SAARLAND UNIVERSITY
Department of Mathematics
Prof. Dr. Mark Groves
MSc Jens Horn

Mathematics for Computer Scientists 1, WS 2018/19
Sheet 5

1. Calculate $(1552303, 233927)$ and find integers m and n such that

$$(1552303, 233927) = 1552303m + 233927n.$$

2. Let a and b be natural numbers and $d = (a, b)$.

(a) Show that d is the smallest element of the set

$$\{ma + nb : m, n \in \mathbb{Z}\} \cap \mathbb{N}.$$

(b) Suppose there are integers m and n such that $ma + nb = 1$. Deduce that $(a, b) = 1$.

3. (a) Compute the solution set of the simultaneous equations

$$\begin{aligned} x &\equiv 2 \text{ (mod 3)},\\ x &\equiv 5 \text{ (mod 7)},\\ x &\equiv 8 \text{ (mod 11)} \end{aligned}$$

by applying the Chinese remainder theorem twice.

(b) What are the last two digits of the number 49^{19}? [Hint: We want to compute the number 49^{19} (mod 100). Note that $100 = 25 \times 4$.]

4. (a) Show using Fermat's little theorem that 63 and 341 are not prime numbers.
[Hint: $62 = 6.10 + 2$, $340 = 3.113 + 1$ and

$$1 \equiv 2^6 \pmod{63}, \qquad 1 \equiv 56^3 \pmod{341}.]$$

(b) Show using Fermat's little theorem that 561 and 32769 are not prime numbers.

(c) Let p be a prime number. Show using Fermat's little theorem that

$$(a + b)^p \equiv (a^p + b^p) \pmod{p}.$$

(d) Compute

$$(3743^{3709} + 7420^{11127})^{3709} \pmod{3709}.$$

[Hint: 3709 is a prime number.]