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 $a = \pm b$.

Solution 1. If $a \mid b$ and $b \mid a$, then there are integers c, d such that $ac = b$ and $bd = a$. This implies $acd = bd = a$, hence

$$a(cd - 1) = 0.$$

Now either $a = 0$, in which case $0 = ac = b$, or $cd = 1$, which implies $c = d = \pm 1$. In either case, we find that $a = \pm b$.

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

Solution 2. Write $n = ab$ with $1 < a, b < n$. Suppose that $b \geq \sqrt{n}$. Then $a = \frac{n}{b} \leq \frac{n}{\sqrt{n}} = \sqrt{n}$. Hence n has a factor $\leq \sqrt{n}$. If a is not prime, then any prime factor of a (here we use that $a > 1$, so a has prime factors) will also be a prime factor of n, which is $\leq \sqrt{n}$.

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

Solution 3. We first divide by 2 several times:

$$\begin{aligned} 1584 &= 2 \cdot 792 \\ &= 2 \cdot 2 \cdot 396 \\ &= 2 \cdot 2 \cdot 2 \cdot 198 \\ &= 2 \cdot 2 \cdot 2 \cdot 2 \cdot 99. \end{aligned}$$

Next, we divide by 3 as along as possible

$$\begin{aligned} 1584 &= 2 \cdot 2 \cdot 2 \cdot 2 \cdot 3 \cdot 33 \\ &= 2 \cdot 2 \cdot 2 \cdot 2 \cdot 3 \cdot 3 \cdot 11. \end{aligned}$$

We obtain the prime factorization $1584 = 2^4 \cdot 3^2 \cdot 11$.

In general, the prime factorization of n can be obtained by dividing n by 2 as long as possible, then by 3, then by 5, 7, 11, and so on.

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

Solution 4. Assume that there are only finitely many primes $p_1, \dots, p_r$. By the Fundamental Theorem of Arithmetic, $m = p_1 \cdots p_r + 1$ has a prime factorization. In particular, m is divisible by some prime p. However, since m is not divisible by any of the primes $p_1, \dots, p_r$ ($p_j \mid m$ would would imply that $p_j \mid m - p_1 \cdots p_r = 1$, which is impossible), this prime p is not in our finite list of primes $p_1, \dots, p_r$, which is a contradiction.

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.

Solution 5. 1. We have $2n + 2m = 2(n + m)$ and $2n \cdot 2m = 2(2mn)$, so $2\mathbb{Z}$ is closed under addition and multiplication.

2. The first 10 positive irreducible even integers are:

$$2, 6, 10, 14, 18, 22, 26, 30, 34, 38.$$

The irreducible even integers are those of the form $2n$ with n odd. Alternatively, they are of the form $4m + 2$ with $m \in \mathbb{Z}$.

3. Let $n \in 2\mathbb{Z}$ and consider the prime factorization

$$n = 2^k p_1^{\nu_1} \cdots p_r^{\nu_r}$$

with $k \in \mathbb{N}$ and $p_1, \ldots, p_r$ odd primes. In particular, we can write $n = 2^k m$ with m an odd integer. Hence

$$n = 2m \cdot 2^{k-1}$$

is a factorization of n into irreducible even numbers (since $2m$ and 2 are irreducible).

4. The factorization into irreducible even number is not unique since we can distribute the odd prime factors of an integer to different irreducible factors. For example, we take $60 = 2^2 \cdot 3 \cdot 5$, and get the irreducible factorizations

$$60 = \underbrace{6}_{=2\cdot 3} \cdot \underbrace{10}_{=2\cdot 5} = 2 \cdot \underbrace{30}_{=2\cdot 3\cdot 5}.$$

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.

Solution 6. Since m is odd, all prime factors of m are odd (in other words, the prime 2 does not appear in the prime factorization of m). Note that every odd number is either of the form $4n + 1$ or $4n + 3$. Moreover, the product of two numbers of the form $4n + 1$ is again of this form:

$$(4n + 1)(4k + 1) = 16nk + 4(k + n) + 1 = 4(4nk + k + n) + 1.$$

Hence, if all prime factors of m would be of the form $4n + 1$, then m would also be of this form. But m is of the form $4n + 3$, so it must have a prime factor p of the form $4n + 3$. Note that m is not divisible by 3 (this would imply $3 \mid m - 3 = 4p_1 \cdots p_r$, but none of the primes $p_1, \ldots, p_r$ is equal to 3), so $p \neq 3$. Similarly, m is not divisible by any of the primes $p_1, \ldots, p_r$, so p is none of these primes. Hence, p is a prime of the form $4n + 3$ that is not in our finite list of primes, which is 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 ν_j.