Wolfgang K. Seiler
Tel. 2515

B6, B4.08

28. Oktober 2022

8. Übungsblatt Kryptologie

Aufgabe 1:

a) Zeigen Sie, daß das Polynom $f(x) = \left(x - [\sqrt{N}]\right)^2 - N$ die Diskriminante N hat!

b) Berechnen Sie dieses Polynom für $N = 31\,123\,153$ explizit!

c) Bestimmen Sie alle einstelligen Primzahlen p mit der Eigenschaft, daß es ganze Zahlen x gibt, für die $f(x)$ durch p teilbar ist, und geben Sie die Menge dieser Zahlen x jeweils an!

Aufgabe 2:

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

Aufgabe 3:

Der Rechenaufwand von Faktorisierungsalgorithmen sowie von Algorithmen zur Berechnung diskreter Logarithmen für eine Zahl n ist oft ungefähr von der Form

$$L_n(\alpha, c) = e^{c(\log n)^\alpha (\log\log n)^{1-\alpha}}$$

mit $\alpha \in [0,\ 1]$ und $c > 0$.

a) Wie sieht diese Funktion in den Grenzfällen $\alpha = 0$ und $\alpha = 1$ aus?

b) Zeigen Sie: Für $\alpha < \beta$ ist $L_n(\alpha, c) < L_n(\beta, c)$!

c) Der Aufwand für das Zahlkörpersieb ist ungefähr $L_n(\frac{1}{3}, c)$ mit $c = \sqrt[3]{\frac{64}{9}}$, der für eine gute Implementierung des quadratischen Siebs liegt bei $L_n(\frac{1}{2}, 1)$. Ab welcher Größe von n ist das Zahlkörpersieb schneller?

Aufgabe 4:

a) Bestimmen Sie für $g = 2, 3$ und 5 die Menge aller $x \in \mathbb{Z}/23$, die einen diskreten Logarithmus zur Basis g modulo 23 haben!

b) Berechnen Sie jeweils eine Tabelle dieser Logarithmen!

Besprechung am Mittwoch, dem 2. November 2022, um 15.30 Uhr