Kryptographie **Blatt 3A**

hhu Düsseldorf
WiSe 2023/24

Abgabe: bis Montag 06.11.2023, vor der Vorlesung

Vorlesungswebseite: `http://reh.math.uni-duesseldorf.de/~khalupczok/krypto/`

Aufgabe 1: Ordnung von Potenzen in einer zyklischen Gruppe

Sei G eine endliche zyklische Gruppe mit Erzeuger $a \in G$.

Zeigen Sie, dass $\operatorname{ord}(a^j) = \dfrac{\operatorname{ord}(a)}{(j, \operatorname{ord}(a))}$ für alle $j \in \mathbb{Z}$ gilt.

Berechnen Sie damit in der Untergruppe $H = \langle \underline{5} \rangle$ der Gruppe $G = \mathbb{Z}_{5963}^{\times}$ die Ordnung von $\underline{5}^{11}$.

Aufgabe 2: Berechnung von $\varphi(N)$ und Faktorisierung von N

Seien $p \neq q$ Primzahlen und $N = pq$. Zeigen Sie:
Die Primzahlen p und q sind genau die Nullstellen des quadratischen Polynoms

$$T^2 - (N + 1 - \varphi(N))T + N.$$

Wer $\varphi(N)$ kennt, kann also N faktorisieren. (Mit anderen Worten: $\varphi(N)$ zu berechnen ist ebenso schwierig, wie N zu faktorisieren.)
Berechnen Sie damit die Primfaktoren von $N = 542029$ mit

$$\varphi(N) = 540540.$$

$*$ Kennen Sie einen schriftlichen Algorithmus zum Quadratwurzelziehen in $\mathbb{N}$? Hat dieser i. a. eine kurze Laufzeit?