bmod 15$$

verwenden?

e) Faktorisieren Sie die Zahl $N = 56\,723$ nach der Kettenbruchmethode!

Aufgabe 3: *(3 Punkte)*
Bezeichnet $L_{\alpha,c}(x)$ für $\alpha \in [0, 1]$ und $c > 0$ die Funktion $e^{c(\log x)^{\alpha}(\log\log x)^{1-\alpha}}$, so ist der Aufwand des quadratischen Siebs zur Faktorisierung von N ungefähr proportional zu $L_{1/2,1}(N)$, der des Zahlkörpersiebs zu $L_{1/3,\sqrt[3]{64/9}}(N)$.

a) Zeigen Sie: Ist $\alpha < \beta$, so ist $\lim\limits_{N\to\infty} \frac{L_{\alpha,c}(N)}{L_{\beta,d}(N)} = 0$.

b) Drücken Sie $L_{0,c}(x)$ und $L_{1,c}(x)$ einfacher aus!

c) Ab welcher Stellenzahl von $N \in \mathbb{N}$ ist $L_{1/3,\sqrt[3]{64/9}}(N) < L_{1/2,1}(N)$?

Aufgabe 4: *(7 Punkte)*
Faktorisieren Sie die Zahl $N = 851$ mit dem quadratischen Sieb mit Hilfe der Faktorbasis $\mathcal{B} = \{2, 5, 11, 17, 23\}$ und dem Siebintervall $[1, 40]$!

Abgabe bis zum Freitag, dem 19. April 2013, um 11.55 Uhr