# Elementary Number Theory - Exercise 1a

ETH Zürich - Dr. Markus Schwagenscheidt - Spring Term 2023

**Problem 1.** Show that $a \mid b$ and $b \mid a$ imply $a = \pm b$.

**Problem 2.** Show that each composite natural number $n$ has a prime factor $\leq \sqrt{n}$.

**Problem 3.** Determine the prime factorization of 1584. Can you turn your method into an algorithm?

**Problem 4.** Show that there are infinitely many primes.
*Hint:* Assume that there are only finitely many primes $p_1, \ldots, p_r$ and consider $m = p_1 p_2 \cdots p_r + 1$.

**Problem 5.** (Homework) We have seen in the lecture that every natural number $n > 1$ has a unique prime factorization. In this problem, we want to see that an analogous statement may fail in other number systems. We consider the set

$$2\mathbb{Z} = \{2n \,:\, n \in \mathbb{Z}\}$$

of even integers.

1. Check that $2\mathbb{Z}$ is closed under addition and multiplication.
2. An even integer is called *irreducible* if it cannot be written as a product of two even integers. Write down the first 10 positive irreducible even integers. How do they look in general?
3. Show that every even integer can be written as a product of irreducible even integers.
4. Shows that the decomposition into irreducible even integers is not unique.

**Problem 6.** (Homework) Show that there are infinitely many primes of the form $4n + 3$.

*Hints:*

1. Assume that there are only finitely many such primes, $p_0 = 3, p_1 = 7, \ldots, p_r$, and consider $m = 4p_1 \cdots p_r + 3$ (omit $p_0 = 3$ in the product).
2. Show that the product of two numbers of the form $4n + 1$ is again of this form.
3. Show that $m$ has a prime factor of the form $4n + 3$, and derive a contradiction.

**Problem 7** (sage)**.** Implement the following functions in sage:

1. `divides(a,b)`: given two integers $a, b$, return `true` if $a \mid b$, and `false` otherwise.
2. `is_prime(n)`: given a natural number $n$, return `true` if $n$ is prime, and `false` otherwise.
3. `primes_below(N)`: given a natural number $N$, print all primes $p \leq N$.
4. `factor(n)`: given a natural number $n$, compute the prime factorization of $n$.
   If $n = p_1^{\nu_1} \cdots p_r^{\nu_r}$ with different primes $p_j$, the output could be an array

   $$[[p_1, \nu_1], \ldots, [p_r, \nu_r]]$$

   consisting of $r$ tuples (=arrays) containing the primes $p_j \mid n$ with their multiplicities $\nu_j$.