Humboldt-Universität zu Berlin
Prof. Dr. Johannes Köbler

Übungsblatt 9

Aufgabe 63 ***mündlich***

Wir betrachten den Linear-Kongruenz-Generator $\texttt{LinGen}_{n,l,a,b}$. Zeigen Sie, dass $N(z_1 \cdots z_{i-1}, 1^l) = 1 - z_{i-1}$ im Fall $n = qa + 1$, $b = 1$ und $a \equiv_2 1 \not\equiv_2 q$ ein ε-NBP für $\texttt{LinGen}_{n,l,a,b}$ mit $1/2 + \varepsilon = q(a+1)/2n$ ist.

Aufgabe 64 ***mündlich***

Betrachten Sie den BBS-Generator $\texttt{BBS}_{n,l}(x_0)$.

(a) Überlegen Sie, wie sich aus dem Keim x_0 jedes x_i möglichst effizient berechnen lässt, falls die Primfaktorzerlegung von n bekannt ist.

(b) Lässt sich x_i mit vergleichbarem Aufwand auch aus jedem beliebigem x_j bestimmen? Betrachten Sie insbesondere den Fall $j > i$.

(c) Zeigen Sie, dass die Periode des BBS-Generators höchstens $t = \text{kgV}(u_1, v_1)$ ist, wobei u_1 die Ordnung von 2 in $\mathbb{Z}^*_{(p-1)/2}$ und v_1 die Ordnung von 2 in $\mathbb{Z}^*_{(q-1)/2}$ ist.

(d) Zeigen Sie, dass diese Schranke im Fall $p = 103$, $q = 127$ scharf ist.

Hinweis: Benutzen Sie den Keim 49.

Aufgabe 65 ***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 66 ***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 67 ***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 68 ***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?

Aufgabe 69 ***mündlich***

Faktorisieren Sie die Zahlen 262063, 9420457 und 181937053 mit dem ρ-Algorithmus von Pollard. Wieviele Iterationen werden hierzu jeweils bei Verwendung der Funktion $f(x) = x^2 + 1$ benötigt?

Aufgabe 70 ***mündlich***

Beschreiben Sie eine Modifikation des Algorithmus von Shanks, die den diskreten Logarithmus von β zur Basis α in Zeit $\mathcal{O}(\sqrt{r-l})$ berechnet, falls bereits bekannt ist, dass dieser im Teilintervall $[r, l]$ von $[0, \text{ord}(\alpha) - 1]$ liegt.

Aufgabe 71 ***mündlich***

Berechnen Sie in der Gruppe $\mathbb{Z}^*_p$ mit $p = 458009$ den diskreten Logarithmus von $\beta = 56851$ zur Basis $\alpha = 2$ mit der Ordnung $\text{ord}(\alpha) = 57251$.