

25. Oktober 2016

## 7. Übungsblatt Kryptologie

### Aufgabe 1: (4 Punkte)

Faktorisieren Sie die Zahl 990 675 589 nach der Methode von FERMAT!

### Aufgabe 2: (8 Punkte)

Bereits 1931 entwickelten D.H. LEHMÉR 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  $a^2 \equiv x^2 \pmod{N}$ , die uns vielleicht zu einer Faktorisierung von  $N$  führt.

- Warum verwenden D.H. LEHMÉR und R.E. POWERS Kettenbrüche und nicht irgendwelche rationalen Approximationen von  $\sqrt{N}$ ?
- Berechnen Sie die ersten fünf Konvergenten  $a_i/b_i$  der Kettenbruchentwicklung von  $\sqrt{15}$ !
- Welche davon liefern direkt eine Relation der Form  $a_i^2 \equiv x_i^2 \pmod{15}$ , und wann führt diese Relation zu einer Faktorisierung?
- Was ändert sich, wenn Sie anstelle der Relation  $a_i^2 - 15b_i^2 = q_i$  die Relation

$$a_i^2 \equiv (q_i \pmod{15}) \pmod{15}$$

verwenden?

### Aufgabe 3: (5 Punkte)

Faktorisieren Sie die Zahl  $N = 56723$  nach der Kettenbruchmethode!

### Aufgabe 4: (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  $L_{1/3, \sqrt[3]{64/9}}(N)$ .

- Zeigen Sie: Ist  $\alpha < \beta$ , so ist  $\lim_{N \rightarrow \infty} \frac{L_{\alpha,c}(N)}{L_{\beta,d}(N)} = 0$ .
- Drücken Sie  $L_{0,c}(x)$  und  $L_{1,c}(x)$  einfacher aus!
- Ab welcher Stellenzahl von  $N \in \mathbb{N}$  ist  $L_{1/3, \sqrt[3]{64/9}}(N) < L_{1/2,1}(N)$ ?

Abgabe bis zum Dienstag, dem 8. November 2016, um 15.25 Uhr