Wolfgang K. Seiler
Tel. 2515

A5, C201

6. Oktober 2015

4. Übungsblatt Algebra

Aufgabe 1: *(6 Punkte)*

Die Firmen `dot.com` und ΕΥΚΛΕΙΔΗΣ oHG beziehen beide ihre RSA-Moduln von der Firma *THRIFTY PRIMES* Inc. Diese erzeugt, getreu ihrem Namen, für beide zusammen nur drei Primzahlen p, q, r und schickt $m = pq = 88051$ an `dot.com` sowie $n = qr = 89197$ an die ΕΥΚΛΕΙΔΗΣ oHG.

a) Verschlüsseln Sie die „Nachricht“ 34159 an `dot.com` mit deren öffentlichem Exponenten $e = 3$!

b) Die ΕΥΚΛΕΙΔΗΣ oHG hat den öffentlichen Exponenten $e = 1943$. Berechnen Sie die Primzahlen p, q, r und den privaten Exponenten der ΕΥΚΛΕΙΔΗΣ oHG!

c) Unterschreiben Sie die „Nachricht“ 12345 im Namen der ΕΥΚΛΕΙΔΗΣ oHG!

NB: Alle notwendigen Rechnungen lassen sich auf einem Taschenrechner mit mindestens zehn Stellen ausführen, zur Not sogar von Hand. Bei *b)* wird es nicht gewertet, wenn Sie die beiden RSA-Moduln von einem Computeralgebrasystem faktorisieren lassen; der Rechengang Ihrer Faktorisierung muß vollständig dokumentiert sein.

Aufgabe 2: *(4 Punkte)*

G sei eine abelsche Gruppe und $g_1, \ldots, g_n \in G$. Zeigen Sie: Für jede Permutation

$$\pi\colon\{1,\ldots,n\} \to \{1,\ldots,n\} \qquad \text{ist} \qquad \prod_{i=1}^{n} g_i = \prod_{i=1}^{n} g_{\pi(i)}\,.$$

Aufgabe 3: *(5 Punkte)*

$G = \mathfrak{S}_3$ sei die Menge aller Permutationen $\pi\colon\{1,2,3\} \to \{1,2,3\}$.

a) Bestimmen für die Transposition $\tau = (1,2)$ die Rechts- und die Linksnebenklassen, und bestimmen Sie für jedes Element von $\mathfrak{S}_3$ sein Bild unter der Konjugation mit τ!

b) Bestimmen für den Dreierzyklus $\pi = (1,2,3)$ die Rechts- und die Linksnebenklassen, und bestimmen Sie für jedes Element von $\mathfrak{S}_3$ sein Bild unter der Konjugation mit π!

Aufgabe 4: *(5 Punkte)*

Zeigen Sie:

a) Eine Teilmenge $U \subseteq G$ einer Gruppe G ist genau dann eine Untergruppe, wenn sie nicht leer ist und wenn für alle $g, h \in U$ auch gh^{-1} in U liegt.

b) Eine endliche Teilmenge $U \subseteq G$ einer Gruppe G ist genau dann eine Untergruppe, wenn sie nicht leer ist und wenn $UU \subseteq U$ ist.

Abgabe bis zum Dienstag, dem 13. Oktober 2015, um 15.30 Uhr