



Lösungsblatt 11

Aufgabe 1 (Elementordnungen)

- (a) Eine endlich erzeugte Gruppe hat genau dann eine Primitivwurzel, wenn sie zyklisch ist. (Definition in Übung 7, Aufg. 3.)
- (b) Wie wir in der 7. Übung Aufg. 3(b) gesehen haben, gibt es genau eine Untergruppe der Ordnung p und eine der Ordnung q , in der jeweils p bzw. q Elemente sind. Das Einselement ist natürlich in beiden genannten Untergruppen, daher gibt es $p + q - 1$ Elemente, die nicht volle Gruppenordnung haben, und somit $(p - 1)(q - 1)$ Primitivwurzeln. Die gesuchte Wahrscheinlichkeit ist daher

$$\frac{(p-1)(q-1)}{pq}.$$

Achtung! Die hier gewählten Bezeichnungen stimmen nicht mit den Bezeichnungen bei RSA überein. Es gibt nicht $\varphi(pq)$ Primitivwurzeln in \mathbb{Z}_{pq}^\times !

- (c) Wie wir gesehen haben, gibt es $\varphi(n)$ Elemente in \mathbb{Z}_n^\times . Sei nun g eine Primitivwurzel von (G, \circ) , dann sind auch alle g^i mit $i \in \mathbb{Z}_n^\times$ Primitivwurzeln. Die gesuchte Wahrscheinlichkeit ist daher

$$\frac{\varphi(n)}{n}.$$

Aufgabe 2 (Elementordnungen)

Es gilt: $(353 - 1) = (2^5 * 11)$, sowie

$$\begin{aligned} -1 &\equiv 2^{(2^2 \cdot 11)} \pmod{353} \\ -1 &\equiv 3^{(2^4 \cdot 11)} \pmod{353} \\ -1 &\equiv 5^{(2^4 \cdot 11)} \pmod{353}. \end{aligned}$$

Damit ergibt sich folgende Tabelle:

| x | $\text{ord}(x)$ | $ \langle x \rangle $ |
|----------|-----------------|-----------------------|
| 2 | $2^3 \cdot 11$ | $2^3 \cdot 11$ |
| 3 | $2^5 \cdot 11$ | $2^5 \cdot 11$ |
| 4 | $2^2 \cdot 11$ | $2^2 \cdot 11$ |
| 5 | $2^5 \cdot 11$ | $2^5 \cdot 11$ |
| 2^{11} | 2^3 | 2^3 |

Aufgabe 3 (Index Calculus)

- (a) Wir stellen zunächst das folgende Gleichungssystem auf, wobei x_i der diskrete Logarithmus von i zur Basis 5 ist:

$$\begin{aligned} 0 + 3x_3 + -14x_5 + x_7 &\equiv 0 \pmod{352} \\ 3x_2 + 0 + -19x_5 + x_7 &\equiv 0 \pmod{352} \\ 5x_2 + 2x_3 + -30x_5 + 0 &\equiv 0 \pmod{352} \end{aligned}$$

Dieses formen wir zu

$$\begin{aligned} -3x_2 + 3x_3 + 5x_5 + 0 &\equiv 0 \pmod{352} \\ 3x_2 + 0 + -19x_5 + x_7 &\equiv 0 \pmod{352} \\ 21x_2 + 0x_3 + -100x_5 + 0 &\equiv 0 \pmod{352} \end{aligned}$$

um. Wir erhalten somit: $5^{-12} \equiv 2 \pmod{353}$, $5^{221} \equiv 3 \pmod{353}$ und $5^{55} \equiv 7 \pmod{353}$.

- (b) Wir wählen zufällig die Exponenten $y_2 = 5$, $y_3 = 0$, $y_5 = 0$ und $y_7 = 3$ und stellen fest, daß $11 \cdot (2^{y_2} \cdot 3^{y_3} \cdot 5^{y_5} \cdot 7^{y_7}) \equiv (2 \cdot 5) \pmod{353}$. Damit erhalten wir den diskreten Logarithmus x von 11 zur Basis 5 als die Lösung der Gleichung:

$$x + 3 \cdot 55 + 5 \cdot (-12) \equiv (-12) + 1 \pmod{352}.$$

Damit ist $x = 236$.

Aufgabe 4 (Primzahlen)

- (a) Wenn n eine Primzahl wäre, so würde nach dem kleinen Satz von Fermat $x^{n-1} \equiv 1 \pmod{n}$ für alle $0 \neq x \in \mathbb{Z}_n$ gelten. Daher ist n in diesem Fall keine Primzahl.
- (b) Falls für alle $x \in \mathbb{Z}_n^\times$ gilt, daß $x^{n-1} \equiv 1 \pmod{n}$ ist n prim oder eine sogenannte Carmichael-Zahl. Wir erläutern dieses: Ist n nicht prim, so sei p eine Primzahl, die n teilt. Damit gilt für alle $x \in \mathbb{Z}_n^\times$: $x^{n-1} \equiv 1 \pmod{p}$, was nur sein kann, falls $p-1 | n-1$. Sei andererseits q eine Primzahl, so daß $q^2 | n$, dann würde gelten: $q | n$ und $q | \varphi(n) \Rightarrow q | (n-1)$. Dies ist ein Widerspruch. Tatsächlich sind alle Carmichael-Zahlen so charakterisiert (Siehe Buch "Einführung in die Kryptographie"). Ein Beispiel für eine Carmichael-Zahl ist $n = 561$.

Aufgabe 5 ((p-1)-Methode)

Wir wählen $B = 9$. Damit ergibt sich $k = 2^3 \cdot 3^2 \cdot 5 \cdot 7$. In der Tat gilt: $\gcd(3^k - 1, 69647) = 271 < 69647$. Wir haben offensichtlich Glück gehabt, denn erst mit einem Exponenten k , der ein Vielfaches von $2 \cdot 3^3 \cdot 5$, aber kein Vielfaches von 2^8 ist, hätten wir 69647 mit jeder Basis a , so daß $\gcd(a, 69647) = 1$ ist, faktorisieren können.