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

Mathematics for Computer Scientists 1, WS 2018/19
Sheet 6

---

1. Bob's public key is (in the notation used in lectures)

$$n = 391, \qquad d = 13.$$

(a) Eve was however easily able to determine his private key. What is it?

(b) Which word did Alice send to Bob via the message

$$172, 260, 260, 192, 43, 260, 334, 68?$$

(c) Which message would Alice use to send the word 'INFORMATIK' to Bob?

[You should give all the steps in your calculations. Powers may be efficiently calculated in modular arithmetic using the 'square and multiply' procedure. For example:

$$\begin{aligned} 106 &\equiv 106 \pmod{143} \\ 106^2 &\equiv 11236 \equiv 82 \pmod{143} \\ 106^4 &\equiv (82)^2 \equiv 6724 \equiv 3 \pmod{143} \\ 106^8 &\equiv (3)^2 \equiv 9 \equiv 9 \pmod{143}, \end{aligned}$$

so that

$$106^{11} \equiv (106)^8 (106)^2 106 \equiv 9.82.106 \equiv 78227 \equiv 7 \pmod{143}. \,]$$

2. Prove the following assertions by mathematical induction.

(a) $\displaystyle\sum_{i=1}^{n} \log\left(1 + \frac{1}{i}\right) = \log(1+n)$ for each natural number n;

(b) $\displaystyle\prod_{i=1}^{n} (2i-1) = \frac{(2n)!}{2^n n!}$ for each natural number n;

(c) $n^2 \leq 2^n \leq n!$ for each natural number $n \geq 4$;

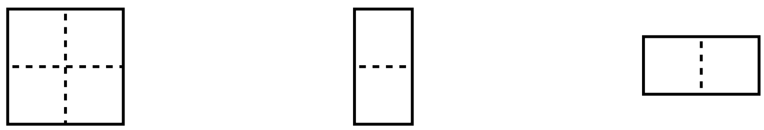
(d) $6 | (2^n + 3^n - 5^n)$ for each natural number n.

3. (a) Let $\mathcal{P}(n)$, $n \in \mathbb{N}$ be a predicate with the following properties:

- There exists $m \in \mathbb{N}$ such that $\mathcal{P}(1)$, $\ldots$, $\mathcal{P}(m)$ are true.
- Let $k > m$. $P(k)$ is true whenever $\mathcal{P}(j)$ is true for all $j < k$.

Deduce from the well-ordering axiom of the natural numbers that $P(n)$ is true for all $n \in \mathbb{N}$. (This is called **strong induction**.)

(b) The aim of 'mini-tetris' is to fill a $2 \times n$ rectangle (completely, and without overlaps) with tiles of the following type:



Let T_n be the number of ways of filling a $2 \times n$ rectangle with these tiles.

Determine T_1 und T_2, find a formula for T_n for $n \geq 3$ as a function of T_{n-1} and T_{n-2}, and prove by strong induction that

$$T_n = \frac{1}{3}[2^{n+1} + (-1)^n].$$