Kryptologie

Übung, LVA 405.321
C. Fuchs

14. Übungsblatt, SS 2022

22.06.2022

1. Faktorisiere 18349 mit Hilfe des Quadratischen Siebes (wähle $F(B) = \{-1, 2, 3, 5, 7, 11\}$ und ein geeignetes Siebintervall der Länge 31).

2. Faktorisiere mit dem Quadratischen Sieb die Zahl $N = 11111111111111111$ (das sind 17 Einser). Das muss kein lauffähiges Programm sein, wichtig ist, dass jeder Schritt des Quadratischen Siebes klar hervorgeht.

3. Löse die Gleichung $X^k = X + 1$ im endlichen Körper $\mathbb{Z}_5[X]/(X^2 + 3X + 3)$ mit Hilfe des Babystep-Giantstep Algorithmus.

4. Finde das kleinste $x \geq 0$ mit a) $5^x = 98787 \pmod{224737}$ und b) $3^x \equiv 4 \pmod{722912266876050904361}$. Verwende Babystep-Giantstep.