KRY: Wahlfach Kryptologie

Serie 9: Quadratisches Sieb, modulare Wurzeln, diskrete Logarithmen

Aufgabe 1 (T)
Wir betrachten die zusammengesetzte Zahl $n = 91$. In dieser Aufgabe geht es darum, die Berechnungs-Schritte für das **Quadratische Sieb** durchzugehen.
Verwenden Sie folgende Werte:

- $m = \lfloor\sqrt{91}\rfloor = 9$
- $q(x) = (m + x)^2 - n$
- $F = \{-1, 2, 3, 5\} \quad (B = 5)$
- $S = \{-4, -3, -2, -1, 0, 1, 2, 3, 4\}$

(a) Bestimmen Sie mit Hilfe des Siebverfahrens diejenigen $q(x)$, die "B-glatt modulo n" sind[1].

(b) Notieren Sie das lineare Gleichungssystem (mod 2) zum Bestimmen eines geeigneten Produktes von B-glatten Quadraten.

(c) Bestimmen Sie durch Lösen des Gleichungssystems aus Aufgabe b) ein geeignetes Produkt von B-glatten Quadraten, und berechnen Sie damit einen Faktor von n.

Aufgabe 2 (T)

(a) Bestimmen Sie die quadratischen Reste modulo 11 mit Hilfe des Kriteriums von Euler.

(b) Suchen sie mit dem Kriterium von Euler einen quadratischen Nichtrest modulo 97.

Aufgabe 3 (T)
Bestimmen Sie mit Hilfe von Tonellis Algorithmus die Lösungen der untenstehenden Gleichungen.

(a) $x^2 = 11 \,(\text{mod } 43)$

(b) $x^2 = 6 \,(\text{mod } 97)$

[1] bedeutet: diejenigen $q(x)$, deren Faktoren alle in $\{-1, 2, 3, 5\}$ liegen

Aufgabe 4 (T)
Bestimmen Sie mit Hilfe des Baby Step – Giant Step Algorithmus in $\mathbb{Z}_{61}^*$ den diskreten Logarithmus $\log_{17}(42)$.

Aufgabe 5 (T)
Lösen Sie die Gleichung $78x = 246 \pmod{264}$.

Aufgabe 6 (T)
Bestimmen Sie mit Hilfe der Pollard ρ - Methode in $\mathbb{Z}_{23}^*$ den diskreten Logarithmus $\log_5(10)$.
Hinweis: Wählen Sie die folgende Zerlegung von $\mathbb{Z}_{23}^*$: $G_1 = \{1, 2, \ldots, 7\}$, $G_2 = \{8, 9, \ldots, 15\}$, $G_3 = \{16, 17, \ldots, 22\}$.