

## Übungsblatt 13

### Aufgabe 71

Seien  $p$  und  $q$  ungerade Primzahlen und  $n = pq$ .

(a) Zeigen Sie, dass  $\text{ord}_n(\alpha) = \text{kgV}(\text{ord}_p(\alpha), \text{ord}_q(\alpha))$  für alle  $\alpha \in \mathbb{Z}_n^*$ .

(b) Zeigen Sie, dass es ein  $\alpha \in \mathbb{Z}_n^*$  gibt mit  $\text{ord}_n(\alpha) = \frac{\varphi(n)}{\text{ggT}(p-1, q-1)}$ .

(c) Sei nun  $\text{ggT}(p-1, q-1) = 2$  und  $p, q > 3$ . Angenommen, wir haben ein Orakel, das für ein  $\alpha \in \mathbb{Z}_n^*$  mit  $\text{ord}_n(\alpha) = \varphi(n)/2$  den diskreten Logarithmus in der Untergruppe  $[\alpha]$  berechnet. Das Orakel berechnet also für beliebige  $\beta \in [\alpha]$  den diskreten Logarithmus  $a = \log_{n,\alpha} \beta$  mit  $0 \leq a \leq \varphi(n)/2 - 1$ . (Der Wert  $\varphi(n)/2$  bleibt dabei geheim.)

Zeigen Sie, dass für das vom Orakel bei Eingabe  $\beta = \alpha^n$  berechnete  $a$  gilt:  $n - a = \varphi(n)$ .

(d) Geben Sie einen effizienten Algorithmus an, der  $n$  unter Benutzung des Orakels aus (c) faktorisiert.

### Aufgabe 72

Betrachten Sie das Rabin-System mit dem Schlüssel  $p = 199$ ,  $q = 211$ ,  $n = pq$  und  $e = 1357$ .

(a) Berechnen Sie den Kryptotext  $y$  des Klartextes  $x = 32767$ .

(b) Bestimmen Sie die vier möglichen Entschlüsselungen von  $y$ .

### Aufgabe 73

Sei  $p$  prim mit  $p \equiv_8 5$ , und sei  $a$  ein quadratischer Rest modulo  $p$ . Weiterhin bezeichne  $L_i(\beta)$  für  $\beta \in \mathbb{Z}_p^*$  das Bit mit Wertigkeit  $2^i$  in der Binärdarstellung von  $\log_{n,\alpha} \beta$ , wobei  $\alpha$  ein Erzeuger von  $\mathbb{Z}_p^*$  ist. Zeigen Sie:

(a)  $a^{(p-1)/4} \equiv_p \pm 1$ .

(b) Wenn  $a^{(p-1)/4} \equiv_p 1$ , dann ist  $a^{(p+3)/8} \pmod p$  eine Quadratwurzel von  $a$  modulo  $p$ .

(c) Wenn  $a^{(p-1)/4} \equiv_p -1$ , dann ist  $2^{-1}(4a)^{(p+3)/8} \pmod p$  eine Quadratwurzel von  $a$  modulo  $p$ .

*Hinweis:* Verwenden Sie die Tatsache, dass im Fall  $p \equiv_8 5$   $\left(\frac{2}{p}\right) = -1$  ist.

(d) Bei Kenntnis von  $\alpha$  kann  $L_1(\beta)$  effizient berechnet werden.

*Hinweis:* Machen Sie davon Gebrauch, dass im Fall  $p \equiv_8 5$  Quadratwurzeln modulo  $p$  effizient berechnet werden können und für alle  $\beta \in \mathbb{Z}_p^*$  die Gleichheit  $L_0(\beta) = L_1(p - \beta)$  gilt.

### Aufgabe 74

Seien  $m_1, \dots, m_{n+1} \in \mathbb{N}$ . Sei  $g_i = \text{ggT}(m_i, m_{n+1})$ ,  $i = 1, \dots, n$ . Zeigen Sie

$$\text{kgV}(g_1, \dots, g_n) = \text{ggT}(\text{kgV}(m_1, \dots, m_n), m_{n+1}).$$

### Aufgabe 75

Betrachten Sie für  $a_1, \dots, a_n \in \mathbb{Z}$  und  $m_1, \dots, m_n \in \mathbb{N}$  folgendes System von linearen Kongruenzen:

$$x \equiv_{m_i} a_i, \quad i = 1, \dots, n \quad (*)$$

(a) Zeigen Sie, dass das Kongruenzgleichungssystem (\*) höchstens eine Lösung modulo  $\text{kgV}(m_1, \dots, m_n)$  hat.

(b) Zeigen Sie, dass das System (\*) genau dann lösbar ist, wenn für alle  $1 \leq i < j \leq n$  die Zahl  $\text{ggT}(m_i, m_j)$  ein Teiler von  $(a_i - a_j)$  ist.

*Hinweis:* Führen Sie einen Induktionsbeweis und verwenden Sie Aufgabe 74.

### Aufgabe 76

Wir betrachten das ElGamal-System über der Gruppe  $\mathbb{F}_{27}^*$ , wobei wir zur Konstruktion des Körpers  $\mathbb{F}_{27}$  das irreduzible Polynom  $m(x) = x^3 + 2x^2 + 1$  benutzen. Angenommen, wir wählen als Erzeuger das Element  $\alpha = x$  und als privaten Schlüssel  $a = 11$ . Wie lässt sich damit der Kryptotext

$$y = (K, H)(P, X)(N, K)(H, R)(T, F)(V, Y)(E, H)(F, A)(T, W)(J, D)(U, J)$$

entschlüsseln, wenn wir die 25 Zeichen  $A, \dots, Z$  der Reihe nach mit den Körperelementen  $1, 2, x, x + 1, x + 2, 2x, \dots, 2x^2 + 2x + 2$  kodieren?