D_M-07 MA-217 Discrete Mathematics / Jan-Apr 2007

Lectures : Tuesday/Thursday 15:45–17:15 ; Lecture Hall-1, Department of Mathematics

3. The Natural Numbers — The Fundamental Theorem of Arithmetic[1]), Factorisation in Monoids

3.1. a). Let $a, b, m, k \in \mathbb{N}$ be such that $\binom{a}{k} \leq m < \binom{a+1}{k}$ and $\binom{b}{k} \leq m < \binom{b+1}{k}$. Show that $a = b$. (**Hint :** Suppose that $a < b$, i.e., $a + 1 \leq b$, then $m < \binom{a+1}{k} \leq \binom{b}{k} \leq m$, since $\mathfrak{P}_k(\{1, \ldots, a+1\}) \subseteq \mathfrak{P}_k(\{1, \ldots, b\})$ a contradiction.)

b). Let $k \in \mathbb{N}^+$ be a positive natural number and let $n \in \mathbb{N}$ be an arbitrary natural number. Show that there exist unique natural numbers $a_1, \ldots, a_k \in \mathbb{N}$ such that $0 \leq a_1 < a_2 < \cdots < a_k$ and $n = \sum_{j=1}^{k} \binom{a_j}{j}$. (**Hint :** The existence of $a_1, \ldots, a_k$ is proved by induction on k. If $k = 1$, then $n = \binom{n}{1}$ is the required representation. Assume $k > 1$ and choose $a_k \in \mathbb{N}$ with $\binom{a_k}{k} \leq n \langle \binom{a_k+1}{k}$. For the number $m := n - \binom{a_k}{k} \geq 0$ by induction hypothesis there exists a representation $m = \sum_{j=1}^{k-1} \binom{a_j}{j}$ with $0 \leq a_1 < a_2 < \cdots < a_{k-1}$. Now we need to show that $a_{k-1} < a_k$. Since $\binom{a_k+1}{k} = \binom{a_k}{k} + \binom{a_k}{k-1}$, we have $n = \sum_{j=1}^{k-1} \binom{a_j}{j} + \binom{a_k+1}{k} - \binom{a_k}{k-1} < \binom{a_k+1}{k}$; in particular, $\binom{a_{k-1}}{k-1} < \binom{a_k}{k-1}$ and hence $a_{k-1} < a_k$. Now we prove the uniqueness of $a_1, \ldots, a_k$. If $k = 1$, this is trivial. Assume $k \rangle 1$ and suppose that $n = \sum_{j=1}^{k} \binom{a_j}{j} = \sum_{j=1}^{k} \binom{b_j}{j}$ with $0 \leq a_1 < a_2 < \cdots < a_k$ and $0 \leq b_1 < b_2 < \cdots < b_k$. It is enough to show that $\binom{a_k}{k} \leq n < \binom{a_k+1}{k}$ and $\binom{b_k}{k} \leq n < \binom{b_k+1}{k}$, for then, $a_k = b_k$ by part a) and by induction hyposthesis to the two representations of $m := n - \binom{a_k}{k} = n - \binom{b_k}{k}$, we get $a_j = b_j$ for all $k = 1, \ldots, k-1$. Now, we show that $\binom{a_k}{k} \leq n < \binom{a_k+1}{k}$. If $a_k < k$, then $a_j = j - 1$ for all $j = 1, \ldots, k$ and $\binom{a_k}{k} = \binom{k-1}{k} = 0 = n < \binom{a_k+1}{k} = \binom{k}{k} = 1$. Therefore suppose that $a_k \geq k$. Then $\binom{a_k+1}{k} = \sum_{i=0}^{k} \binom{a_k-i}{k-i}$ (by recursion formula) and hence $\binom{a_k}{k} = \binom{a_k+1}{k} - \sum_{i=1}^{k} \binom{a_k-i}{k-i}$ and $n = \sum_{i=0}^{k} \binom{a_i}{i} = \sum_{j=1}^{k-1} \binom{a_{k-j}}{k-j} + \binom{a_k}{k} = \binom{a_k+1}{k} - \binom{a_k-k}{0} + \sum_{j=1}^{k-1} \left(\binom{a_{k-j}}{k-j} - \binom{a_k-j}{k-j} \right) = \binom{a_k+1}{k} - 1 - \sum_{j=1}^{k-1} \left(\binom{a_{k-j}}{k-j} - \binom{a_k-j}{k-j} \right)$. Now, since $a_k - 1 \geq a_{k-1}$ and by induction $a_k - j \geq a_{k-j}$ for every $1 \leq j \leq k-1$ and hence $\sum_{j=1}^{k-1} \left(\binom{a_{k-j}}{k-j} - \binom{a_k-j}{k-j} \right) \geq 0$. This proves that $n < \binom{a_k+1}{k}$, the other inequality $\binom{a_k}{k} \leq n$ is trivial.)

c). For $k \in \mathbb{N}$, $k \geq 1$, show that the map $\mathbb{N}^k \to \mathbb{N}$ defined by

$$(m_1, m_2, \ldots, m_k) \mapsto \binom{m_1}{1} + \binom{m_1 + m_2 + 1}{2} + \cdots + \binom{m_1 + m_2 + \cdots + m_k + k - 1}{k}$$

is bijective. (**Hint :** Use part b).)

3.1. (Gödelisation) Let $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, ... be (infinite) sequence of the prime numbers.

a). Let A be a countable set with an enumeration $A = \{a_1, a_2, a_3, \ldots\}$, $a_i \neq a_j$ for $i \neq j$. Then the map $(a_{i_1}, \ldots, a_{i_n}) \mapsto p_1^{i_1} \cdots p_n^{i_n}$ is an injective map from the set $\mathrm{W}(A) := \biguplus_{n \in \mathbb{N}} A^n$ of finite sequences (of arbitrary lengths) of elements from A - such sequences are also called words over the alphabet A - into the set $\mathbb{N}^*$ of positive natural numbers. (**Remark :** Such a coding of the words over A is called a Gödelisation (due to K. Gödel). The natural number associated to a word is called the Gödel number of this word.)

b). Let A be a finite alphabet $\{a_1, a_2, \ldots, a_g\}$ with g letters, $g \geq 2$, and $a_0 \notin A$ be another letter. A word $W = (a_{i_1}, \ldots, a_{i_n})$ over A can be identified by filling a_0 with the infinite sequence

[1]) The Fundamental Theorem of Arithmetic does not seem to have been stated explicitly in EUCLIDs elements, although some of the propositions in book VII and/or IX are almost equivalent to it. Its first clear formulation with proof seems to have been given by GAUSS in *Disquisitiones arithmeticae* §16 (Leipzig, Fleischer, 1801). It was, of course, familier to earlier mathematicians; but GAUSS was the first to develop arithmetic as a systematic science.

$(a_{i_1}, \ldots a_{i_n}, a_0, a_0, \ldots)$. Show that: the map $(a_{i_\nu})_{\nu\in\mathbb{N}^*} \mapsto \sum_{\nu=1}^{\infty} i_\nu g^{\nu-1}$ is a bijective map from the set of words over A onto the set $\mathbb{N}$ of the natural numbers and in particular, is a Gödelisation. (**Remark :** This is a variant of the g-adic expansion (see T3.4.)

3.2. Let $g \in \mathbb{N}^*$, $g \geq 2$, n be a natural number with digit-sequence $(r_i)_{i\in\mathbb{N}}$ in the g-adic expansion of n and let $d \in \mathbb{N}^*$. (see T3.4.)

a). Suppose that d is a divisor of g^α for some $\alpha \in \mathbb{N}^*$. Then $n \equiv (r_{\alpha-1}, \ldots, r_0)_g \bmod d$. In particular, d divides the number n if and only if d divides the number $(r_{\alpha-1}, \ldots, r_0)_g$.

b). Suppose that d is a divisor of $g^\alpha - 1$ for some $\alpha \in \mathbb{N}^*$ and

$$S := (r_{\alpha-1}, \ldots, r_0)_g + (r_{2\alpha-1}, \ldots, r_\alpha)_g + \cdots .$$

Then $n \equiv S \bmod d$. In particular, d divides the number n if and only if d divides the sum S.

c). Suppose that d is a divisor of $g^\alpha + 1$ for some $\alpha \in \mathbb{N}^*$ and

$$W := (r_{\alpha-1}, \ldots, r_0)_g - (r_{2\alpha-1}, \ldots, r_\alpha)_g + \cdots .$$

Then $n \equiv W \bmod d$. In particular, d divides the number n if and only if d divides the alternating sum W. (**Remark :** With the help of this exercise one can find criterion, which one can decide on the basis the digit-sequence of the natural number n in the decimal system whether d is a divisor of n with $2 \leq d \leq 16$. (with $d = 3$ and $d = 9$ one uses the simple check-sum, with $d = 11$ the simple alternating sum. The divisibility by $7, 11$ and 13 at the same time can be tested with the alternating sum of the 3- groupped together in view of the part c). See T3.4. for details.)

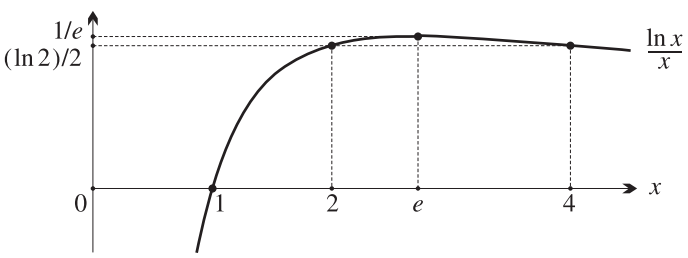
3.3. a). For $a, m, n \in \mathbb{N}^*$ with $a \geq 2$ and $d := \gcd(m, n)$, show that $\gcd(a^m - 1, a^n - 1) = a^d - 1$. In particular, $a^m - 1$ and $a^n - 1$ are relatively prime if and only if $a = 2$ and m and n are relatively prime. (**Hint :** By substituting a^d by a one may assume that $d = 1$. Then show that $(a^m - 1)/(a - 1) = a^{m-1} + \cdots + a + 1$ and $(a^n - 1)/(a - 1) = a^{n-1} + \cdots + a + 1$ are relatively prime.)

b). Suppose that $a_1, \ldots, a_n \in \mathbb{N}^*$ are relatively prime. Show that there exists a natural number $f \in \mathbb{N}$ such that every natural number $b \geq f$ ca be represented as $b = u_1a_1 + \cdots + a_na_n$ with *natural* numbers $u_1, \ldots, u_n$. In the case $n = 2$, we have $f := (a_1 - 1)(a_2 - 1)$ is the smallest such number; further in this case there are exactly $f/2$ natural numbers c, which donot have a representation of the form $u_1a_1 + u_2a_2$, $u_1, u_2 \in \mathbb{N}$. (**Hint :** For $0 \leq c \leq f - 1$, exactly one of the number c and $f - 1 - c$ can be represented in the above form.)

c). Let $a, b \in \mathbb{N}^*$ and $d := \gcd(a, b) = sa + tb$ with $s, t \in \mathbb{Z}$. Then $d = s'a + t'b$ for $s', t' \in \mathbb{Z}$ if and only if there exists $k \in \mathbb{Z}$ such that $s' = s - k\frac{b}{d}$, $t' = t + k\frac{a}{d}$.

3.4. a). Let $x, y \in \mathbb{Q}_+^\times$ and $y = c/d$ be the canonical representation of y with $c, d \in \mathbb{N}^*$ and $\gcd(c, d) = 1$. Show that x^y is rational if and only if x is the d-th power of a rational number.

b). Show that other than $(2, 4)$ there is no pair (x, y) of positive *rational* numbers with $x < y$ and $x^y = y^x$. (**Hint :** Prove that for each *real* positive number of x with $1 < x < e$ there exists exactly one real number $y > x$ such that $x^y = y^x$. (observe that necessarily $y > e$.) For the proof of the above assertion : note that $x^y = y^x$ if and only if $(\ln x)/x = (\ln y)/y$ and consider the function $(\ln x)/x$ on $\mathbb{R}_+^\times$.)



c). Let $x \in \mathbb{Q}_+^\times$ and a be a positive natural number which is not of the form b^d with $b, d \in \mathbb{N}^*$, $d \geq 2$. Then show that $\log_a x$ is either integer or irrational.

d). For which $x, y \in \mathbb{Q}_+^\times$, $y \neq 1$, the real number $\log_y x$ rational? For which $x \in \mathbb{Q}_+^\times$, the real number $\log_{10} x$ rational?

e). Let $n \in \mathbb{N}^*$, $n \geq 2$ and $y \in \mathbb{Q}_+^\times \setminus \mathbb{N}^*$. Then both the numbers $\sqrt[n]{n!}$ and $(n!)^y$ are irrational. (**Hint :** The natural number $n!$ has simple prime factors.)

3.5. a). (Mersenne Numbers) Let $a, n \in \mathbb{N}$ with $a, n \geq 2$. If $a^n - 1$ is prime, then $a = 2$ and n is prime. (**Hint :** Use geometric series $a^n - 1 = (a-1)(a^{n-1} + a^{n-2} + \cdots + a + 1)$ to conclude that $a = 2$; if $n = rs$ with $r > 1, s > 1$, then $2^n - 1 = (2^r)^s - 1 = (2^r - 1)(1 + 2^r + 2^{2r} + \cdots + (2^r)^{s-1})$. — The natural numbers of the form $a^p - 1$, $p \in \mathbb{P}$ prime, are called Mersenne numbers. For $p = 2, 3, 5, 7$ the corresponding Mersenne numbers $3, 7, 31, 127$ are prime, but corresponding to $p = 11$, it is $M_{11} = 2^{11} - 1 = 2047 = 23 \cdot 89$ which is not prime. — **Remarks :** It was asserted by MERSENNE in 1644 that : *$M_p = 2^p - 1$ is prime for $2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, , 127$, and composite for the other remaining 44 values of $p \leq 257$.* For example, $47 \big| M_{23}$, $233 \big| M_{29}$, $223 \big| M_{37}$, $431 \big| M_{43}$ and $167 \big| M_{83}$. The first mistake was found in 1886 by PERUSIN and SEELHOFF that M_{61} is prime. Subsequently four further mistakes were found and it need no longer be taken seriously. In 1876 LUCAS found a method for testing whether M_p is prime and used it to prove that M_{127} is prime. This remained the largest known prime until 1951. The problem of Mersenne's numbers is connected with that of "perfect" numbers which are defined in the part c) below. Every two distinct Mersenne numbers are relatively prime. It is not known whether there are infinitely many Mersenne numbers that are prime. The biggest known[2]) prime is the Mersenne number M_p corresponding to $p = 25964951$; this prime number has $[\log_{10}(2^{25964951})] + 1 = [25964951 \cdot \log_{10} 2] + 1 = 7816230$ digits!)

b). (Fermat Numbers) Let $a, n \in \mathbb{N}^*$ with $a \geq 2$. If $a^n + 1$ is prime, then a is even and n is a power of 2. (**Hint :** If a is odd then $a^n + 1$ is even and if $n = 2^t \cdot m$ with $t, m \in \mathbb{N}$ and m odd, then (put $k := 2^t$) $2^n + 1 = 1 - (-2^k)^m = (1 + 2^k)(1 - 2^k + 2^{2k} - \cdots + 2^{(m-1)k})$ and if $m > 1$, then $k < n$ and hence $1 < 1 + 2^k < 1 + 2^n$. Therefore $m = 1$. — **Remarks :** The natural number of the form $2^{2^n} + 1$, $n \in \mathbb{N}$ is called the n-th Fermat number and is denoted by $F_n := 2^{2^n} + 1$, $n \in \mathbb{N}$. The Fermat numbers corresponding to $n = 0, 1, 2, 3, 4$ are $F_0 = 2, F_1 = 5, F_2 = 17, F_3 = 257, F_4 = 65537$ are prime (already discovered by Fermat himself) and hence conjectured that all were prime, but in 1732 EULER proved that : $F_5 = 2^{2^5} + 1 = 2^{32} + 1 = 641 \cdot 6700417$, since $641 = 5^4 + 2^4 = 5 \cdot 2^7 + 1$ divides $5^4 \cdot 2^{28} + 2^{32}$ and $5^4 \cdot 2^{28} - 1$ and hence the difference $2^{32} + 1 = F_5$. In 1880 LANDRY proved that $F_6 = 2^{2^6} + 1 = 274177 \cdot 67280412310721$. More recently it is proved that F_n is composite for $7 \leq n \leq 16$ $n = 18, 19, 23, 36, 38, 39, 55, 63, 73$ and many larger alues of n. MOREHEAD and WESTERN proved that F_7 and F_8 are composite without determining a factor. No factor is known for F_{13} or for F_{14}, but in all the other cases proved to be composite a factor is known. No prime F_n has been found beyond F_4, so that Fermat's conjecture has not proved a very happy one. It is perhaps more probable that the number of primes F_n is finite. is not prime. Fermat numbers are of great interest in many ways, for example, it was proved by GAUSS that : *if F_n is a prime p, then a regular polygon of p sides cane be inscribed in a circle by Euclidean methods.* The property of the Fermat numbers which is relevant here is : *No two Fermat numbers have a common divisor greater than* 1, i.e., $\gcd(F_n, F_m) = 1$, $n \neq m$. For, suppose that d divides both the Fermat numbers F_n and F_{n+k}, $k > 0$. Then putting $x = 2^{2^n}$, we have $\frac{F_{n+k}-2}{F_n} = \frac{2^{2^{n+k}}-1}{2^{2^n}+1} = \frac{x^{2^k}-1}{x+1} = x^{2^k-1} - x^{2^k-2} + \cdots - 1$ and so $F_n \big| F_{n+k} - 2$. This proves that $d \big| F_{n+k}$ and $d \big| F_{n+k} - 2$ and therefore $d \big| 2$. But F_n is odd and so $d = 1$. Therefore each of the Fermat numbers $F_1, F_2, \ldots, F_n$ is divisible by an odd prime number which does not divide any of the others and hence there are at least n odd primes not exceeding F_n. This proves (proof due to PÓLYA) Euclid's theorem (see T3.1.-3)-b)). Moreover, we have the inequality $p_n \leq F_n = 2^{2^n} + 1$ which is little stronger than the inequality in T3.1.-3)-d)-(1)-(i).)

c). (Perfect numbers) A natural number $n \in \mathbb{N}^*$ is called perfect if $\sigma(n) = 2n$. (Theorem of Euclid-Euler) *An even number $n \in \mathbb{N}^*$ is perfect if and only if n is of the form $2^s(2^{s+1} - 1)$ with $s \in \mathbb{N}^*$ and $2^{s+1} - 1$ prime.* (**Hint :** Suppose that n is perfect, $n = 2^s b$ $s, b \in \mathbb{N}^*$ and b odd. Then $2^{s+1} b = 2n = \sigma(n) = (2^{s+1} - 1)\sigma(b)$ and so there exists $c \in \mathbb{N}^*$ such that $\sigma(b = 2^{s+1} c$, $b = (2^{s+1} - 1)c$, $\sigma(b) = b + c$.)

[2]) On February 18, 2005, Dr. Martin Nowak, an eye surgeon from Germany, found the new largest known prime number, $2^{25964951} - 1$. This prime number has 7816230 digits! It took more than 50 days of calculations on Dr. Nowak's 2.4 GHz Pentium 4 computer. This discovery was part of the Great Internet Mersenne Prime Search (GIMPS) project in which more than 60000 volunteers from around the world took part. Such huge numbers are used in problems related to Cryptography.

3.6. Let $m, n \in \mathbb{N}^*$ be relatively prime numbers and let $a_0, a_1, \ldots$ be the sequence defined recursively as $a_0 = n$, $a_{i+1} = a_0 \cdots a_i + m$, $i \in \mathbb{N}$. Then $a_{i+1} = (a_i - m)a_i + m = a_i^2 - ma_i + m$ for all $i \geq 1$.

a). $\gcd(a_i, a_j) = 1$ for all $i, j \in \mathbb{N}$ with $i \neq j$. The prime divisors of a_i, $i \in \mathbb{N}$ supply infinitely many different prime numbers. (**Remark :** The a_i are suitable well for testing prime factorizing procedures.)

b). For all $i \in \mathbb{N}$, show that $\frac{1}{a_0} + \frac{m}{a_1} + \cdots + \frac{m^i}{a_i} = \frac{m+1}{n} - \frac{m^{i+1}}{a_{i+1} - m}$. Deduce that $\sum_{i=0}^{\infty} \frac{m^i}{a_i} = \frac{m+1}{n}$.

c). For $m = 2$ and $n = 1$, from b) prove that $a_{i+1} = F_i = 2^{2^i} + 1$, $i \in \mathbb{N}$. In particular, $\sum_{i=0}^{\infty} \frac{2^i}{F_i} = 1$.

3.7. Let M be a commutative monoid with cancellation law. Suppose that every element $x \in M$ is a product of irreducible elements. Show that the following statements are equivalent :

(i) M is factorial. (ii) Every irreducible element of M is prime. (iii) $\mathrm{lcm}(a, b)$ exists for every $a, b \in M$. (iv) $\gcd(a, b)$ exists for every $a, b \in M$. (**Hint :** Use T3.6.-8) and T3.6.-11).)

3.8. (The Sieve of Eratosthenes[3]) The so-called *sieve of Eratosthenes* is an alogrithm for singling out the prime from among the set of natural numbers $\leq N$ for arbitrary natural number N. It depends on the fact that if a natural number $n > 1$ has no divisior d with $1 < d \leq \sqrt{n}$, then n must be a prime number (See T3.1.-3)-d)-(5)). Let N be a positive natural number and let $\pi(N)$ denote the number of prime numbers $\leq N$. Let $p_1, \ldots, p_r$ be all prime numbers $\leq \sqrt{N}$, i.e, $r = \pi(\sqrt{N})$. Prove the following well-known formula[4]) :

$$\pi(N) = N + r - 1 - \sum_{1 \leq i \leq r} \left[\frac{N}{p_i}\right] + \sum_{1 \leq i_1 < i_2 \leq r} \left[\frac{N}{p_{i_1} p_{i_2}}\right] - \cdots + (-1)^r \left[\frac{N}{p_1 \cdots p_r}\right].$$

(**Proof :** For each $i = 1, \ldots, r$, let $M_i := \{n \in \mathbb{N}^* \mid n \leq N \text{ and } p_i | n\} = \{p_i, 2p_i, \ldots, \left[\frac{N}{p_i}\right] \cdot p_i\}$ and hence $|M_i| = \left[\frac{N}{p_i}\right]$. For an index ν-tuple $(i_1, \ldots, i_\nu)$ with $1 \leq i_1 < i_2 < \cdots < i_\nu \leq r$, we have $M_{i_1} \cap \cdots \cap M_{i_\nu} = \{n \in \mathbb{N}^* \mid n \leq N \text{ and } p_{i1} | n, \ldots, p_{i_n u} | n \text{ equivalently } p_{i_1} \cdots p_{i_\nu} | n\}$ and so $|M_{i_1} \cap \cdots \cap M_{i_\nu}| = \left[\frac{N}{p_{i_1} \cdots p_{i_\nu}}\right]$. This proves that $\pi(N) = N - 1 - |\cup_{i=1}^r M_i| + r$. Now use the Sylvester's sieve formula.)

3.9. Let $n \in \mathbb{N}^*$ and let p be a prime number. Show that

a). The multiplicity of p in $n!$ is $v_p(n!) = \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \left[\frac{n}{p^3}\right] + \cdots$.

In particular, (Legendre's formula : $n! = \prod_{p \leq n} p^{\sum_{r \geq 1} [n/p^r]}$.

(**Proof :** Note that $\left[\frac{n}{p^r}\right] = 0$ if $p^r > n$ and hence the sum on the right hand side is really a finite sum. The assertion is proved by induction. It is trivial for $1!$. Assume $n > 1$ and the asertion is true for $(n-1)!$ and let $j = v_p(n)$, i.e., $p^j | n$ but $p^{j+1} \nmid n$. Since $n! = n \cdot (n-1)!$, it is enough to prove that $\sum[n/p^i] - \sum[(n-1)/p^i] = j$.

---

[3]) This process is named after the Greek scientist who invented it. ERATOSTHENES CYRENE (276-194 BC), a contemporary of ARCHIMEDES, was a many-sided scholar; nicknamed "Beta" because he stood at least second in every field. He gave a mechanical solution of the problem of duplicating the cube, and he calculated the diameter of the earth with considerable accuracy. Chief librarian of the Museum in Alexandria, he became blind in his old age and committed suicide by starvation.

[4]) Proved by the French mathematician LEGENDRE ADRIEN-MARIE (1752-1833). It was Legendre's fate to be eclipsed repeatedly by younger mathematicians. He invented the *method of least squares* in 1806, but GAUSS revealed in 1809 that he had done the same in 1795. He laboured for 40 years on *elliptic integrals* and then ABEL and JACOBI revolutionized the subject in the 1820s with the introduction of *elliptic functions*. He conjectured the *prime number theorem* and the *law of quadratic reciprocity*, but could not prove either. Still, he created much beautiful mathematics, including the determination of the number of representations of an integer as a *sum of two squares*, and the exact conditions under which the equation $ax^2 + by^2 + cz^2 = 0$ holds for some $(x, y, z) \neq (0, 0, 0)$. He also wrote an elementary geometry text in which, in 39 editions of the English translations, replaced Euclid's *Elements* in America schools.

But $\big[n/p^i\big] = \big[(n-1)/p^i\big] = \begin{cases} 1, & \text{if } p^i \big| n\,, \\ 0, & \text{if } p^i \big| n\,, \end{cases}$ and hence $\sum \big[n/p^i\big] = \sum \big[(n-1)/p^i\big] = j$. This proof is rather short and artificial. Another proof: First note that $\left[\frac{n}{p^{r+1}}\right] = \left[\frac{\left[\frac{n}{p^r}\right]}{p}\right]$ for every $r \in \mathbb{N}$ (this follows easily from $[x/m] = [\,[x]/m]$ for all $x \in \mathbb{R}$ and all $m \in \mathbb{N}^*$.) Among the natural numbers $1 < K < n$, those which are divisible by p are $p\,, 2p\,, \ldots\,, \left[\frac{n}{p}\right] \cdot p$; among these that are divisible by p^2 are $p^2\,, 2p^2\,, \ldots\,, \left[\frac{n}{p^2}\right] \cdot p^2$; among these that are divisible by p^3 are $p^3\,, 2p^3\,, \ldots\,, \left[\frac{n}{p^3}\right] \cdot p^3$ and so on. This lead us to conclude that $\sum_{r\geq 1} [n/p^r] = \sum_{K=1}^{n} v_p(K) = v_p(1 \cdot 2 \cdot \cdots \cdot n) = v_p(n!)$. — More generally: If n_i, $i \in I$, is a finite family of positive natural numbers, then the prime number p occurs in the product $\prod_{i\in I} n_i$ with the multiplicity $\sum_{k\in\mathbb{N}^*} \nu_k$, where for each $k \in \mathbb{N}^*$, ν_k is the number $i \in I$ for which n_i is divisible by p^k.

b). Show that $(2n)!/(n!)^2$ is an even integer. Further, $v_p((2n)!/(n!)^2) = \sum_{k\geq 1} \big([2n/p^k] - 2[n/p^k]\big)$ and if $n < p < 2n$, then $v_p((2n)!/(n!)^2) = 1$.

c). Let $n = (r_t, \ldots, r_0)_p$ be the p-adic expansion of n, where $0 \leq r_i < p$ for all $i = 0, \ldots, t$. Then $v_p(n!) = \big(n - \sum_{i\geq 0} r_i\big)\big/(p-1)$. (**Hint:** The sum on the right hand side of part a) can be easily computed by recursion: $\sum_{i\geq 1}[n/p^i] = \big(n - \sum_{i\geq 0} r_i\big)\big/(p-1)$.)

d). $v_p((p^k - 1)!) = [p^k - (p-1)k - 1]/(p-1)$. (**Hint:** Use the identity $(p^k - 1) = (p-1)(p^{k-1} + \cdots + p^2 + p + 1)$.)

e). Find $v_3(80!)$ and $v_7(2400!)$.

f). Find $n \in \mathbb{N}^*$ such that $v_p(n!) = 100$. (**Hint:** For instance for $p = 5$, begin by considering the equation $(n-1)/4 = 100$.)

Next pages one can see Class-Notes and (simple) test-exercises.

Class-Notes/Test-Exercises

T3.1. (Division algorithm/Divisibility/Prime numbers)

1). Let $a, b \in \mathbb{Z}$ with $b \geq 1$. Then there exists unique integers q and r such that $a = qb + r$ with $0 \leq r < b$. Moreover, in the case $a \geq 0$, we have $q \geq 0$. — The integers q and r are called quotient and remainder, respectively, in the division of a by b. (Existence of q and r : The subset $A := \{x \in \mathbb{N} \mid x = a - zb \text{ with } z \in \mathbb{Z}\} \subseteq \mathbb{N}$ is non-empty: if $a \geq 0$, then $a \in A$: if $a < 0$, then $a - ab = a(1-b) \geq 0$ and hence $a - ab \in A$. Therefore by the minimality principle A has a minimal element r. Then $r = a - qb \geq 0$ for some $q \in \mathbb{Z}$. Further, $r < b$; otherwise $a - (q+1)b = r - b \geq 0$ and hence $r - b \in A$ a contradiction to the minimality of r. Therefore $a = qb + r$ is the required equation. If $a \geq 0$, then $q \geq 0$; otherwise $q \leq -1$, i. e., $-q \geq 1$ and $r = a - qb \geq b$ a contradiction. Uniqueness of q and r : If $a = qb + r = q'b + r'$ with $q, q', q, r' \in \mathbb{Z}$ with $0 \leq r, r' < b$. Then $r - r' = (q' - q)b$ and so $b \mid (r - r')$. But since $0 \leq r, r' \leq b$ we have $-b \leq r - r' \leq b$ and hence $r - r' = 0$, i.e., $r' = r$. Now from $(q' - q)b = 0$ and $b \neq 0$, it follows that $q' = q$.)

2). (Divisibility) An integer d is called a divisor of $a \in \mathbb{Z}$ in $\mathbb{Z}$, and is denoted by $d \mid a$, if there exists $v \in \mathbb{Z}$ such that $a = dv$. In this case we also say that d divides a or a is a multiple of d (in $\mathbb{Z}$). If d is not a divisor of a, then we write $d \nmid a$. If $0 \neq d$ is a divisor of a, then $v \in \mathbb{Z}$ in the equation $a = dv$ is uniquely determined by the cancellation law. An integer $a, \in \mathbb{Z}$ is called even (respectively odd) if $2 \mid a$ (respectively, $2 \nmid a$), i. e., a is of the form $2v$ (respectively, $2v + 1$).

a). The *divisibility* defines a relation on Z and it satisfies the following basic rules: For all $a, b, c, d \in \mathbb{Z}$, we have: (i) (Reflexivity) $a \mid a$. (ii) (Transitivity) If $a \mid b$ and $b \mid c$, then $a \mid c$. (iii) If $a \mid b$ and $c \mid d$, then $ac \mid bd$. (iv) If $a \mid b$ and $a \mid c$, then $a \mid (xb + yc)$ for all $x, y \in \mathbb{Z}$. (**Remarks:** The rule (iii) does not hold if one replaces ac (respectively, bd) by $a + c$ (respectively, $b + d$). The number 0 is divisible by every integer $d \in \mathbb{Z}$, since $0 = d \cdot 0$; this is the only case of an integer which has infinitely many distinct divisors. This is proved in the part b) below which is an important connection between divisibility relation $\mid$ and the (standard) order.)

b). Let $a \in \mathbb{Z}$, $a \neq 0$ and let $d \in \mathbb{Z}$ be a divsor of a. Then: $1 \leq |d| \leq |a|$. In particular, every non- zero integer a has at most finitely many divisors.

c). Let $a, d \in \mathbb{Z}$, $a > 0$, $d > 0$. If $d \mid a$ and $a \mid d$ then $d = a$.

(**Remarks:** Every integer a has the four (distinct) divisors $a, -a, 1, -1$; these are called the trivial divisors of a; other divisors are called proper divisors of a. Therefore from b) it follows that: *If d is a proper divisor of $a \neq 0$, then $1 < |d| < |a|$.* Since $a = dv$ if and only if $-a = d(-v)$, the integers a and $-a$ havs the same divisors. Therefore, since for every integer a, exactly one of a or $-a$ is a natural number, for the divisibility questions, we may without loss of generality assume that $a \in \mathbb{N}$. Further, if d is a divisor of a, then $-d$ is also divisor of a (since if $a = dv$ with $v \in \mathbb{Z}$, then $a = (-d)(-v)$) Therefore if one knows *all divisors of an integer a* are known if one knows *all positive divisors of $|a|$*. On this basis many considerations in number theory can be reduced to the set N^* of positive integers.)

3). (Prime numbers) A natural number p is called a prime number or an irreducible (in $\mathbb{N}$) if $p > 1$ and $p = ab$ with $a, b \in \mathbb{N}$, then either $a = 1$ or $b = 1$. A natural number $n > 1$ is called composite if it is not a prime number. The set of all prime numbers is denoted by $\mathbb{P}$. Then by definition $1 \notin \mathbb{P}$. For a natural number $p > 1$, the following statements are equivalent: (i) $p \in \mathbb{P}$. (ii) 1 and p are the only positive divisors of p. (iii) p has no proper divisor. (**Remark:** On the basis of the property (iii) prime numbers are also called *irreducible*.)

a). (Existence Theorem) Every natural number $a > 1$ has a smallest (positive) divisor $t > 1$. Moreover, this divisor t is a prime number. (**Proof:** The set $T = \{d \in \mathbb{N}^* \mid d \mid a \text{ and } d > 1\}$ is non-empty, since $a \in T$. Therefore by the minimality principle T has a minimal element t. This integer t is a prime number. For, if not, then there is a divisor t' of t with $1 < t' < t$. But then $t' \mid t$ and $t \mid a$ and hnce $t' \mid a$ a contradiction to the minimality of t in T.)

b). (Euclid's Theorem [5]) There are infinitely many prime numbers, i. e., the set $\mathbb{P}$ is infinite. (**Proof:** In the text of Euclid the word "infinite" is not mentioned; this theorem was formulated as: *Given any finite set of prime numbers, one can always find a prime number which does not belong to the given set.* Show that: *Let $q_1, \ldots, q_n$ be finite set of prime numbers. Then the smallest (positive) divisor $t > 1$ of the natural number $a := q_1 \cdot q_2 \cdots q_n + 1$ is a prime number which is different from all the prime numbers $q_1, \ldots, q_n$.* — Since

[5]) Proved in the "Elements (Book IX, Theorem 20)" of Euclid. Euclid's argument is universally regarded as a model of mathematical elegance.

$a > 1$, t exists and hence t is a prime number by the Exitence theorem in part a). If t is one of the numbers $q_1, \ldots, q_n$, then $t \mid q_1 \cdot q_2 \cdots q_n$. Then $t \mid a - q_1 \cdot q_2 \cdots q_n = 1$ a contradiction.)

c). (Irreducibility and Prime property) Let p be a natural number. Then: (1) (Euclid's Lemma) *If a prime number p divides a product ab of two natural numbers a and b, then p divides one of the factor a or b.* (**Proof:** The set $A := \{x \in \mathbb{N}^* \mid p \mid ax\}$ contains p and b and hence by the minimality principle it has a smallest element c. We claim that $c \mid y$ for every $y \in A$. For, by division algorithm $y = qc + r$ with $q, r \in \mathbb{N}$ and $0 \leq r < c$. Then, since $p \mid ay$ and $p \mid ac$, $p \mid ay - q(ac) = ar$. This proves that $r = 0$; otherwise $r \in A$ and $r < c$ a contradiction to the minimality of c in A. Theorefore $c \mid y$ for every $y \in A$; in particular, $c \mid p$ and hence $c = 1$ or $c = p$. If $c = 1$, then $p \mid ac = a$. If $c = p$, then (since $b \in A$) by the above claim $p \mid b$.)

(2) *If a prime number p divides a product $a_1 \cdots a_n$ of n positive natural numbers $a_1, \ldots, a_n$, then p divides one of the factor a_i for some $1 \leq i \leq n$.* (**Hint:** Prove by induction on n using (1) above.)

(3) For a natual number the following statements are equivalent: (i) p is a prime number. (ii) If p divides a product ab of two integers a and b, then $p \mid a$ or $p \mid b$. (**Proof:** We may assume that a and b are both positive. The implication (i)⇒(ii) is proved in (1). For the implication (ii)⇒(i) Let d be any positive divisor of p, i.e., $p = dd'$ with $d' \in \mathbb{N}$. This means that $p \mid dd'$ and hence by (ii) either $p \mid d$ or $p \mid d'$. But since $1 \leq d \leq p$ and $1 \leq d' \leq p$ it follows that either $p = d$ or $p = d'$, i.e., either $d = p$ or $d = 1$. This proves that the only positive divisors of p are 1 and p and hence p is a prime numebr. — **Remark:** The property (ii) is (usually distinguished from the irreducibility property of p) called the prime property. Therefore we can reformulate (3) as: *A natural number $p > 1$ is irreducible if and only if p has the prime property.* See also ???.)

d). Let $\mathbb{P}$ denote the set of all prime numbers.

(1). Let p_n denote the n-th prime (in the natural order $\leq$). Then show that: (i) $p_n \leq 2^{2^{n-1}}$. (**Hint:** Note that $p_{n+1} \leq p_1 \cdot p_2 \cdots p_n + 1$.) (ii) $p_n > 2n - 1$ for $n \geq 5$. (iii) none of the natural number $P_n := p_1 \cdot p_2 \cdots p_n + 1$ is a perfect square. (**Hint:** Each P_n is of the form $4m + 3$.) (iv) the sum $\frac{1}{p_1} + \frac{1}{p_2} + \cdots + \frac{1}{p_n}$ is never an integer. (v) Give another proof of infiniteness of $\mathbb{P}$ by assuming that there are only finitely many primes, say, $p_1, \ldots, p_n$ and using the natural number $N = p_2 \cdot p_3 \cdots p_n + p_1 \cdot p_3 \cdots p_n + \cdots + p_2 \cdot p_3 \cdots p_{n-1}$.

(vi) (Conjectures/Open questions) (a) *If q_n is the smallest prime which is $> P_n = p_1 \cdot p_2 \cdots p_n + 1$, then the difference $(p_1 \cdot p_2 \cdots p_n) - q_n$ is always a prime.* Verify this for first 5 values of n. (b) Let $d_n = p_{n+1} - p_n$. An open question is: *whether the equation $d_n = d_{n+1}$ has infinitely many solutions.* Give 5 solutions.

(2). Let $n \in \mathbb{N}^*$. Show that (i) if $n > 2$, then there exists a prime number p with $n < p < n!$. (**Hint:** Consider a prime divisor p of $n! - 1$.) (ii) if $n > 1$, then every prime divisor of $n! + 1$ is an odd integer $> n$. (**Remark:** This shows again that there are infinitely many prime numbers. It is unknown whether infinitely many of $n! + 1$ are prime.)

(3). For $n \in \mathbb{N}^*$, none of the n natural numbers $(n+1)! + 2, \ldots, (n+1)! + n + 1$ are prime. (**Remark:** Therefore there are gaps of any size between prime numbers.)

(4). For $a = 3, 4, 6$, show that in the sequence $an + (a - 1)$, $n \in \mathbb{N}$, there are infinitely many prime numbers. (**Hint:** Make an argument with $ap_1 \cdots p_r + (a - 1)$.) (**Remark:** More generally, if a, b are relatively prime positive natural numbers, then there are infinitely many prime numbers of the form $an + b$, $n \in \mathbb{N}$ (Dirichlet's Theorem).)

(5). Let $n, r \in \mathbb{N}^*$, $n \geq 2$. If n has no prime divisor $\leq \sqrt[r+1]{n}$, then n is a product of at the most r (not necessarily different) prime numbers. In particular, if n has no prime divisor $\leq \sqrt{n}$, then n is prime.

(6). For $n \in \mathbb{N}$, $n \geq 2$, the natural number $4^n + n^4$ is never prime. (**Hint:** For odd n, we have $n^4 + 4^n = (n^2 - 2^{\frac{n+1}{2}} \cdot n + 2^n)(n^2 + 2^{\frac{n+1}{2}} \cdot n + 2^n)$.)

T3.2. (GCD and LCM/Euclidean algorithm)

1). (GCD) For an integer $a \in \mathbb{Z}$, let $\mathrm{D}(a)$ denote the set of all positive divisors of a. Then 1 and $a \in \mathrm{D}(a)$; $\mathrm{D}(a) = \mathbb{N} \Longleftrightarrow a = 0$; if $a \neq 0$, then $\mathrm{D}(a)$ is a finite subset of $\mathbb{N}$. For $a, b \in \mathbb{Z}$, the intersection $\mathrm{D}(a) \cap \mathrm{D}(b)$ is precisely the set of all common divisors of a and b. Moreover, if $(a, b) \neq (0, 0)$, then $\mathrm{D}(a) \cap \mathrm{D}(b)$ is a finite subset of $\mathbb{N}$ and hence it has a largest element, this element is called the greatest common divisor of a and b and is denoted by $\gcd(a, b)$. Therefore for $a, b \in \mathbb{Z}$ with $(a, b) \neq (0, 0)$, the $\gcd(a, b)$ is the positive integer d satisfying: (i) $d \mid a$ and $d \mid b$; (ii) if c is a positive integer with $c \mid a$ and $c \mid b$, then $c \leq d$. We put $\gcd(0, 0) := 0$. Two integers $a, b \in \mathbb{Z}$ with $(a, b) \neq (0, 0)$ are said to be relatively prime if $\gcd(a, b) = 1$.

a). (Bezout's Lemma) For integers $a, b \in \mathbb{Z}$ with $(a, b) \neq (0, 0)$ there exists integers $s, t \in \mathbb{Z}$ such that $\gcd(a, b) = sa + tb$. Deduce that: (i) For two non-zero integers $a, b \in \mathbb{Z}^*$ with $(a, b) \neq (0, 0)$, show

that the set $\{sa + tb \mid s, t \in \mathbb{Z}\}$ is precisely the set of all multiples of $d = \gcd(a, b)$. (ii) if $d = \gcd(a, b)$, then $\gcd(a/d, b/d) = 1$, i.e., a/d and b/d are relatively prime. (iii) if $a, b, c \in \mathbb{Z}$ and $a|c$ and $b|c$ with $\gcd(a, b) = 1$, then $ab|c$. (iv) if $a, b, c \in \mathbb{Z}$ and $a|bc$ and $\gcd(a, b) = 1$, then $a|c$. (v) (Euclid's lemma) Let p be an irreducible element in $\mathbb{N}^*$ (i.e. 1 and p are the only divisors of p in $\mathbb{N}$). If p divides a product $a_1 \cdots a_n$ of positive natural numbers, then p divides at least one of the factor a_i for some $1 \le i \le n$.
(vi) For integers $a, b \in \mathbb{Z}$ with $(a, b) \neq (0, 0)$, a positive integer d is a gcd of a and b if and only if (i) $d|a$ and $d|b$ and (ii) whenever a positive integer c divides both a and b, then $c|d$. (**Remark:** The assertion (vi) often serves as a definition of $\gcd(a, b)$. The advantage is the order relationship is not involved.)

(vii) $\mathrm{D}(a) \cap \mathrm{D}(b) = \mathrm{D}(\gcd(a, b))$. (viii) For integers $a, b \in \mathbb{Z}$ with $b \neq 0$ and $a = qb + r$, $q, r \in \mathbb{Z}$, show that $\gcd(a, b) = \gcd(b, r)$.

b). (Rules for GCD) For integers $a, b, c \in \mathbb{Z}$, we have:

(i) $\gcd(a, a) = |a|$; (ii) $a|b \iff a = \gcd(a, b)$.

(iii) (Commutativity) $\gcd(a, b) = \gcd(b, a)$. (iv) (Associativity) $\gcd(\gcd(a, b), c) = \gcd(a, \gcd(b, c))$.

(iv) (Distributivity) $\gcd(ca, cb) = |c| \gcd(a, b)$. (v) (Product formula) $\gcd(ab, c) = \gcd(\gcd(a, c) \cdot b, c)$.
(**Remark:** These rules are elementary to prove, but gives unwieldy impression; probably because of the unaccountability of the classical notation gcd. If instead of gcd one uses an elegante symbol, for example, $a \sqcap b := \gcd(a, b)$, then these rules are more suggesstive: (i) $a \sqcap a = |a|$; (ii) $a|b \iff a = a \sqcap b$; (iii) (Commutativity) $a \sqcap b = b \sqcap a$; (iv) (Associativity) $(a \sqcap b) \sqcap c = a \sqcap (b \sqcap c)$; (iv) (Distributivity) $(c \cdot a) \sqcap (c \cdot b) = |c| \cdot (a \sqcap b)$; (v) (Product formula) $(a \cdot b) \sqcap c = ((a \sqcap c) \cdot b) \sqcap c$; and the use of the terms "associativity" and "distributivity" is immediately clear. This example shows the importance of the good notation; unfortunately in literature till today everybody use the tradational noatation $\gcd(a, b)$.)

c). For positive natural numbers $a, b, c, d, m, n \in \mathbb{N}^*$, show that: (i) $\gcd(a, 1) = 1$.

(ii) $\gcd(a, a + n)|n$ and hence $\gcd(a, a + 1) = 1$.

(iii) If $\gcd(a, b) = 1$ and $\gcd(a, c) = 1$, then $\gcd(a, bc) = 1$. (**Hint:** $1 = sa + tb = ua + vc$ for some $s, t, u, v \in \mathbb{Z}$. Then $1 = (sa + tb)(ua + vc) = (aus + cvs + btu)a + (tv)bc$.)

(iv) If $\gcd(a, b) = 1$, then $\gcd(a^m, b^n) = 1$ (**Hint:** Use the above part (iii).)

(v) The relation $a^n|b^n$ implies that $a|b$. (**Hint:** Let $d := \gcd(a, b)$ and write $a = rd$ and $b = sd$. Then $\gcd(r, s) = 1$ and hence $\gcd(r^n, s^n) = 1$ by (ii). Now show that $r = 1$, whence $a = d$, i.e, $a|b$.)

(vi) If $\gcd(a, b) = 1$ and $c|a$, then $\gcd(b, c) = 1$.

(vii) If $\gcd(a, b) = 1$, then $\gcd(ac, b) = \gcd(c, b)$.

(viii) If $\gcd(a, b) = 1$ and $c|(a + b)$, then $\gcd(a, c) = \gcd(b, c)$. (**Hint:** Let $d = \gcd(a, c)$. Then $d|a$ and $d|c|(a + b)$ and hence $d|(a + b) - a = b$.)

(ix) If $\gcd(a, b) = 1$, then $\gcd(a + b, ab) = 1$.

(x) If $\gcd(a, b) = 1$, $d|ac$ and $d|bc$, then $d|c$.

(xi) If $d|n$, then $2^d - 1|2^n - 1$.

(xii) Show that there are no positive natural numbers $a, b \in \mathbb{N}^*$ and $n \in \mathbb{N}$ with $n > 1$ and $a^n - b^n$ divides $a^n + b^n$. (**Hint:** We may assume that $b < a$ and $\gcd(a, b) = 1$.)

(xiii) Show that for $a, b \in \mathbb{N}^*$, $b > 2$, $2^a + 1$ is not divisible by $2^b - 1$ (**Hint:** Prove that $a > b$.)

(xiv) For $m, n \in \mathbb{N}$ with $m > n$, show that $a^{2^n} + 1$ divides $a^{2^m} - 1$. Moreover, if $m, n, a \in \mathbb{N}^*$, $m \neq n$, then $\gcd(a^{2^m} + 1, a^{2^n} + 1) = \begin{cases} 1, & \text{if } a \text{ is even,} \\ 2, & \text{if } a \text{ is odd.} \end{cases}$ (**Hint:** $a^{2^n} + 1|a^{2^{n+1}} - 1$. For the second part use the first part.)

(xv) Suppose that $2^n + 1 = xy$, where $x, y \in \mathbb{N}^*$, $x > 1$, $y > 1$ and $n \in \mathbb{N}^*$. Show that 2^a divides $x - 1$ if and only if 2^a divides $y - 1$. (**Hint:** Write $x - 1 = 2^a \cdot b$ and $y - 1 = 2^c \cdot d$ with b and d odd.)

(xvi) Show that $\gcd(n! + 1, (n + 1)! + 1) = 1$.

2). (LCM) The concept parallel to that of a gcd is the concept of the *least common multiple*. For an integer $a \in \mathbb{Z}$, let $\mathrm{M}(a) = \mathbb{Z}a = \{na \mid n \in \mathbb{Z}\}$ denote the set of all multiples of a. Then $\mathrm{M}(a) = \{0\} \iff a = 0$; if $a \neq 0$, then $\mathrm{M}(a) = \mathbb{N} \cdot a \uplus \mathbb{Z}^- \cdot a$. Further, for $a, b \in \mathbb{Z}^*$, the intersection $\mathrm{M}(a) \cap \mathrm{M}(b)$ is precisely the set of all common multiples of a and b. Moreover, $ab \in \mathrm{M}(a) \cap \mathrm{M}(b)$, in particular, $|ab| \in \mathbb{N} \cdot a \cap \mathbb{N} \cdot b$ and hence by minimality principle, it has a minimal element, this element is called the least common multiple of a and b and is denoted by $\mathrm{lcm}(a, b)$. Therefore for $a, b \in \mathbb{Z}^*$, the $\mathrm{lcm}(a, b)$ is the positive integer m satisfying: (i) $a|m$ and $b|m$; (ii) if c is a positive integer with $a|c$ and $b|c$, then $m \le c$. We put $\mathrm{lcm}(0, 0) := 0$. It is clear that for any two non-zero integers $a, b \in \mathbb{Z}$, $\mathrm{lcm}(a, b)$ always exists and $\mathrm{lcm}(a, b) \le |ab|$.

a). Let $a, b \in \mathbb{Z}^*$. Then $\gcd(a,b)$ divides $\operatorname{lcm}(a,b)$ and $\gcd(a,b)\cdot\operatorname{lcm}(a,b) = ab$. Moreover, (i) $\gcd(a,b) = \operatorname{lcm}(a,b)$ if and only if $a = b$. (ii) $\gcd(a,b) = 1$ if and only if $\operatorname{lcm}(a,b) = ab$.

b). For $a, b, c \in \mathbb{Z}^*$, show that the following statements are equivalent: (i) $a \mid b$. (ii) $\gcd(a,b) = a$. (iii) $\operatorname{lcm}(a,b) = b$.

c). For $a, b, c \in \mathbb{Z}$, show that $\operatorname{lcm}(ca, cb) = |c|\operatorname{lcm}(a,b)$.

d). For non-zero integers $a, b \in \mathbb{Z}$, a positive integer m is a lcm of a and b if and only if (i) $a \mid m$ and $b \mid m$ and (ii) whenever a positive integer c is a multiple of both a and b, then $m \mid c$. (**Hint:** Put $v = \operatorname{lcm}(a,b)$ and use division algorithm to write $m = qt + r$ with $q, r \in \mathbb{Z}$, $0 \le r < t$. Then r is common multiple of a and b. — **Remark:** This assertion often serves as a definition of $\operatorname{lcm}(a,b)$. The advantage is the order relationship is not involved.)

e). For integers $a, b \in \mathbb{Z}$, show that $\mathrm{M}(a) \cap \mathrm{M}(b) = \mathrm{M}(\operatorname{lcm}(a,b))$.

3). (Euclidean algorithm[6]) Let $a, b \in \mathbb{N}^*$ with $a \ge b$. We put $r_0 := a$ and $r_1 := b$ and consider the system of equations obtained by the repeated use of division algorithm: $r_0 = q_1 r_1 + r_2, 0 < r_2 < r_1$; $r_1 = q_2 r_2 + r_3, 0 < r_3 < r_2$; $\cdots$ $r_{k-1} = q_k r_k + r_{k+1}, 0 < r_{k+1} < r_k$; $r_k = q_{k+1} r_{k+1}$. Then:

(i) $\gcd(a,b) = r_{k+1}$. (**Hint:** By repeated use of 1)-vii) we have $\gcd(a,b) = \gcd(r_0, r_1) = \gcd(r_1, r_2) = \cdots = \gcd(r_k, r_{k+1}) = \gcd(r_{k+1}, 0) = r_{k+1}$.)

(ii) For $i = 0, \ldots, k+1$, define s_i and t_i recursively by: $s_0 = 1$, $t_0 = 0$; $s_1 = 0$, $t_1 = 1$; $s_{i+1} = s_{i-1} - q_i s_i$, $t_{i+1} = t_{i-1} - q_i t_i$, $i = 1, \ldots, k$. Then $a = r_0 = s_0 a + t_0 b$, $r_1 = s_1 a + t_1 b$ and $r_{i+1} = r_{i-1} - q_i r_i = s_{i-1}a + t_{i-1}b - q_i s_i a - q_i t_i b = s_{i+1}a + t_{i+1}b$ for all $i = 1, \ldots, k$. (**Remark:** This proves once again Bezout's Lemma.)

4). The notion of greatest common divisor can be extended to more than two integers in an obvious way. Let $a_1, \ldots, a_n \in \mathbb{N}$, $n \ge 1$, not all zero. Then $\gcd(a_1, \ldots, a_n)$ is defined to be the positive integer d satisfying the following two properties: (i) $d \mid a_i$ for every $i = 1, \ldots, n$; (ii) if c is a positive integer with $c \mid a_i$ for every $i = 1, \ldots, n$, then $c \le d$. Note that $\gcd(a_1, \ldots, a_{n-1}, a_n) = \gcd(\gcd(a_1, \ldots, a_{n-1}), a_n) = \cdots = \gcd(a_1, \gcd(a_2, \ldots, a_n))$ by T3.2-1)-b) and hence the gcd depends only on $a_1, \ldots, a_n$ and not on the order in which they are written.

a). Let $a_1, \ldots, a_n \in \mathbb{N}^*$, $n \ge 1$ and let $a = a_1 \cdots a_n$. Show that the following statements are equivalent:

(i) $a_1, \ldots, a_n$ are pairwise relatively prime. (ii) If each of the numbers $a_1, \ldots, a_n$ divide the natural number c, then a also divide the number c. (iii) $\operatorname{lcm}(a_1, \ldots, a_n) = a$. (iv) The natural numbers $b_1 := a/a_1, \ldots, b_n := a/a_n$ are relatively prime. (v) There exist integers $s_1, \ldots, s_n$ such that $\frac{1}{a} = \frac{s_1}{a_1} + \cdots + \frac{s_n}{a_n}$. (**Remark:** lcm and gcd of finite many numbers $a_1, \ldots, a_n$ are defined like in the case $n = 2$. If $\gcd(a_1, \ldots, a_n) = 1$, then $a_1, \ldots, a_n$ are called relatively prime. Note that this concept is different from that of pairwise relatively prime.)

b). For $a_1, \ldots, a_n \in \mathbb{N}^*$, $n \ge 1$, show that there exist integers $u_1, \ldots, u_n \in \mathbb{Z}$ such that $\gcd(a_1, \ldots, a_n) = u_1 a_1 + \cdots + u_n a_n$. In particular, $a_1, \ldots, a_n$ are relatively prime if and only if there exist integers $u_1, \ldots, u_n$ such that $1 = u_1 a_1 + \cdots + u_n a_n$. (**Remark:** One can find the coefficients $u_1, \ldots, u_n$ algorithmically by succesive use of the lemma of Bezout (see T3.2-1)-a)). This algorithm supplies frequently disproportionately large coefficients $u_1, \ldots, u_n$. It is better to proceed as follows: First by renumbering assume that a_1 is minimal in $\{a-1, \ldots, a_n\}$, and goes then to tuple $(a_1, r_2, \ldots, r_n)$, where r_j the remainder of a_j after dividing by a_1, after removing the zeros among r_j, consider the new tuple as at the beginning. One has to control, how the coefficients of the tuple constructed are represented as linear combinations of the $a_1, \ldots, a_n$, beginning with $a_i = \sum_{k=1}^{n} \delta_{ik} a_k$.) Find integers u_1, u_2, u_3 such that $1 = u_1 \cdot 88 + u_2 \cdot 152 + u_3 \cdot 209$.

T3.3. (Fundamental Theorem of Arithmetic) Proposition 14 of Book IX of Euclid's "Elements" embodies the result which later became known as the *Fundamental Theorem of Arithmetic*:

1). Every Natural number $a > 1$ is a product of prime numbers and this representation is "essentially" unique, apart from the order in which the prime factors occur.

---

[6]) A more efficient method involving repeated application of division algorithm is given in the VII-th book of the *Elements* and it is referred to as the Euclidean algorithm. The French mathematician GABRIEL LAMÉ (1795-1870) proved that the number of steps required to find gcd in the Euclidean algorithm is at most five times the number of the digits in the smaller integer, i.e., $5\log_{10} b = (2.17\ldots)\log b$. Lamé was a primarily a mathematical physicist. is only other known contributions to number theory were the first proof of *Fermat's Last Theorem* for the exponent 7 and a fallacious "proof" for the general n.

a). (Existence of prime decomposition) *Every natural number $a > 1$ has a prime decomposition $a = p_1 \cdots p_n$, where we may choose p_1 as the smallest (prime) divisor t of a.* (**Proof:** Either a is prime or composite.; in the former case there is nothing to prove. If a is composite, then by T3.1-3)-a) there exists a smallest prime divisor p_1 of a, i.e., $a = p_1 \cdot b$ with $1 \leq b < a$ (since $1 < p_1 \leq a$). Now, by induction hypothesis b has a prime decomposition $b = P_2 \cdots p_n$ and hence a has a prime decomposition $a = p_1 \cdot p_2 \cdots p_n$.)

b). (Uniqueness of prime decomposition) *A prime decomposition of every natural number $a > 1$ is essentially unique. More precisely, if $a = p_1 \cdots p_n$ and $a = q_1 \cdots q_m$ are two prime decompositions of a with prime numbers $p_1, \ldots, p_n$; $q_1, \ldots, q_m$, then $m = n$ and there exists a permutation $\sigma \in \mathfrak{S}_n$ such that $q_i = p_{\sigma(i)}$ for every $i = 1, \ldots, n$.* (**Proof:** We prove the assertion by induction on n. If $n = 1$, then $p_1 = a = q_1 \cdots q_m$, i.e., $p_1 \big| q_1 \cdots q_m$ and hence by the prime property T3.1-3)-c)-(2) $p_1 \big| q_j$ for some j, $1 \leq j \leq m$. Renumering if necessary, we may assume that $j = 1$; further, since q_1 is a prime number, we must have $p_1 = q_1$ by the irreducibility of q_1. Now, by cancelling p_1, we get two prime decompositions of the number $a' = p_2 \cdots p_n = q_2 \cdots q_m$. Therefore by induction hypothesis $m - 1 = n - 1$ and there exists a permutation $\sigma' \in \mathfrak{S}(\{2, \ldots, n\})$ such that $q_{\sigma(i)} = p_i$ for all $i = 2, \ldots, n$. Now, define $\sigma \in \mathfrak{S}_n$ by $\sigma(1) = 1$ and $\sigma(i) = \sigma'(i)$ for all $i = 2, \ldots, n$. — **Remarks:** The above proof for uniqueness use the Euclid's lemma on the prime property (see T3.1-3)-c)) and hence uses implicitly the division algorithm and therefore make use of the additive structure of $\mathbb{N}$. The existence of prime decomposition only uses the multiplicative structure on $\mathbb{N}$ and not the additive structure on $\mathbb{N}$. This leads to the question: *Can one give a proof of the uniqueness of the prime decomposition which only depends on the multiplicative structure of $\mathbb{N}$?* The answer to this question is negative as we can see in the example given in c). The uniqueness of the decomposition of a positive natural number into product of irreducible elements is less obvious than the existence of such a decomposition. This can also be seen in the examples in c) and d).)

c). Let M be the set of all natural numbers which have remainder 1 upon division by 3, i.e., $M = \{3n + 1 \mid n \in \mathbb{N}\}$. Then M is a *multiplicative submonoid* of $\mathbb{N}$, i.e., $1 \in M$ and if $a_1, \ldots, a_n \in M$, then $a_1 \cdots a_n \in M$. For, it is enough (by induction) to note that $(3n_1 + 1)(3n_2 + 1) = 3(3n_1n_2 + n_1 + n_2) + 1$. Similar to the irreducibility in $\mathbb{Z}$, we say that an element $c \in M$ is *irreducible* if $c > 1$ and if $c = ab$ with $a, b \in M$, then either $a = 1$ or $b = 1$. The first few irreducible elements in M are: $4, 7, 10, 13, 19, 22, 25, 31$; the elements $16 = 4 \cdot 4$ and $28 = 4 \cdot 7$ are not irreducible in M. One can easily (by induction — analogous proof as in the existence of a prime decomposition): *Every element $a \in M$ is a (finite) product $a = c_1 \cdots c_n$ of irreducible elements $c_1, \ldots, c_n$ in M.* However, the uniqueness of this representation does not hold, for example, the element $100 \in M$ has two irreducible decompositions $100 = 4 \cdot 25$ and $100 = 10 \cdot 10$ which are not essentially unique. One can (similar to those of in Z) also define divisibility and prime property in M, with these definitions $4 \big| 100 = 10 \cdot 10$ in M, but $4 \not| 10$ in M, i.e., the element 4 is irreducible in M, but does not have the prime property in M. In this example what is missing is that the set M is not additively closed, for example, $4 \in M$, but $8 = 4 + 4 \notin M$ or more generally, $3n_1 = 1 \in M$ and $3n_2 + 1 \in M$, but $(3n_1 + 1) + (3n_2 + 1) = 3(n_1 + n_2) + 2 \notin M$. We further note that gcd of 40 and 100 does not exists in M and lcm of 4 and 10 does not exits in M (since $4 \not| 10$ in M).

d). Let $q \in \mathbb{N}^*$ be an arbitrary prime number (e.g. $q := 2$ or $q := 1234567891$ [7])) and $N := \mathbb{N}^* - \{q\}$. Then N is a multiplicatively closed and every element in N is a product of irreducible elements of N; such a decomposition is not any more, in general unique. More precisely, prove that: The irreducible elements in N are usual prime numbers $p \neq q$ and their products pq with q and both the elements $q_2 := q^2$ and $q_3 := q^3$. The element $n := q^6 \in N$ has two essentially different decompositions $n = q_2 \cdot q_2 \cdot q_2 = q_3 \cdot q_3$ as product of irreducible elements of N. The irreducible element q_3 divides (in N) the product $q_2 \cdot q_2 \cdot q_2$, but none of its factor. Similarly, q_2 divides (in N) the product $q_3 \cdot q_3$, but not q_3. Similarly, $m := pq^3 = (pq)q^2$ has (in N) two essentaily different decompositions (p prime number $\neq q$).

2). (Zermelo's proof of uniqueness of prime decomposition)

T3.4. (g-adic expansion) Let $g \in \mathbb{N}^*$, $g \geq 2$. For every natural number $n \in \mathbb{N}$, there exists a uniquely determined sequence $(r_i)_{i \in \mathbb{N}}$ of natural numbers almost all of which are 0 such that $n = \sum_{i=0}^{\infty} r_i g^i$ and $0 \leq r_i < g$ for all $i \in \mathbb{N}$.(**Remark:** This unique representation of n is called the g-adic expansion of n and the r_i, $i \in \mathbb{N}$, are called the digits of n in the g-adic system. If $r_i = 0$ for $i > t$, then we write $n = (r_t, \ldots, r_0)_g$ and say that the g-adic expansion $n = \sum_{i=0}^{t} r_i g^i$ of n, which can lead to no misunderstandings. Moreover, if $r_t \neq 0$, then $r_t, \ldots, r_0$ are called the essential digits of n. — For $g = 2$ resp. $g = 10$ we also use the terms

[7]) One can check this with a small computer programm that this number is really a prime number. Is the number 12345678901 also prime?

dual– resp. decimal system.) Let $n \in \mathbb{N}^*$ and let $a_m 10^m + a_{m-1}10^{m-1} + \cdots + a_1 10 + a_0$, $m \in \mathbb{N}$ and $a_j \in \{0, 1, \ldots, 9\}$ be the decimal expansion of n. Then

a). $3|n \iff 3|(a_0 + a_1 + \cdots + a_m)$; $5|n \iff 5|a_0$; $9|n \iff 9|(a_0 + a_1 + \cdots + a_m)$; $11|n \iff 11|(a_0 - a_1 + \cdots + (-1)^m a_m)$.

b). $7|n \iff 7|(a_2, a_1, a_0)_{10} - (a_5, a_4, a_3)_{10} + \cdots$; $11|n \iff 11|(a_2, a_1, a_0)_{10} - (a_5, a_4, a_3)_{10} + \cdots$; $13|n \iff 13|(a_0 + 2a_1 + \cdots + 2^m a_m)$;

T3.5. (Irrational numbers) A real number which is not rational is called an irrational number.

1). Prove that the irrational numbers are not closed under addition, subtraction, multiplication, or division; The sum, difference, product and quotient of two real numbers, one irrational and the other a non-zero rational, are irrational.

2). Let $n \in \mathbb{N}^*$, $y \in \mathbb{Q}$, $y > 0$ and let $y = p_1^{m_1} \cdots p_r^{m_r}$ be the canonical prime factorisation of y. Show that the following statements are equivalent: (i) There exists a positive rational number x with $x^n = y$. (ii) n divides all the exponents m_i, $i = 1, \ldots, r$.

3). (Lemma of Gauss) Let $x := a/b \in \mathbb{Q}$ be a *normalised* fraction, i.e., $a, b \in \mathbb{Z}$, $b > 0$ and $\gcd(a, b) = 1$. Suppose that $a_n x^n + \cdots + a_1 x + a_0 = 0$ with $a_0, \ldots, a_n \in \mathbb{Z}$ and $a_n \neq 0$, $n \geq 1$, i.e., x is a zero of the polynomial function $a_n t^n + \cdots + a_0$. Then a is a divisor of a_0 and b is a divisor of a_n. Deduce that:

(i) if the leading coefficient $a_n = 1$, then $x \in \mathbb{Z}$. (ii) For any integer $a \in \mathbb{Z}$ and a natural number $n \in \mathbb{N}^*$, every rational solution of $x^n - a$ is an integer, in particular, $x^n - a$ has a rational solution if and only if a is the n- th power of an integer. (**Remark:** It follows at once that $\sqrt{2}$ (Phythagoras)[8]) $\sqrt{3}, \sqrt{5}, \ldots, \sqrt{p}$, where p is prime number, are irrational numbers.) More generally: (iii) Let $r \in \mathbb{N}^*$, $p_1, \ldots, p_r$ be distinct prime numbers and let $m_2, \ldots, m_r \in \mathbb{N}^*$ Then for every $n \in \mathbb{N}^*$, $n > 1$, the real number $\sqrt{p_1 p_2^{m_2} \cdots p_r^{m_r}}$ is an irrational number. (iv) For $a, b \in \mathbb{Z}$, $a > 0, b > 0$ with $\gcd(a, b) = 1$ and a natural number $n \in \mathbb{N}^*$, the equation $x^n - a/b$ has a rational solution if and only if both a and b are n- th power of integers.

4). Let $a_1, \ldots, a_r \in \mathbb{Q}_+^\times$ be positive rational numbers. Show that $\sqrt{a_1} + \cdots + \sqrt{a_r}$ is rational if and only if each a_i, $i = 1, \ldots, r$ is a square of rational number.

5). Determine all rational zeros of the polynomial functions $t^3 + \frac{3}{4}t^2 + \frac{3}{2}t + 3$ and $3t^7 + 4t^6 - t^5 + t^4 + 4t^3 + 5t^2 - 4$.

6). Let t be a rational multiple of π [9]), i.e. $t = r\pi$ with $r \in \mathbb{Q}$. Then $\cos t$, $\sin t$ and $\tan t$ are irrational numbers apart from the cases where $\tan t$ is undefined and the exceptions $\cos t = 0, \pm 1/2, \pm 1$; $\sin t = 0, \pm 1/2, \pm 1$; $\tan t = 0, \pm 1$.

7). The real numbers $\log_6 9$ and $\log 3 / \log 2$ are irrational numbers.

8). Let z be a real number. Show that the following statments are equivalent: (i) z is rational. (ii) There exists a positive integer k such that $[kz] = kz$. (iii) There exists a positive integer k such that $[(k!)z] = (k!)z$.

9). Use the above part 8) to prove that the number e is irrational. (**Hint:** The number $e = \sum_{i=0}^{\infty} \frac{1}{i!}$ is called the Euler's number. For any positive integer k, we have $[(k!)e] = k! \sum_{i=0}^{k} 1/i! < (k!)e$.) (**Remark:** The proof of irrationality of the number π is not quite so easy!)

T3.6. In this Exercise we investigate some simple results and rules concerning the divisibility relation in a commutative monoid M with cancellation law. An element $u \in M$ is called invertible if there exists $v \in M$ such that $uv = vu = e_M\}$. Moreover, the element v is unique and is called the inverse of u (in M) and therefore is denoted by u^{-1}. The set $M^\times := \{u \in M \mid u \text{ is invertible in } M\}$ is a group with respect to the same binary operation of M and is called the unit group of M. A monoid M is called pointed if the unit group $M^\times$ is the trivial group $\{e_M\}$. For example, the monoid $(\mathbb{N}^*, \cdot)$ of non-zero natural numbers, is a pointed monoid, but the monoid $(\mathbb{Z}^*, \cdot)$ of non-zero integers, is not a pointed monoid, since $(\mathbb{Z}^*, \cdot)^\times = \{\pm 1\}$.

In all statements below M denote a commutative monoid with cancellation law, $e = e_M$ denote the neutral (identity) element of M and let a, b, c be elements of M.

---

[8]) PHYTHAGORAS (569-500 B. C.) deserve the credit for being the first to classify numbers into odd and even, prime and composite. The following elementary short proof was given by (T. ESTERMANN in Math. Gazette 59 (1975), pp. 110): If $\sqrt{2}$ is tradational, then there exists $k \in \mathbb{N}^*$ such that $k\sqrt{2} \in \mathbb{Z}$. By the principle of the minimality chhose a minimal k with this property. Then, since $1 < \sqrt{2} < 2$, $m := (\sqrt{2} - 1)k \in \mathbb{N}^*$ with $m < k$, but $m\sqrt{2} = (\sqrt{2} - 1)k\sqrt{2} = 2k - k\sqrt{2} \in \mathbb{Z}$ a contradiction.

[9]) What is the definition of the number π ?,

1). If M is pointed, i.e., if $M^\times = \{e\}$, then the divisiblity relation on M is an order on M, i.e., it is a reflexive, transitive and anti-symmetric relation on M. For example, the divisibility is an order on $\mathbb{N}^*$.

2). Two elements a, b in any monoid M are called associates (in M) if $b = ua$ with $u \in M^\times$. The relation on M defined by $a \sim b$ if a and b are associates in M is an equivalence relation. Show that $a \sim b$ if and only if a divides b and b divides a, i.e., $a|b$ and $b|a$.

3). An element $a \in M$ is called irreducible if $a \notin M^\times$ and if the only divisors of $a \in M$ are the units and the associates of a in M, i.e., if $a = bc$ with $b, c \in M$, then either $b \in M^\times$ or $c \in M^\times$. —An element $a \in M$ is called prime if $a \notin M^\times$ and if $a|bc$ with $b, c \in M$, then either $a|b$ or $c|c$ in M. *Every prime lement in a monoid M is irreducible in M.* (**Proof:** If $a \in M$ is a prime element in M and if $p = bc$, then $p \notin M^\times$ and $p|bc$ and hence either $p|b$ or $p|c$. We may assume $p|b$, i.e., $b = pq$ for some $q \in M$. Then $p = bc = pqc$ and so $1 = qc$, since M has cancellative law. This proves that $c \in M^\times$ and hence p is irreducible. The converse is not true in general, i.e., there are irrducible elements in a commutative cancellative monoids which are not prime. For example, in the monoid M of example T3.3-1)-c) the element 4 is irreducible but not prime. See also Examples in T3.3.-1)-d).)

4). The quotient set $\overline{M} := M/\sim$ of M with respect to the relation $\sim$ of "associates" defined in the part 2) above, is a monoid with (well-defined) multiplication defined by $\overline{a} \cdot \overline{b} := \overline{ab}$ and the unit group $\overline{M}^\times = \{\overline{e}\}$, i.e, $\overline{M}$ is a pointed monoid. Moreover, $\overline{a}|\overline{b}$ if and only if $a|b$.

5). The element $a \in M$ is irreducible (resp. prime) if and only if $\overline{a} \in \overline{M}$ is irreducible (resp. prime).

6). (Factorial Monoids) A commutative monoid M with cancellation law is called a factorial monoid or unique factorisation monoid if every element $a \in M$, $a \notin M^\times$ is a product of irreducible elements in M and such a factorization is unique upto permutation and upto units in M, i.e., if $a = p_1 \cdots p_r = q_1, \cdots q_s$ with $p_1, \ldots, p_r$; $q_1, \ldots, q_s$ are irreducible elements in M, then $r = s$ and there exists a permutation $\sigma \in \mathfrak{S}_r$ such that $q_i = u_i p_{\sigma(i)}$ with $u_i \in M^\times$ for every $i = 1, \ldots, r$.

7). Show that the following statements are equivalent: (i) M is factorial (or a unique factorisation monoid). (ii) $\overline{M}$ is factorial. (iii) $\overline{M}$ is isomorphic to the monoid $(\mathbb{N}^{(I)}, +)$ for some set I. Moreover, in this case the monoid M is isomorphic to the product monoid $M^\times \times \overline{M}$.

8). In the ordered set $(\overline{M}, |)$, if $\inf(\overline{a}, \overline{b}) \in \overline{M}$ exists, then any of its representative in M is called the greatest common divisor of a and b and is denoted by $\gcd(a, b)$. Similarly, if $\sup(\overline{a}, \overline{b}) \in \overline{M}$ exists, then any of its representative in M is called the least common multiple of a and b and is denoted by $\operatorname{lcm}(a, b)$. Prove the formula: $\gcd(a, b)\operatorname{lcm}(a, b) = \overline{a}\overline{b}$ if both $\gcd(a, b)$ and $\operatorname{lcm}(a, b)$ exist.

9). Show that if $\gcd(ac, bc)$ exists, then $\gcd(a, b)$ exists. and $\gcd(ac, bc) = \gcd(a, b) \cdot \overline{c}$. Similarly, show that if $\operatorname{lcm}(ac, bc)$ exists, then $\operatorname{lcm}(a, b)$ exists and $\operatorname{lcm}(ac, bc) = \operatorname{lcm}(a, b) \cdot \overline{c}$.

10). Show that the following statements are equivalent: (i) $\operatorname{lcm}(a, b)$ exists (ii) $\operatorname{lcm}(ax, bx)$ exists for all $x \in M$. (iii) $\gcd(ax, bx)$ exists for all $x \in M$.

11). Give an example of a monoid M to show that $\gcd(a, b)$ exists, but $\operatorname{lcm}(a, b)$ does not.

12). Show that the following statements are equivalent: (i) $\operatorname{lcm}(x, y)$ exists for all $x, y \in M$.

(ii) $\gcd(x, y)$ exists for all $x, y \in M$. (iii) $\overline{M}$ is a *lattice* with respect to the divisibility order. (**Remark:** An ordered set $(X, \leq)$ is called a lattice if $x \sqcup y := \sup(x, y)$ and $x \sqcap y := \operatorname{Inf}(x, y)$ exist for all $x, y \in M$. In this case the binary operations $\sqcup$ and $\sqcap$ on M are associative, commutative and fullfill the following *merging rules*: $x \sqcup (x \sqcap y) = x$ and $x \sqcap (x \sqcup y) = x$ for all $x, y \in M$. Conversely, if $\sqcup$ and $\sqcap$ are binary operations on a set X, then X is lattice with respect to the order on $\leq$ on X defined by "$x \leq y$ if and only if $x \sqcap y = x$" and the operations $(x, y) \mapsto \sup(x, y)$ and $(x, y) \mapsto \inf(x, y)$ are given binary operations $\sqcup$ and $\sqcap$.)