Fachbereich Mathematik
Elena Klimenko

WS 2017/18
Homework 2

NUMBER THEORY AND CRYPTOGRAPHY

Due in class on Friday, November 3rd, or on Tuesday, November 7th, at 12:05 pm.

1. Finding p and q using n and $\phi(n)$.

(a) Given n and $\phi(n)$, show how you can find p and q if you know that $n = pq$. Write your answer in the form of a quadratic equation whose solutions are p and q.

(b) Let $n = pq = 64777$ and $\phi(n) = 64260$. Use your result from (a) to find p and q with the help of a calculator.

2. We denote by $\mathbb{Z}_n$ the additive group of the ring $\mathbb{Z}/n\mathbb{Z}$ of integers modulo n. This group is cyclic.

(a) Find all generators of $\mathbb{Z}_{10}$.

(b) Prove that a number $a \in \mathbb{Z}_n$ generates $\mathbb{Z}_n$ if and only if $\gcd(a, n) = 1$.

3. Prove that

(a) $(\mathbb{Z}/8\mathbb{Z})^* \cong \mathbb{Z}_2 \times \mathbb{Z}_2$;

(b) $(\mathbb{Z}/16\mathbb{Z})^* \cong \mathbb{Z}_2 \times \mathbb{Z}_4$.

4. Prove Legendre's theorem from the theory of continued fractions: Let $p, q \in \mathbb{N}$ with $\gcd(p, q) = 1$. If $\left| x - \frac{p}{q} \right| < \frac{1}{2q^2}$, then $\frac{p}{q}$ is a convergent for x.