Übungsblatt 12

Aufgabe 75 ***mündlich***

Sei p eine ungerade Primzahl.

(a) Zeigen Sie, dass α oder $\alpha + p$ ein Erzeuger von $\mathbb{Z}_{p^2}^*$ ist, falls α ein Erzeuger von $\mathbb{Z}_p^*$ ist.

(b) Überlegen Sie, wie sich effizient verifizieren lässt, dass 3 sowohl ein Erzeuger von $\mathbb{Z}_{29}^*$ als auch von $\mathbb{Z}_{29^2}^*$ ist.

(c) Bestimmen Sie die Ordnung von 3 in $\mathbb{Z}_m^*$ mit $m = 29^3$.

Hinweis: Es ist bekannt, dass α für alle $k \geq 1$ ein Erzeuger von $\mathbb{Z}_{p^k}^*$ ist, falls α ein Erzeuger von $\mathbb{Z}_p^*$ und von $\mathbb{Z}_{p^2}^*$ ist.

(d) Bestimmen Sie einen Erzeuger von $\mathbb{Z}_{29}^*$, der nicht gleichzeitig Erzeuger von $\mathbb{Z}_{29^2}^*$ ist.

(e) Berechnen Sie mit dem Algorithmus von Pohlig und Hellman den diskreten Logarithmus von $\beta = 3344$ zur Basis $\alpha = 3$ in der Gruppe $\mathbb{Z}_m^*$ mit $m = 29^3$.

Aufgabe 76 ***mündlich***

Seien die Primzahl $p = 227$ und der Erzeuger $\alpha = 2$ von $\mathbb{Z}_p^*$ gegeben.

(a) Berechnen Sie die Potenzen α^{32}, α^{40}, α^{59} und α^{156} in $\mathbb{Z}_p^*$ und faktorisieren Sie diese über der Faktorbasis $B = \{2, 3, 5, 7, 11\}$.

(b) Bestimmen Sie die diskreten Logarithmen $\log_\alpha p$ der Basisprimzahlen $q \in B$.

(c) Berechnen Sie $\log_\alpha \beta$ für $\beta = 173$ mit der Index-Calculus Methode.

Hinweis: Benutzen Sie die Faktorbasis B und die Zufallszahl 177.

Aufgabe 77 ***mündlich***

Faktorisieren Sie $n = 256961$ mit der Methode der zufälligen Quadrate. Verwenden Sie die Faktor-Basis

$$\{-1, 2, 3, 5, 7, 11, 13, 17, 19, 29, 31\}$$

und testen Sie die Zahlen $z^2 \bmod n$ mit $z = 500, 501, \ldots,$ bis Sie eine Kongruenz der Form $x^2 \equiv_n y^2$ erhalten und die Faktorisierung von n finden.

Aufgabe 78 ***mündlich***

Mit welcher Wahrscheinlichkeit kann eine Zahl n mit der Methode der zufälligen Quadrate erfolgreich faktorisiert werden, wenn als Basis $\mathcal{B} = \{2, 3, 5, \ldots, p_b\}$ verwendet wird und $c > b+1$ Quadratzahlen $z_i = x_i^2$ über $\mathcal{B}$ faktorisiert werden konnten?