1. Divisibility. Unique Factorization Theorem

1.1. Definition. Let $x, y \in \mathbb{Z}$ be two integers. We define

$$x \mid y \qquad \text{(read: } x \textit{ divides } y\text{)},$$

iff there exists an integer q such that $y = qx$. We write $x \nmid y$, if this is not the case.

1.2. We list some simple properties of divisibility for numbers $x, y, z \in \mathbb{Z}$.

i) $(x \mid y \ \wedge \ y \mid z) \implies x \mid z$.

ii) $x \mid 0$ for all $x \in \mathbb{Z}$.

iii) $0 \mid x \implies x = 0$.

iv) $1 \mid x$ and $-1 \mid x$ for all $x \in \mathbb{Z}$.

v) $(x \mid y \ \wedge \ y \mid x) \implies x = \pm y$.

1.3. Definition. A *prime number* is an integer $p \geq 2$ such that there doesn't exist any integer x with $1 < x < p$ and $x \mid p$.
So the only positive divisors of a prime number p are 1 and p. Note that by definition 1 is not a prime number.

Every integer $x \geq 2$ is either a prime or a product of a finite number of primes. This can be easily proved by induction on x. The assertion is certainly true for $x = 2$. Let now $x > 2$, and assume that the assertion has already been proved for all integers $x' < x$. If x is a prime, we are done. Otherwise there exists a decomposition $x = yz$ with integers $2 \leq y, z < x$. By induction hypothesis, y and z can be written as products of primes

$$y = \prod_{i=1}^{n} p_i, \quad z = \prod_{j=1}^{m} q_j, \qquad (m, n \geq 1, \ p_i, q_j \text{ prime})$$

Multiplying these two formulas gives the desired prime factorization of x.
Using the convention that an empty product (with zero factors) equals 1, we can state that any positive integer x is a product of primes

$$x = \prod_{i=1}^{n} p_i, \quad n \geq 0, \ p_i \text{ primes}.$$

We can now state and prove Euclid's famous theorem on the infinitude of primes.

1.4. Theorem (Euclid). *There exist infinitely many prime numbers.*
Proof. Assume to the contrary that there are only finitely many primes and that

$$p_1 := 2, \ p_2 := 3, \ p_3, \ldots, p_n$$

Chap. 1 last revised: 2003-04-14

is a complete list of all primes. The integer

$$x := p_1 \cdot p_2 \cdot \ldots \cdot p_n + 1$$

must be a product of primes, hence must be divisible by at least one of the p_i, $i = 1, \ldots, n$. But this is impossible since

$$\frac{x}{p_i} = (\text{integer}) + \frac{1}{p_i}$$

is not an integer. Hence the assumption is false and there exist infinitely many primes.

Whereas the existence of a prime factorization was easy to prove, the uniqueness is much harder. For this purpose we need some preparations.

1.5. Definition. Two integers $x, y \in \mathbb{Z}$ are called *relatively prime* or *coprime* (G. *teilerfremd*) if they are not both equal to 0 and there does not exist an integer $d > 1$ with $d \mid x$ and $d \mid y$.

This is equivalent to saying that x and y have no common prime factor.

In particular, if p is a prime and x an integer with $p \nmid x$, then p and x are relatively prime.

1.6. Theorem. *Two integers x, y are coprime iff there exist integers n, m such that*

$$nx + my = 1.$$

Proof. "$\Leftarrow$" If $nx + my = 1$, every common divisor d of x and y is also a divisor of 1, hence $d = \pm 1$. So x and y are coprime.

"$\Rightarrow$" Suppose that x, y are coprime. Without loss of generality we may assume $x, y \geq 0$. We prove the theorem by induction on $\max(x, y)$.

The assertion is trivially true for $\max(x, y) = 1$.

Let now $N := \max(x, y) > 1$ und suppose that the assertion has already been proved for all integers x', y' with $\max(x', y') < N$. Since x, y are coprime, we have $x \neq y$, so we may suppose $0 < x < y$. Then $(x, y - x)$ is a pair of coprime numbers with $\max(x, y - x) < N$. By induction hypothesis there exist integers n, m with

$$nx + m(y - x) = 1,$$

which implies $(n - m)x + my = 1$, q.e.d.

1.7. Theorem. *Let $x, y \in \mathbb{Z}$. If a prime p divides the product xy, then $p \mid x$ or $p \mid y$.*

Proof. If $p \mid x$, we are done. Otherwise p and x are coprime, hence there exist integers n, m with $np + mx = 1$. Multiplying this equation by y and using $xy = kp$ with an integer k, we obtain

$$y = npy + mxy = npy + mkp = p(ny + mk).$$

This shows $p \mid y$, q.e.d.

1.8. Theorem (Unique factorization theorem). *Every positive integer can be written as a (finite) product of prime numbers. This decomposition is unique up to order.*

Proof. The existence of a prime factorization has already been proved, so it remains to show uniqueness. Let

$$x = p_1 \cdot \ldots \cdot p_n = q_1 \cdot \ldots \cdot q_m \tag{$*$}$$

be two prime factorizations of a positive integer x. We must show that $m = n$ and after rearrangement $p_i = q_i$ for all i. We may assume $n \le m$. We prove the assertion by induction on n.

a) If $n = 0$, it follows $x = 1$ and $m = 0$, hence the assertion is true in this case.

b) *Induction step* $n-1 \to n$, $(n \ge 1)$. We have $p_1 \mid q_1 \cdot \ldots \cdot q_m$, hence by theorem 1.7, p_1 must divide one of the factors q_i and since q_i is prime, we must have $p_1 = q_i$. After reordering we may assume $i = 1$. Dividing equation $(*)$ by p_1 we get

$$p_2 \cdot \ldots \cdot p_n = q_2 \cdot \ldots \cdot q_m.$$

By induction hypothesis we have $n = m$ and, after reordering, $p_i = q_i$ for all i, q.e.d.

If we collect multiple occurrences of the same prime, we can write every positive integer in a unique way as

$$x = \prod_{i=1}^{n} p_i^{e_i}, \quad p_1 < p_2 < \ldots < p_n \text{ primes}, \; n \ge 0, e_i > 0.$$

This is called the canonical prime factorization of x.

Sometimes a variant of this representation is useful. For an integer $x \ne 0$ and a prime p we define

$$\operatorname{ord}_p(x) := \sup\{e \in \mathbb{N}_0 : p^e \mid x\}.$$

Then every nonzero integer x can be written as

$$x = \operatorname{sign}(x) \prod_p p^{\operatorname{ord}_p(x)}$$

where the product is extended over all primes. Note that $\operatorname{ord}_p(x) = 0$ for all but a finite number of primes, so there is no problem with the convergence of the infinite product.

1.9. Definition (Greatest common divisor). Let $x, y \in \mathbb{Z}$. An integer d is called *greatest common divisor* of x and y, if the following two conditions are satisfied:

i) d ist a common divisor of x and y, i.e. $d \mid x$ and $d \mid y$.

ii) If d_1 is any common divisor of x and y, then $d_1 \mid d$.

If d_1 and d_2 are two greatest common divisors of x and y, then $d_1 \mid d_2$ and $d_2 \mid d_1$, hence by 1.2.v) we have $d_1 = \pm d_2$. Therefore the greatest common divisor is (in case of existence) uniquely determined up to sign. The positive one is denoted by $\gcd(x, y)$. The existence can be seen using the prime factor decomposition. For $x \neq 0$ and $y \neq 0$,

$$\gcd(x, y) = \prod_p p^{\min(\operatorname{ord}_p(x), \operatorname{ord}_p(y))}$$

and $\gcd(x, 0) = \gcd(0, x) = |x|$, $\gcd(0, 0) = 0$.

Two integers x, y are relatively prime iff $\gcd(x, y) = 1$.

The following is a generalization of theorem 1.6.

1.10. Theorem. *Let $x, y \in \mathbb{Z}$. An integer d is greatest common divisor of x and y iff*

i) *d is a common divisor of x and y, and*

ii) *there exist integers n, m such that*

$$nx + my = d.$$

Proof. The case when at least one of x, y equals 0 is trivial, so we may suppose $x \neq 0$, $y \neq 0$.

"$\Rightarrow$" If d is greatest common divisor of x and y, then x/d and y/d are coprime, hence by theorem 1.6 there exist integers n, m with

$$n\frac{x}{d} + m\frac{y}{d} = 1,$$

which implies ii).

The implication "$\Leftarrow$" is trivial.

1.11. Definition (Least common multiple). Let $x, y \in \mathbb{Z}$. An integer m is called *least common multiple* of x and y, if the following two conditions are satisfied:

i) m ist a common multiple of x and y, i.e. $x \mid m$ and $y \mid m$.

ii) If m_1 is any common multiple of x and y, then $m \mid m_1$.

As in the case of the greatest common divisor, the least common multiple of x and y is uniquely determined up to sign. The positive one is denoted by $\operatorname{lcm}(x, y)$. For $x \neq 0$ and $y \neq 0$ the following equation holds

$$\operatorname{lcm}(x, y) = \prod_p p^{\max(\operatorname{ord}(x), \operatorname{ord}(y))}$$

and $\operatorname{lcm}(x, 0) = \operatorname{lcm}(0, x) = \operatorname{lcm}(0, 0) = 0$.

The definitions of the greatest common divisor and least common multiple can be extended in a straightforward way to more than two arguments. One has

$$\begin{aligned}
\gcd(x_1, \ldots, x_n) &= \gcd(\gcd(x_1, \ldots, x_{n-1}), x_n), \\
\operatorname{lcm}(x_1, \ldots, x_n) &= \operatorname{lcm}(\operatorname{lcm}(x_1, \ldots, x_{n-1}), x_n).
\end{aligned}$$