1) Imagine your PS-teacher has baked some cookies for the proseminar. If the cookies were given to three of you (shared equally) there would be one cookie left. If the cookies were given to four of you (shared eqally) there would be two cookies left. If the cookies were partitioned to all participants (25 students) of the proseminar then four would be left. Further the PS-teacher give you the hint that there was definitely no time to bake more than 300 cookies. How many cookies were baked?

   Solution: The situation described in the exercise corresponds to having three modulo equations, namely $x \equiv 1 \pmod 3$, $x \equiv 2 \pmod 4$, and $x \equiv 4 \pmod{25}$, where x is the number of cookies. Given that $0 \leq x \leq 300$ we have to find *the* number x, i.e. we have to find an x satisfying these constraints and show that it is the unique such.

   We proceed by first solving the first *two* congruences, i.e. by transforming it into a *single* new one, and then do that once more to solve the combination of that new one with the *third*.

   Consider the first two congruences $x \equiv 1 \pmod 3$ and $x \equiv 2 \pmod 4$. By the Chinese Remainder Theorem, which may be applied since $\gcd(3,4) = 1$, the solutions to these *two* congruences are the *same* as the solutions of the *single* congruence $x \equiv 10 \pmod{3 \cdot 4}$, where the 10 in the congruence is computed as $v \cdot q \cdot a + u \cdot p \cdot b$ after setting $a = 1$, $p = 3$, $b = 2$, $q = 4$ in Bézout's Lemma and computing u and v. That yields the solutions $u = -1$ and $v = 1$ of $\gcd(3,4) = 1 = u \cdot 3 + v \cdot 4$, from which we indeed find $v \cdot q \cdot a + u \cdot p \cdot b = 1 \cdot 4 \cdot 1 + (-1) \cdot 3 \cdot 2 = -2 = 10 \pmod{12}$.

   Now we are left with solving both the new congruence $x \equiv 10 \pmod{12}$ and the third one $x \equiv 4 \pmod{25}$. Again we apply the Chinese Remainder Theorem, using that $\gcd(12,25) = 1$, so the solutions to these two congruences are the same as the solutions to the single congruence $x \equiv 154 \pmod{12 \cdot 25}$, where the 154 is computed as $v \cdot q \cdot a + u \cdot p \cdot b$ now by taking $a = 10$, $p = 12$, $b = 4$, $q = 25$ in Bézout's Lemma, again computing u and v. That yields solutions $u = -2$ and $v = 1$ of $\gcd(12,25) = 1 = u \cdot 12 + v \cdot 25$, from which we indeed find $v \cdot q \cdot a + u \cdot p \cdot b = 1 \cdot 25 \cdot 10 + (-2) \cdot 12 \cdot 4 = 154 \pmod{300}$.

   Thus the solutions to the initial three congruences are the *same* as the solutions to $x \equiv 154 \pmod{300}$. Since 154 is the only such satisfying the further constraint $0 \leq x \leq 300$, we conclude that 154 is the *one and only* solution.

2) a) Let $C = \{(x,y) \mid x, y \in \mathbb{R},\ x^2 + y^2 = 1\}$ be the unit circle in 2 dimensions. What is $|C|$?

   b) Show that if $f : A \to B$ is surjective then $|A| \geq |B|$.

   c) Show that $|2^{\mathbb{N}}| = |4^{\mathbb{N}}|$. Recall that $2 = \{0,1\}$ and analogously $4 = \{0,1,2,3\}$ (or more generally any set with 2 elements, or with 4, respectively).

   d) Generalise the previous subexercise: under what conditions does $|A^{\mathbb{N}}| = |2^{\mathbb{N}}|$ hold? Give a sketch of the proof!

   Solution:

   a) The function $t : [0, 2\pi) \to C$, $(\cos t, \sin t)$ is a bijection. Since we showed $[0, 2\pi) = |\mathbb{R}|$ last time, we have $|C| = |\mathbb{R}|$.

b) For every value $y \in B$, there exists at least one $x \in A$ such that $f(x) = y$ (that is simply the definition of surjectivity). So, given some $y \in B$, let us pick an arbitrary such x and call it $g(y)$. We now claim that g is injective: if we have $g(y_1) = g(y_2)$ for $y_1, y_2 \in B$, then also $f(g(y_1)) = f(g(y_2))$, but $f(g(y_1)) = y_1$ and $f(g(y_2)) = y_2$ by definition of g. Thus, $y_1 = y_2$. The existence of an injection from B to A then implies $|B| \leq |A|$ as desired.

c) We can think of elements of $2^{\mathbb{N}}$ as infinite sequences of bits. If we group these into chunks of two, we obtain an infinite sequence of two-bit numbers, which can be interpreted as numbers from 0 to 3. This gives us an obvious bijection between $2^{\mathbb{N}}$ to $4^{\mathbb{N}}$. More formally, the following two functions are bijections:

$$g : 2 \times 2 \to 4,\ g(a, b) = 2a + b$$

$$f : 2^{\mathbb{N}} \to (2 \times 2)^{\mathbb{N}},\ f(h) = i \mapsto (h(2i), h(2i + 1))$$

And thus $|2^{\mathbb{N}}| = |(2 \times 2)^{\mathbb{N}}| = |4^{\mathbb{N}}|$.

d) $|A^{\mathbb{N}}| = |2^{\mathbb{N}}|$ holds if A is finite and $|A| \geq 2$. We use Schröder–Bernstein to prove it. The inequality $|A^{\mathbb{N}}| \geq |2^{\mathbb{N}}|$ is obvious since there is an injection $2 \to A$ since we assumed $|A| \geq 2$.

For the other direction, we choose $n \in \mathbb{N}$ such that $2^n \geq |A|$, which is possible since A is finite. Then we again group the bits, but this time in chunks of n, to get a bijection $2^{\mathbb{N}} \to (2^n)^{\mathbb{N}}$. Since $2^n \geq |A|$, we have $|(2^n)^{\mathbb{N}}| \geq |A^{\mathbb{N}}|$ and that concludes the proof.

3) All the following exercises should be computable by hand using appropriate results from the lecture. Don't use anything stronger than a 16-bit calculator.

a) Compute $(411^{4110} + 410) \bmod 4111$ given that 4111 is a prime.

b) Compute $\gcd(77, 111)$ using the two variants of the Euclidean algorithm from the lecture (the difference and the remainder variants). How many steps do you need with each of the variants?

c) Is the congruence class $\overline{77}$ modulo 111 invertible? If so, compute its inverse. Then find some n such that $\overline{77}$ modulo n is not invertible.

d) Compute $111^{60} \bmod 77$ using the Euler's theorem.

Solution:

a) Since 4111 is a prime number and $4111 \nmid 411$ we can use the Fermat's little theorem and we obtain $411^{(4111-1)} \equiv 1 \bmod 4111$. Hence $411^{4110} + 410 \equiv 1 + 410 \equiv 411 \bmod 4111$.

b) We obtain that $\gcd(77, 111) = 1$. With the difference variant we get the following.

$$(77, 111) \to (77, 34) \to (43, 34) \to (9, 34) \to (9, 25) \to (9, 16) \to$$
$$(9, 7) \to (2, 7) \to (2, 5) \to (2, 3) \to (2, 1) \to (1, 1)$$

With the remainder variant we get the following.

$$(77, 111) \to (77, 34) \to (9, 34) \to (9, 7) \to (2, 7) \to (2, 1)$$

c) Yes, it is invertible since $\gcd(77, 111) = 1$. Using the Bezout's lemma we obtain that $1 = -49 \cdot 77 + 34 \cdot 111$. The algorithm runs as follows.

A	B	q
$(77, 1, 0)$	$(111, 0, 1)$	0
$(111, 0, 1)$	$(77, 1, 0)$	1
$(77, 1, 0)$	$(34, -1, 1)$	2
$(34, -1, 1)$	$(9, 3, -2)$	3
$(9, 3, -2)$	$(7, -10, 7)$	1
$(7, -10, 7)$	$(2, 13, -9)$	3
$(2, 13, -9)$	$(1, -49, 34)$	

Hence by the lemma from the lecture we obtain that the inverse of $\overline{77}$ modulo 111 is $\overline{-49} = \overline{62}$.

The congruence class $\overline{77}$ modulo n is invertible if and only if $\gcd(77, n) = 1$. Hence it is not invertible for $n = 7$ or for $n = 11$, for example.

d) We notice that $77 = 7 \cdot 11$ is a product of two primes, and that $(7 - 1) \cdot (11 - 1) = 60$. We also know from above that $\gcd(7 \cdot 11, 111) = 1$ and hence by the Euler's theorem we obtain that $111^{60} = 111^{(7-1)\cdot(11-1)} \equiv 1 \bmod 7 \cdot 11$.

4*) In the following exercise, provide a *constructive* definitions of the functions which allow you to compute function values from arguments (as if you were to write a program).

a) Construct a bijection f_3 from $\mathbb{N}^3$ to $\mathbb{N}$. (Hint: Extend the *dove tailing* function from the lecture.)

b) Generalize the above function f_3 to a bijection f_n from $\mathbb{N}^n$ to $\mathbb{N}$ ($n > 3$).

c) Let $\mathbb{N}^\star$ be the set of all finite sequences of natural numbers which don't end with 0. Provide a constructive definition of a bijection from $\mathbb{N}$ to $\mathbb{N}^\star$. List the first 10 sequences in your enumeration.

d) Let A be the set of all finite words over the alphabet $\{\mathtt{a}, \mathtt{b}\}$ (including the empty word). Construct a bijection from A to $\mathbb{N}$.

Solution:

a) We can use the *dove tailing* function f_2 from the lecture $f_2(a, b) = a + \frac{1}{2}(a + b)(a + b + 1)$ to encode pairs of natural $\langle a, b\rangle$ numbers by a natural number. We can easily encode the triple $\langle a, b, c\rangle$ using pairs as $\langle a, \langle b, c\rangle\rangle$. This gives us the function $f_3(a, b, c) = f_2(a, f_2(b, c))$.

b) Similarly as above, we can encode a sequence of n numbers $\langle a_1, a_2, \ldots, a_n\rangle$ just like lists in functional programming using pairs as $\langle a_1, \langle a_2, \ldots, \langle a_{n-1}, a_n\rangle \cdots\rangle\rangle$ and this gives us the function $f_n(a_1, \ldots, a_n) = f_2(a_1, f_2(\ldots, f_2(a_{n-1}, a_n)))$ or written recursively as $f_n(a_1, \ldots, a_n) = f_2(a_1, f_{n-1}(a_2, \ldots, a_n))$.

c) Let p_n denote the n-th prime number ($p_0 = 2$, $p_1 = 3$, $\ldots$). Given $n \geq 2$, we can write n uniquely as a product of powers of primes as $n = p_0^{c_0} p_1^{c_1} \cdots p_k^{c_k}$ where p_k is the largest prime that divides n and hence $c_k > 0$. Note that some c_i might be 0 for $i < k$. We can define function f_0 which maps each $n \geq 2$ to this sequence as $f_0(n) = \langle c_0, c_1, \ldots, c_k\rangle$. This is almost the desired bijection with the problem that 0 and 1 are not mapped to anything in $\mathbb{N}^\star$, and nothing is mapped to the empty sequence

$\langle\rangle$. However, f_0 is a bijection from $\mathbb{N} \setminus \{0, 1\}$ to $\mathbb{N}^\star \setminus \{\langle\rangle\}$. Hence we define $f_\star(0) = \langle\rangle$ and $f_\star(n) = f_0(n+1)$ for $n > 0$. The first 10 sequences in this enumeration are: $\langle\rangle, \langle 1\rangle, \langle 0, 1\rangle, \langle 2\rangle, \langle 0, 0, 1\rangle, \langle 1, 1\rangle, \langle 0, 0, 0, 1\rangle, \langle 3\rangle, \langle 0, 2\rangle, \langle 1, 0, 1\rangle$.

d) We can interpret `a` and `b` as 0 and 1, and consider the sequence of characters as a binary number representation. However, a straightforward attempt like this will map both `aab` and `ab` to the same binary number 001 and 01, that is 1.

To fix this, we simply always add a leading 1, e.g. the word `aab` is mapped to 1001 and the word `ab` is mapped to 101. With this, we have a bijection between A and $\mathbb{N} - 1$. By subtracting 1 from the result, it becomes a bijection between A and $\mathbb{N}$ as desired.