Math 3140 - Assignment 3

Due September 14, 2016

(1) Let p, q be distinct primes. Show that $\varphi(pq) = (p-1)(q-1)$.

Hint: Count the multiples of p in $\{1, \ldots, pq\}$.

(2) Choose $p = 5, q = 11, e = 13$ for the RSA-system:

(a) What is the public key and what the private key?

(b) Encode $e_1 = 3$ and $e_2 = 22$ and then decode them again. Do you notice any problems?

(3) Let $n \in \mathbb{N}$ and $\mathbb{R}^{n \times n}$ the set of $n \times n$-matrices over $\mathbb{R}$. Which of the following are groups and why or why not?

(a) $(\mathbb{R}^{n \times n}, +)$ with matrix addition,

(b) $(\mathbb{R}^{n \times n}, \cdot)$ with matrix multiplication.

(4) Let $(G, \cdot)$ be a group.

(a) Show that each row of the multiplication table of G contains each element of G at least once (i.e., for given $a, c \in G$ find $b \in G$ such that $ab = c$).

(b) Show that each row of the multiplication table of G contains each element of G exactly once (i.e., $ab = ac$ implies $b = c$ for all $a, b, c \in G$).

Note that the same is true for columns.

(5) Show that there is only one group with three elements $1, a, b$.

Hint: Use the previous exercise to write down its multiplication table.