Fachbereich Mathematik
Elena Klimenko

WS 2017/18
Homework 5

NUMBER THEORY AND CRYPTOGRAPHY

Due in class on Friday, November 24th, at 12:05 pm.

1. Let $x > 0$ be a fixed real number. We consider a non-empty set of positive integers $S = \{a_1, a_2, \dots, a_n\}$ so that

$$a_1 < a_2 < \cdots < a_n \leq x$$

and neither of a_i's divides the product of the other elements in S.
Prove that then $n \leq \pi(x)$, where $\pi(x)$ is the prime-counting function.

2. For $n = 13$, find the smallest prime r that satisfies the following inequality:

$$\mathrm{ord}_r(n) > \log_2^2 n.$$

Explain your solution.

3. Find all pairs of integers (m, n) that satisfy the equation:

$$(5 + 3\sqrt{2})^m = (3 + 5\sqrt{2})^n.$$

Justify your answer.

4. Let p be a prime satisfying $p \equiv 3 \pmod 4$ and suppose that a is a quadratic residue modulo p.

(a) Show that $x = a^{(p+1)/4}$ is a solution to the congruence

$$x^2 \equiv a \pmod p.$$

(b) Find all solutions to the following congruence that lie in the interval between 1 and 163:

$$x^2 \equiv 74 \pmod{163}.$$

Show all work.