



Lösungsblatt 7

Aufgabe 1 (Kleiner Satz von Fermat)

- (a) Abgeschlossenheit: Für $a, b \in \mathbb{Z}_m^*$ ist $(ab)^{-1} = b^{-1}a^{-1}$, also ist auch $ab \in \mathbb{Z}_m^*$.
Neutrales Element: $1 \in \mathbb{Z}_m^*$.
Inverse Elemente: Für jedes $a \in \mathbb{Z}_m^*$ existiert nach Definition a^{-1} und es ist $a^{-1} \in \mathbb{Z}_m^*$ wegen $(a^{-1})^{-1} = a$.
Die Assoziativität wird von der Multiplikation über den ganzen Zahlen vererbt.
- (b) Jedes $x \in \mathbb{Z}_{35}$ mit $\gcd(x, 35) = 1$ erzeugt \mathbb{Z}_{35} . Die einzigen nicht trivialen Untergruppen werden deshalb von der 5 und von der 7 erzeugt und haben die Ordnung 7 und 5.
- (c) Der kleine Satz von Fermat in additiven Gruppen G lautet $\forall x \in G : x \cdot |G| = e$, wobei e das neutrale Element von G ist. Bei uns ist also $8 \cdot 35 \equiv 0 \pmod{35}$. Damit ist das additive Inverse $8 \cdot 34 \equiv -8 \pmod{35}$.
- (d) Nicht modulo 35 invertierbar sind alle Zahlen aus \mathbb{Z}_{35} , die Vielfache von 5 oder 7 sind, d.h. die Menge $\{0, 5, 7, 10, 14, 15, 20, 21, 25, 28, 30\}$. Daraus folgt $|\mathbb{Z}_{35}^*| = 35 - 11 = 24 = \varphi(35)$.
- (e) Nach dem kleinen Satz von Fermat gilt: $1 \equiv 8^{24} \equiv 8 \cdot 8^{23} \pmod{35}$. Folglich ist $8^{23} \equiv 22 \pmod{35}$ das multiplikative Inverse von 8.

Aufgabe 2 (RSA)

- (a) Wir berechnen den Schlüsseltext $c = 15^{13} \equiv 257 \pmod{323}$.
- (b) Wir berechnen zunächst den privaten Schlüssel $d = e^{-1} \pmod{\varphi(n)}$: $13^{-1} \equiv 133 \pmod{288}$.
Damit können wir den Klartext berechnen: $m \equiv 66^{133} \equiv 308 \pmod{323}$.
- (c) Es gilt, daß $(\sqrt{n} - 1)^2 \geq \varphi(n)$. Da $299 \geq (\sqrt{323} - 1)^2$ ist, scheint Alices Schlüssel nicht korrekt zu sein.

Aufgabe 3 (Untergruppen zyklischer Gruppen)

- (a) Sei $G = \langle g \rangle$ und $U \subset G$ eine nicht triviale Untergruppe von G . Die Menge $\{m \in \mathbb{N} : e \neq a^m \in U\}$ hat ein kleinstes Element n . Es ist $\langle a^n \rangle \subset U$. Für jedes $x \in U$ existiert ein $k \in \mathbb{N}$ mit $x = a^k$. Division mit Rest liefert $k = qn + r$ für ein q und $0 \leq r < n$. Es folgt $a^r = a^{k-qn} = a^k \cdot (a^n)^{-q} \in U$. Da n minimal war, ist $r = 0$ und somit $x = a^k = (a^n)^q \in \langle a^n \rangle$.
- (b) Angenommen, es gäbe zwei Elemente h_1 und h_2 , die verschiedene Untergruppen von $G = \langle g \rangle$ der Ordnung a erzeugen. Es gibt $j_1, j_2 \in \mathbb{N}$, so daß $h_1 = g^{j_1}$ und $h_2 = g^{j_2}$. Weiterhin gilt $1 = h_i^a = g^{j_i a}$ für $i = 1, 2$. Demnach gibt es für $i = 1, 2$ ein $k_i \in \mathbb{N}$ mit $j_i a = k_i |G|$ (siehe z.B. Buch Satz 3.9.2). Weiterhin muß $\gcd(k_i, a) = 1$ sein für $i = 1, 2$, da sonst wegen $j_i a / \gcd(k_i, a) = k_i / \gcd(k_i, a) |G|$ die von h_i erzeugte Untergruppe eine Ordnung kleiner a hätte.
Wir setzen $k_3 = k_1^{-1} \pmod{a}$ und erhalten $h_2 = h_1^{k_2 k_3}$. Damit liegen h_1 und h_2 in der gleichen Untergruppe. Also gibt es nur eine Untergruppe der Ordnung a in G .

Aufgabe 4 (Untergruppen von Primzahlordnung)

Sei e_i das neutrale Element von G_i und g_i ein Generator der (eindeutigen, siehe Aufgabe 3) Untergruppe der Ordnung a von G_i für $i = 1, 2$. Alle Gruppen, die von den Elementen (g_1^j, g_2) , $j = 1, \dots, a - 1$ erzeugt werden, haben Ordnung a und sind verschieden. Auch die zwei Gruppen, die von (g_1, e_2) und (e_1, g_2) erzeugt werden, haben Ordnung a .

Um zu zeigen, daß das alle Untergruppen von $G_1 \times G_2$ der Ordnung a sind, beweisen wir, daß jedes

Element $(x_1, x_2) \in G_1 \times G_2$ der Ordnung a in einer der Untergruppen liegt.

Ist x_1 oder x_2 das neutrale Element, ist der Fall klar. Nehmen wir also an, daß $x_1 \neq e_1$ und $x_2 \neq e_2$ ist. Offensichtlich ist $x_1^a = e_1$ und $x_2^a = e_2$. Also liegt x_i in der Untergruppe der Ordnung a von G_i für $i = 1, 2$. Sei also $x_2 = g_2^k$, und $l = k^{-1} \pmod a$. Dann ist $(x_1, x_2) \in \langle (x_1^l, g_2) \rangle$, also in einer der oben genannten Untergruppen, denn x_1^l ist in der Untergruppe der Ordnung a von G_1 .

Also gibt es $a + 1$ Untergruppen der Ordnung a von $G_1 \times G_2$.

Aufgabe 5 (RSA)

Sei $\psi : \mathbb{Z}_{pq} \rightarrow \mathbb{Z}_p \times \mathbb{Z}_q$, $x \mapsto (x \pmod p, x \pmod q)$ für $p, q \in \mathbb{P}$. Wir zeigen, dass die Abbildung bijektiv ist.

Für die Injektivität nehmen wir an, daß $\psi(x) = (x_p, x_q) = (y_p, y_q) = \psi(y)$ ist für $x, y \in \mathbb{Z}_{pq}$. Da ψ linear ist, gilt: $\psi(x - y) = (0, 0)$, und damit $y = x + k_p p$ und $y = x + k_q q$ für ein $(k_p, k_q) \in \mathbb{Z}^2$. Folglich gilt $k_p p = k_q q$. Da p und q prim sind, gilt $p|k_q$ und $q|k_p$. Damit ist $x \equiv y \pmod n$. Also ist die Abbildung injektiv. Weiterhin gilt, daß $|\mathbb{Z}_{pq}| = |\mathbb{Z}_p \times \mathbb{Z}_q|$, also ist ψ wegen der Injektivität auch surjektiv und damit bijektiv.

Zum Lösen der Aufgabe müssen wir daher nur ein e finden mit $\psi(m) = \psi(m^e)$. Dies ist offensichtlich der Fall, wenn $e - 1$ ein Vielfaches der Gruppenordnung von \mathbb{Z}_p^* und \mathbb{Z}_q^* , also von $p - 1$ und $q - 1$, ist.

In unserem Fall stellen wir fest, dass für Charlies öffentlichen Schlüssel gilt: $e = 145 = 16 \cdot 9 + 1 = 18 \cdot 8 + 1$. Also ist Charlies Schlüssel unsicher.

Auf einem der nächsten Übungsblätter werden wir sehen, dass auch Bobs Schlüssel verdächtig ist, da $e - 1 = 54 = 27 \cdot 2$ viele Primfaktoren von $p - 1$ und $q - 1$ enthält.

Aufgabe 6 (φ -Funktion)

$\varphi(n)$ ist definiert als die Anzahl der Elemente der Menge $\mathcal{A} = \{a \mid 1 \leq a < n, \gcd(a, n) = 1\}$. Entsprechend ist $\varphi(2n)$ die Anzahl der Elemente von $\mathcal{B} = \{a \mid 1 \leq a < 2n, \gcd(a, 2n) = 1\}$. Wir bilden die Mengen \mathcal{A} und \mathcal{B} aufeinander ab mit der Abbildung

$$f : \mathcal{A} \longrightarrow \mathcal{B} : a \longmapsto \begin{cases} a & \text{falls } a \text{ ungerade,} \\ a + n & \text{sonst.} \end{cases}$$

Wir zeigen, daß f korrekt definiert (also $\text{Im}(f) \subset \mathcal{B}$) und bijektiv ist (wir geben die Umkehrabbildung an). Daraus folgt, daß beide Mengen gleich groß sind, also die gewünschte Behauptung.

Korrektheit: Für ungerade a ist $\gcd(a, n) = \gcd(a, 2n)$. Ist a gerade, so ist $a + n$ ungerade und wie eben gilt $\gcd(a + n, n) = \gcd(a + n, 2n)$. Außerdem ist offensichtlich $1 \leq f(a) < 2n$ für alle $a \in \mathcal{A}$.

Umkehrabbildung: Die inverse Abbildung von f ist

$$g : \mathcal{B} \longrightarrow \mathcal{A} : b \longmapsto \begin{cases} b & \text{wenn } b < n, \\ b - n & \text{sonst.} \end{cases}$$

Aus $\gcd(b, 2n) = 1$ folgt $\gcd(b, n) = \gcd(b - n, n) = 1$, also ist $\text{Im}(f) \subset \mathcal{A}$. Man sieht leicht, daß $g(f(a)) = a$ für alle $a \in \mathcal{A}$. Schließlich ist $f(g(b)) = b$ für alle $b \in \mathcal{B}$, da alle $b \in \mathcal{B}$ ungerade sind und alle $b - n$ gerade.