Kryptologie: Übungsblatt 5, Besprechung ab dem 28.5.2018, 10:15, H20

50.) Man bestimme das multiplikative Inverse von 27 in $\mathbb{Z}_{101}^*$.

51.) Für alle $a \in \mathbb{Z}_{14}^*$ bestimme man $\langle a \rangle$. Welche Mächtigkeiten haben diese Untergruppen? Gibt es ein erzeugendes Element (eine Primitivwurzel) von $\mathbb{Z}_{14}^*$?

52.) Berechne $27^{101} \bmod 101$.

53.) Finde die kleinste Sophie-Germain-Primzahl q größer als 100.
Sei $n = 2q + 1$. Welche Tests muss man nun durchführen, um zu testen, ob a eine Primitivwurzel modulo n ist?

54.) Welche der folgenden multiplikativen Gruppen sind zyklisch:

$$\mathbb{Z}_{18}^*,\ \mathbb{Z}_{30}^*,\ \mathbb{Z}_{27}^*,\ \mathbb{Z}_{125}^*,\ \mathbb{Z}_{101}^*,\ \mathbb{Z}_{64}^*$$

55.) U_1 ist eine echte Untergruppe von U_2 und U_2 ist eine echte Untergruppe der Gruppe G, also

$$U_1 \subset U_2 \subset G$$

Wie groß kann $|U_1|$ im Verhältnis zu $|G|$ höchstens sein?

56.) Man berechne (die Primfaktorisierung von) $\varphi(\, 2^5 \cdot 3^2 \cdot 5^4 \cdot 11^3 \cdot 17\,)$.

57.) Beim RSA-Verfahren setzt sich die Zahl $n = p \cdot q$ aus zwei verschiedenen Primzahlen p und q etwa der halben Bitlänge, im Vergleich zu n, zusammen. Ein wenig können (und sollen) die Anzahlen der Bits von p und q voneinander abweichen, aber auch nicht zu viel. Sagen wir, ein *zulässiges* RSA-System besteht aus drei Zahlen n, p, q wobei $n = p \cdot q$ und

$$\sqrt{n}/8 \leq p < q \leq 8\sqrt{n}$$

Einerseits sollte das Intervall $[\sqrt{n}/8,\ 8\sqrt{n}]$ groß genug sein, um genügend viele Primzahlen p, q in diesem Intervall (also geheime Schlüssel) zur Verfügung zu haben (was der Fall ist).
Aus Sicherheitsgründen sollte andererseits $\varphi(n)$ (im Vergleich zu n) nicht zu klein sein.
Zeigen Sie, dass für zulässige RSA-Systeme gilt:

$$\lim_{n \to \infty} \frac{\varphi(n)}{n} = 1$$

58.) Die Folge der Fibonacci-Zahlen ist wie folgt definiert:

$$f_1 = f_2 = 1,\ f_{n+2} = f_{n+1} + f_n$$

Dies sind die Zahlen

$$1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, 233, \ldots$$

Wenn man den Euklid-Algorithmus anwendet, um den ggT zweier aufeinander folgender Fibonacci-Zahlen zu berechen, etwa ggT$(233, 144)$ – Was fällt dabei auf?

59.) Welches sind die einfachsten Gruppen, mit den wenigsten Elementen? Gibt es eine Gruppe mit nur einem Element, nennen wir es e ? Gibt es eine Gruppe mit zwei Elementen, nennen wir sie e und a ? Man gebe die Tafeln für die Gruppenoperation $\circ$ an.

Welche der Strukturen $(\{0,1\}, \wedge)$, $(\{0,1\}, \vee)$, $(\{0,1\}, \oplus)$ $(\{0,1\}, \Leftrightarrow)$, stellt eine Gruppe dar?

60.) Finde Zahlen $x, y \in \mathbb{Z}$, so dass $ggT(123, 57) = 123 \cdot x + 57 \cdot y$.