Fachbereich Mathematik
Elena Klimenko

WS 2017/18
Homework 4

# NUMBER THEORY AND CRYPTOGRAPHY

Due in class on Friday, November 17th, at 12:05 pm.

**1.** (a) Prove that 101101 is a Carmichael number.

(b) Prove that if the numbers $6k+1$, $12k+1$, and $18k+1$ are all prime (for some $k \in \mathbb{N}$), then their product is a Carmichael number.

(c) Using part (b), find a Carmichael number which is greater than 101101.

**2.** Write your version of the Miller–Rabin primality test with the following:

- INPUT: a natural number $n \geq 3$.
- OUTPUT: **composite** or **probably prime** (with probability $\geq 1 - \dfrac{1}{1000}$).

*Hint*: Please use not more than 10–15 lines. The first line of your algorithm can look as follows:

**1.** If $2|n$, then stop. Return **composite**.

**3.** Let $n$ be an odd number, $n-1 = 2^s d$ with $d$ odd. We denote by $L_n$ the set of all elements in $(\mathbb{Z}/n\mathbb{Z})^*$ that are *not* Miller–Rabin witnesses, that is,

$$L_n := \Big\{ a \in (\mathbb{Z}/n\mathbb{Z})^* \,\Big|\, a^d \equiv 1 (\text{mod } n) \text{ or } a^{2^r d} \equiv -1 (\text{mod } n) \text{ for some } r \in \{0, 1, \ldots, s-1\} \Big\}.$$

We already know that:

- $\#L_n = n - 1$ if $n$ is prime,
- $\#L_n \leq \phi(n)/4$ if $n$ is composite.

Find all elements of the set $L_n$ for $n = 91$.

**4.** Prove that for all $n \in \mathbb{N}$ the following inequalities hold:

$$\frac{4^n}{2\sqrt{n}} \leq \binom{2n}{n} < 4^n.$$