TU Ilmenau
Institut für Mathematik, Diskrete Mathematik
Prof. Michael Stiebitz/Dr. Axel Wolf

Sommersemester 2019

Übungsaufgaben Kryptographie, Serie 3

Aufgabe 1

Es seien $m, n, x, k \in \mathbb{Z}$. Beweisen Sie folgende Aussagen:

(a) $\text{ggT}(m, n) = \text{ggT}(n, m) = \text{ggT}(|m|, |n|)$

(b) $\text{ggT}(n, n) = \text{ggT}(n, 0) = |n|$

(c) $\text{ggT}(n, m) = \text{ggT}(n + mx, m)$

(d) $\text{ggT}(n, m) = \text{ggT}(n \text{ Mod } m, m)$ mit $m \geq 1$

(e) $\text{ggT}(m, n) = an + bm$ mit $a, b \in \mathbb{Z}$ (Lemma von Bezout)

(f) $\text{ggT}(kn, km) = k\text{ggT}(m, n)$ mit $k \geq 1$

Aufgabe 2 Euklidischer Algorithmus

Man benutze die Aussagen (a), (b) und (d) aus Aufgabe 1 und enwerfe einen Algorithmus, der bei Eingabe vom $m, n \in \mathbb{Z}$ den Wert $\text{ggT}(m, n)$ berechnet. Zeigen Sie, das dieser Algorithmus polynomiale Laufzeit hat.

Aufgabe 3 Erweiterter euklidischer Algorithmus

Man enwerfe einen Algorithmus, der bei Eingabe vom $m, n \in \mathbb{Z}$ den Wert $\text{ggT}(m, n)$ berechnet, sowie Zahlen $x, y \in \mathbb{Z}$ mit $\text{ggT}(m, n) = xm + yn$. Zeigen Sie, das dieser Algorithmus polynomiale Laufzeit hat.

Aufgabe 4

Es seien $m, n, k, a, b \in \mathbb{Z}$. Beweisen Sie folgende Aussagen:

(a) n und m relativ prim $\Leftrightarrow 1 = xn + ym$ mit $x, y \in \mathbb{Z}$

(b) n und k relativ prim $\Rightarrow \text{ggT}(n, mk) = \text{ggT}(n, m)$

(c) Sind n und m relativ prim, so gilt $n|k$ und $m|k$

(d) $\text{ggT}(n, m) = \text{ggT}(n \text{ Mod } m, m)$ mit $m \geq 1 \Rightarrow nm|k$

(e) $m|ab$ und $\text{ggT}(m, a) = 1 \Rightarrow n|b$

(f) $ab \equiv ac \bmod m$ und $\mathrm{ggT}(m, a) = 1 \Rightarrow a \equiv c \bmod m$

Aufgabe 5

Es seien n_1, n_2 relative prime natürliche Zahlen, $n = n_1 n_2$, und a_1, a_2 ganze Zahlen. Weiterhin sei

$$L = \{x \in \mathbb{Z} \mid x \equiv a_1 \,(\mathrm{mod}\, n_1) \text{ und } x \equiv a_2 \,(\mathrm{mod}\, n_2)\}.$$

man beweise folgende Aussagen:

(a) $L \neq \varnothing$ (man benutze das Lemma von Bezout über den ggt).

(b) Sine $x, y \in L$, so ist $x \equiv y \,(\mathrm{mod}\, n)$.

(c) $|L \cap \mathbb{Z}_n| = 1$.

Aufgabe 6

Wir betrachten das RSA Systems $\mathrm{RSA}(n, p, q, g, k, g)$ mit $p = 11, q = 23$ und $k = 3$. Geben Sie n und eine Primfaktorzerlegung von $\varphi(n)$ an. Erläutern Sie, wie man mit Hilfe des erweiterten euklidischen Aolgorithmeus g bestimmen kann.

Aufgabe 7

Ein Nutzer des RSA Systems $\mathrm{RSA}(n, p, q, g, k, g)$ hat den öffentlichen Schlüssel $n = 94058057$ und $k = 1723$; er hat die Geheimnachricht $C = 87272685$ erhalten. Wie lautet der Klartext T. Der Klartext T enspricht einen Wort über eine Alphabet $A = \{A = 10, B = 11, \ldots, X = 33, Y = 34, Z = 35\}$.

Aufgabe 8

Erzeugen Sie zwei 8-Bit-Primzahlen p und q, so dass $n = pq$ eine 16-Bit-Zahl ist und der öffentliche Schlüssel $k = 5$ verwendet werden kann. Berechnen Sie den geheimen Schlüssel g.