Algebra, Arithmetic and Geometry – With a View Toward Applications / 2005

Lectures : Tuesday/Thursday 18:15–19:15 ; LH-1, Department of Mathematics

2. The Fundamental Theorem of Arithmetic — Divisibility in Monoids

Euclid of Alexandria[†]

(≈ 325 BC - ≈ 265 BC)

2.1. (Gödelisation) Let $p_1 = 2,\ p_2 = 3,\ p_3 = 5,\ \ldots$ 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 $(a_{i_1}, \ldots a_{i_n}, a_0, a_0, \ldots)$. 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 T2.1 -13)).)

2.2. 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 T2.1 -13))

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.

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 mathmetaicains; but GAUSS was the first to develop arithmetic as a systematic science.

(**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 checksum, 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 T2.1 -14) for details.)

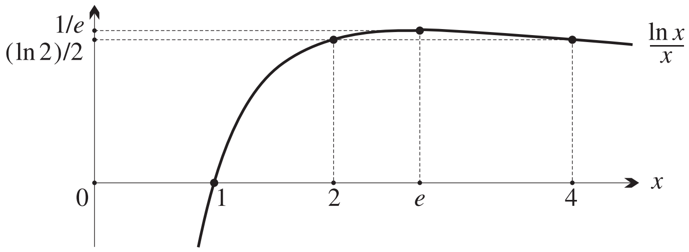
2.3. a). For $a, m, n \in \mathbb{N}^*$ with $a \geq 2$ and $d := \gcd(m, n)$, show that $\gcd(a^m - 1, a^n - 1) = a^d - 1$. In particular, $a^m - 1$ and $a^n - 1$ are relatively prime if and only if $a = 2$ and m and n are relatively prime. (**Hint:** By substituting a^d by a one may assume that $d = 1$. 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 $b = u_1 a_1 + \cdots + a_n a_n$ 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 $u_1 a_1 + u_2 a_2,\ u_1, u_2 \in \mathbb{N}$. (**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 $s' = s - k\frac{b}{d},\ t' = t + k\frac{a}{d}$.

2.4. 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 $x^y = y^x$. (Note 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.)

2.5. 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 $a_{i+1} = (a_i - m)a_i + m = a_i^2 - m a_i + m$ for every $i \geq 1$.

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 $\dfrac{1}{a_0} + \dfrac{m}{a_1} + \cdots + \dfrac{m^i}{a_i} = \dfrac{m+1}{n} - \dfrac{m^{i+1}}{a_{i+1} - m}$. Deduce that $\displaystyle\sum_{i=0}^{\infty} \frac{m^i}{a_i} = \frac{m+1}{n}$.

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, $\displaystyle\sum_{i=0}^{\infty} \frac{2^i}{F_i} = 1$.

2.6. 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) $\operatorname{lcm}(a,b)$ exists for every $a, b \in M$. (iv) $\gcd(a,b)$ exists for every $a, b \in M$. (**Hint:** Use 2.1-h) and 2.1-j).)

2.7. Let $n \in \mathbb{N}^*$ and let $M \subseteq \mathbb{N}^n$ be a submonoid of $(\mathbb{N}^n, +)$. The dimension of the subspace of the $\mathbb{Q}$- vector space of $\mathbb{Q}^n$ generated by M is called the rank of M and is denoted by $\operatorname{rank}(M)$. Show that:

a). Every element in M is a sum of irreducible elements. (**Hint:** Let $a = (a_1, \ldots, a_n) \in M$ and $|a| := a_1 + \cdots + a_n$ Use induction on $|a|$.)

b). The irreducible elements of M form a smallest subset of M which generates M as a monoid, i.e., every generating set $S \subseteq M$ contains the set of irreducible elements of M.

c). M is factorial if and only if M is generated by $r := \operatorname{rank}(M)$ elements. Moreover, in this case M is isomorphic to the monoid $(\mathbb{N}^r, +)$. .

2.8. Let p be a prime number. Then

a). $v_p((2n)!/(n!)^2) = \sum_{k \geq 1} \left([2n/p^k] - 2[n/p^k]\right)$ and if $n < p < 2n$, then $v_p((2n)!/(n!)^2) = 1$.

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

c). Find $n \in \mathbb{N}^*$ such that $v_p(n!) = 100$.

2.9. a). For any $n \in \mathbb{N}^*$, show that:

$$\sum_{d|n} \sigma(d) = \sum_{d|n} \frac{n}{d} \cdot \tau(d) \quad \text{and} \quad \sum_{d|n} \frac{n}{d} \cdot \sigma(d) = \sum_{d|n} d \cdot \tau(d).$$

(**Hint:** Since the functions $F(n) = \sum_{d|n} \sigma(d)$ and $G(n) = \sum_{d|n} \frac{n}{d} \tau(d)$ are both multiplicative, it is enough to prove that $F(p^m) = G(p^m)$ for each prime p and each $m \in \mathbb{N}^*$.)

b). For $n \in \mathbb{N}^*$ and $k \in \mathbb{N}$, let $\sigma_k(n)$ denote the sum of the k-th positive divisors of n, i.e, $\sigma_k(n) = \sum_{d|n} d^k$. Show that:

1). $\sigma_0 = \tau$ and $\sigma_1 = \sigma$.

2). σ_k is a multiplicative function. (**Hint:** The arithmetic function $n \mapsto n^k$ is multiplicative and use T2.9-1)-e).)

3). If $n \in \mathbb{N}^*$, $n > 1$ and $n = p_1^{m_1} \cdots p_r^{m_r}$ is the canonical prime factorisation of n, then

$$\sigma_k(n) = \prod_{i=1}^{r} \frac{(p^{k(m_i+1)} - 1)}{(p_i^k - 1)}.$$

In particular, $\sigma_k(p^m) = \dfrac{p^{k(m+1)} - 1}{p^k - 1}$. Therefore the arithmetic functions σ_k are multiplicative.

2.10. Let $m, n \in \mathbb{N}^*$. Show that

a). If $n > 1$ and $n = p_1^{m_1} \cdots p_r^{m_r}$ is the canonical prime factorisation of n, then

$$\sigma(n) \cdot \varphi(n) \geq n^2 \prod_{i=1}^{r} (1 - 1/p_i^2) \quad \text{and} \quad \tau(n)\varphi(n) \geq n.$$

(**Hint:** Prove that $\tau(n) \cdot \varphi(n) \geq 2^r \cdot n \cdot (1/2^r)$.)

b). If $d|n$, then $\varphi(d)|\varphi(n)$.

c). $\varphi(m) \cdot \varphi(n) = \varphi(mn) \cdot \varphi(\gcd(m,n))/\gcd(m,n) = \varphi(\gcd(m,n)) \cdot \varphi(\operatorname{lcm}(m,n))$.

d). If p is prime and $k \geq 2$, then $\varphi(\varphi(p^k)) = p^{k-1}\varphi((p-1)^2)$.

Below one can see (simple) test-exercises.

Test-Exercises

T2.1. (Divisibility in $\mathbb{N}$ and $\mathbb{Z}$ /gcd/Division algorithm/Euclidean algorithm)

1). (Lemma of Bezout) Let $a, b \in \mathbb{N}$ be two natural numbers. Then there exists integers $s, t \in \mathbb{Z}$ such that $\gcd(a, b) = sa + tb$. In particular, if a and b are relatively prime positive natural numbers, then there exist integers $st \in \mathbb{Z}$ such that $1 = sa + tb$. Deduce that: (i) For two non-zero integers $ab \in \mathbb{Z}^*$, 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 $b_1 \cdots b_r$ of positive natural numbers, then p divides at least one of the factor b_i.

2). For positive natural numbers $a, b, c \in \mathbb{N}^*$ and $m, n \in \mathbb{N}^*$, show that: (i) if $\gcd(a, b) = 1$ and $\gcd(a, c) = 1$, then $\gcd(a, bc) = 1$. (ii) if $\gcd(a, b) = 1$, then $\gcd(a^m, b^n) = 1$. (iii) 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 $\gcd(r^n, s^n) = 1$. Now show that $r = 1$, whence $a = d$.) (iv) if $\gcd(a, b)$ divides $\operatorname{lcm}(a, b)$ and $\gcd(a, b) \cdot \operatorname{lcm}(a, b) = ab$. Moreover, $\gcd(a, b) = \operatorname{lcm}(a, b)$ if and only if $a = b$. (v) $\gcd(a, b) = 1$ if and only if $\operatorname{lcm}(a, b) = ab$. (vi) $a|b \iff \gcd(a, b = a \iff \operatorname{lcm}(a, b) = b$.

3). Let $a_1, \ldots, a_n \in \mathbb{N}^*$, $n \geq 1$ 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.)

4). For $a_1, \ldots, a_n \in \mathbb{N}^*$, $n \geq 1$, 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 T2.1-1)) and $\gcd(a_1, \ldots, a_{n-1}, a_n) = \gcd(\gcd(a_1, \ldots, a_{n-1}), a_n)$. This algorithm supplies frequently disproportionately large coefficients $u_1, \ldots, u_n$. It is better to proceed as follows: One nummeriere first so that a_1 is minimal in a_i, 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 $1 = u_1 \cdot 88 + u_2 \cdot 152 + u_3 \cdot 209$.

5). Let $a_1, \ldots, a_n \in \mathbb{N}^*$, $n \geq 1$. For $J \in \mathfrak{P}(\{1, \ldots, n\})$, put $\varepsilon(J) := (-1)^{|J|+1}$, $d_J := \gcd(a_j \mid j \in J)$ and $m_J := \operatorname{lcm}(a_j \mid j \in J)$. Then $d_I = \gcd(a_1, \ldots, a_n) = \prod\limits_{\substack{J \in \mathfrak{P}(\{1,\ldots,n\}), \\ J \neq \emptyset}} d_J^{\varepsilon(J)}$ and $m_I = \operatorname{lcm}(a_1, \ldots, a_n) = \prod\limits_{\substack{J \in \mathfrak{P}(\{1,\ldots,n\}), \\ J \neq \emptyset}} m_J^{\varepsilon(J)}$. In particular, $\gcd(a, b) \operatorname{lcm}(a, b) = ab$ for $a, b \in \mathbb{N}^*$.

6). 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 $\gcd(a, b) = 1$.)

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

8). For $m, n \in \mathbb{N}$, $m > n$, show that $a^{2^n} + 1$ divides $a^{2^m} - 1$. Moreover, if $m, n, a \in \mathbb{N}^*$, $m \neq n$, then $\gcd(a^{2^m} + 1, a^{2^n} + 1) = \begin{cases} 1, & \text{if } a \text{ is even,} \\ 2, & \text{if } a \text{ is odd.} \end{cases}$

9). 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 $y - 1$.

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

11). (Gauss-bracket) For a real number $x \in \mathbb{R}$, let $[x]$ denote the largest integer $leqx$, i.e., $[x]$ is the unique integer satisfying $[x] \leq x < [x] + 1$. The integer $[x]$ is called the integral part of x. It is also useful to put $\{x\} := x - [x]$. This is the fractional part of x. Many of the basic properties of the function $x \mapsto [x]$ are included below:

Let x and y be real numbers. Then we have

a). $x-1<[x]\leq x<[x]+1$, $0\leq\{x\}=x-[x]<1$ and $-[-x]$ is the least integer $\geq x$.

b). $[x]=\sum_{1\leq i\leq x}1$ if $x\geq 0$. **c).** $[x+n]=[x]+n$ for every integer $n\in\mathbb{Z}$.

d). $[x]+[y]\leq[x+y]\leq[x]+[y]+1$, $[x]+[y]+[x+y]\leq[2x]+[2y]$ and if x, y, are positive, then $[x][y[\leq[xy]$.

e). $[x]+[-x]=\begin{cases}0, & \text{if } x \text{ is an integer,}\\ -1, & \text{if } x \text{ is not an integer.}\end{cases}$ **f).** $\left[\frac{[x]}{m}\right]=\left[\frac{x}{m}\right]$ for any positive integer m.

g). For $m,n,k\in\mathbb{N}^*$, $[n/k]=\operatorname{card}(\{a\in\{1,2,\ldots,n\}\mid k|a\})$ and $[nm/k]\geq n[m/k]$.

12). Show that $\frac{(2n)!}{n!\cdot(n+1)!}$ is an integer. (**Hint:** $\binom{2n}{n}\cdot(2n+1)=\binom{2n+1}{n+1}\cdot(n+1)$.)

13). (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 $n=\sum_{i=0}^{\infty}r_ig^i$ 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 $n=\sum_{i=0}^{t}r_ig^i$ 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 dual– resp. decimal system.)

14). Let $n\in\mathbb{N}^*$ and let $a_m10^m+a_{m-1}10^{m-1}+\cdots+a_110+a_0$, $m\in\mathbb{N}$ and $a_j\in\{0,1,\ldots,9\}$ be the decimal expansion of n. Then

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

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

T2.2. (Primes) Let $\mathbb{P}$ denote the set of all prime numbers. Then

1). (Euclid) $\mathbb{P}$ is an infinite set. Moreover, if 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 infinitely. 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 $n^4+4^n=(n^2-2^{\frac{n+1}{2}}\cdot n+2^n)(n^2+2^{\frac{n+1}{2}}\cdot n+2^n)$.)

T2.3. **1).** (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.) 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 are prime, but corresponding to $p=11$, it is not prime. (**Remark:** 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[1] prime is the Mersenne number M_p corresponding to $p = 25,964,951$; this prime number has $[\log_{10}(2^{25,964,951})] + 1 = [25,964,951 \cdot \log_{10} 2] + 1 = 7816230$ digits!)

2). (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. The natural number of the form $2^q + 1$, $q = 2^n$, $n \in \mathbb{N}$ is called the n-th Fermat number and is denoted by $F_n (:= 2^{2^n} + 1$, $n \in \mathbb{N}$. The Fermat numbers F_0, F_1, F_2, F_3, F_4 are prime, but F_5 is not prime. ($641 = 5^4 + 2^4 = 5 \cdot 2^7 + 1$ divides $5^4 \cdot 2^{28} + 2^3$ and $5^4 \cdot 2^{28} - 1$ and hence the difference $2^{32} + 1 = F_5$. Any two distinct Fermat numbers are relatively prime, since $F_{m+1} = 2 + F_0 \cdots F_m$. (**Remark:** Whether or not there are more Fermat numbers which are prime is unknown.)

3). (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 $\sigma(b = 2^{s+1}c$, $b = (2^{s+1} - 1)c$, $\sigma(b) = b + c$.)

T2.4. Let M be a commutative monoid with cancellation law and let $ab, c \in M$. Let $\sim$ be the relation on M defined by $a \sim b$ if a and b are associates in M, i.e., $b = ua$ for some $u \in M^\times$. Then:

1). $\sim$ is an equivalence relation on M and $a \sim b$ if and only if $a \big| b$ and $b \big| a$.

2). The quotient set $\overline{M} := M/\sim$ of M with respect to $\sim$ is a monoid with (well-defined) multiplication defined by $\overline{a} \cdot \overline{b} := \overline{ab}$ and $\overline{M}^\times = \{\overline{e}\}$, i.e, $\overline{M}$ is a pointed monoid. Moreover, $\overline{a} \big| \overline{b}$ if and only if $a \big| b$.

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

4). 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 $M^\times \times \overline{M}$.

5). Show that divisibility defines an order on $\overline{M}$.

6). 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.

7). 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 $\operatorname{lcm}(ac, bc) = \operatorname{lcm}(a, b) \cdot \overline{c}$.

8). 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 $x \in M$.

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

10). 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 $\sqcap$.)

T2.5. 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 be seen in the following example:

Let $q \in \mathbb{N}^*$ be an arbitrary prime number (e.g. $q := 2$ or $q := 1234567891$[2])) 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

[1] On February 18, 2005, Dr.Martin Nowak, an eye surgeon from Germany, found the new largest known prime number, $2^{25,964,951} - 1$. 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 60, 000 volunteers from around the world took part. Such huge numbers are used in problems related to Cryptography.

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

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 $\neq q$).

T2.6. Let $n \in \mathbb{N}^*$ and let p be a prime number. Then show that

1). The multiplicity of p in $n\,!$ is

$$\left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \left[\frac{n}{p^3}\right] + \cdots .$$

(**Remark:** Since $[x/m] = [\,[x]/m]$ for all $x \in \mathbb{R}$ and all $m \in \mathbb{N}^*$ one can compute the sum on the right hand side easily by recursion. It is easy to prove the equality: $\sum_{i\geq 1}[n/g^i] = \big(n - \sum_{i\geq 0} a_i\big)\big/(g-1)$ *for every* $g \in \mathbb{N}^*$, $g \geq 2$, *where* a_i *are the digits in the* g*-adic expansion of* n. *In particular,* $n \equiv \sum_{i\geq 0} a_i$ *modulo* $g-1$. The sum check-sum $\sum_{i\geq 0} a_i$ of n. In the case $g = 10$, one speaks of the nine proof. – 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.)

2). Let $n, k \in \mathbb{N}^*$, $k \leq n$. Show that every prime power divisor of $\binom{n}{k}$ is $\leq n$. (**Hint:** Use part 1).)

3). Find the canonical prime factorisation of: (i) 81 057 226 635 000. (ii) 50! and 100!. (iii) the product $1 \cdot 3 \cdot 5 \cdots 99$ of the first 50 odd numbers. (iv) the least common mulptiple $\operatorname{lcm}(1, 2, 3, \ldots, 50)$ of the first 50 positive natural numbers.

4). Let $n, k \in \mathbb{N}^*$ be relatively prime numbers. Show that $\binom{n}{k}$ is divisible by n and $\binom{n-1}{k-1}$ is divisible by k. (**Hint:** Use the formula $k\binom{n}{k} = n\binom{n-1}{k-1}$.)

5). For $r, k \in \mathbb{N}$ with $r < k < p$, show that $\binom{p+r}{k}$ is divisible by p. In particular, $\binom{p}{k}$ is divisible by p for $0 < k < p$.

6). Prove (by induction on n) the Fermat's little theorem : *For every natural number* n, $n^p - n$ *is divisible by* p, i.e., $n^p \equiv n$ modulo p. (**Hint:** Use part 5).)

7). For every natural number n, $n^8 - n^2$ is divisible by $4 \cdot 7 \cdot 9 = 252$. (**Hint:** Use induction.)

8). Let $r \in \mathbb{N}^*$, $m = (m_1, \ldots, m_r) \in \mathbb{N}^r$ and $n := \sum_{i=1}^r m_i$. All prime numbers p with Max $(m_1, \ldots, m_r) < p \leq n$ divide $\binom{n}{m} = n!/m_1! \cdots m_r!$.

9). The product of two relatively prime natural numbers a and b is the n-the power of a natural number $(n \in \mathbb{N}^*)$ if and only if both a and b are n-th power of a natural number.

T2.7. 1). Let $p_1, \ldots, p_m$ be prime numbers $\leq n+1$ and let $x = p_1 \cdots p_m$. Then none of the n natural numbers $x+1, x+3, \ldots, x+(n+1)$ is prime.

2). Let $m, n \in \mathbb{N}^*$. Then m has no divisor which is n-th power except 1 if and only if $v_p(m) < n$ for every prime number p. (**Remark:** In the case $n = 2$, we say that m is square- free.)

3). Let $n \in \mathbb{N}^*$, $n > 2$. Then both $\sum_{k=1}^n 1/k$ and $\sum_{k=1}^n 1/(2k-1)$ are not integers. (**Hint:** Find 2-exponents.)

4). Let $a \in \mathbb{R}$, $a > 0$ and $a \neq 1$. Then the real numbers $\log_a p$, $p \in \mathbb{P}$, are linearly independent over $\mathbb{Q}$.

5). Let $n \in \mathbb{N}^*$ be an odd number, $n \geq 3$. Suppose that n has no prime divisors $\leq m$, $m \in \mathbb{N}^*$, $m \geq 3$. Then n is prime if and only if none of the natural number $n + k^2$, $k = 0, 1, \ldots, \dfrac{(n-m)^2}{2m}$ is square free. (**Hint:** $\left(\frac{x+y}{2}\right)^2 - \left(\frac{x-y}{2}\right)^2 = xy$.)

6). Show that $v_2\Big([(1+\sqrt{3})^{2m+1}]\Big) = m + 1$ for every $m \in \mathbb{N}^*$.

7). Let $p_1, \ldots, p_r$ be prime numbers and let $n \in \mathbb{N}^*$. Let $N(n)$ denote the number of positive natural numbers $\leq n$ whose prime divisors are contained in $\{p_1, \ldots, p_r\}$, i.e., $N(n) = |\{m \in \mathbb{N}^* \mid m \leq n$ and $m = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$, $\alpha_1, \ldots, \alpha_r \in \mathbb{N}\}$. Show that

a). $N(n) \leq \binom{[\log_2 n]+r}{r} \leq \big([\log_2 n] + 1\big)^r$. (**Hint:** Use $2^{\alpha_1+\cdots+\alpha_r} \leq p_1^{\alpha_1} \cdots p_r^{\alpha_r} \leq n$.)

b). $N(n) \leq 2^r[\sqrt{n}]$. (**Hint:** Every $m \in \mathbb{N}^*$ can be expressed as $m = m_1^2 \cdot m_2$ with $m_1, m_2 \in \mathbb{N}^*$ and m_2 square-free.)

T2.8. (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 divisior 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)[3]) $\sqrt{3}, \sqrt{5}$ 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 $\sqrt[n]{p_1 p_2^{m_2} \cdots p_r^{m_r}}$ 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[4]), i.e. $t = r\pi$ with $r \in \mathbb{Q}$. Then $\cos t$, $\sin t$, and $\tan t$ are irrational number 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 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; we shall prove this later.)

T2.9. (Arithmetic functions) Any function defined on the set of positive natural numbers is called a number-theoretic or (arithmetic) function. The codomain of an arithmetic function need not be $\mathbb{N}^*$ or, for that matter, even an integer; it is very interesting to study arithmetic functions with values in a fixed ring. An arithmetic function f is said to be multiplicative if $f(mn) = f(m)f(n)$ whenever $\gcd(m, n) = 1$. Multiplicative arithmetic functions are uniquely determined by their values at prime powers. The constant function 1 and the identity function on $\mathbb{N}^*$ are clearly multiplicative arithmetic functions.

1). Show that: **a).** For a fixed integer k, the function $n \mapsto n^k$ is multiplicative. **b).** If f and g are multiplicative arithmetic functions and $f(p^k) = g(p^k)$ for each prime p and each $k \in \mathbb{N}^*$, then $f = g$. **c).** If f and g are multiplicative arithmetic functions, then so is their product fg and the quotient f/g (whenever the quotient function is defined). **d).** The function $\rho : \mathbb{N}^* \to \mathbb{N}$ by $\rho(1) = 1$ and $\rho(n) = 2^r$, if the canonical prime factorisation of $n > 1$ is $n = p_1^{m_1} \cdots p_r^{m_r}$ is multiplicative. **e).** If f is a multiplicative arithmetic function, then the arithmetic function F defined by $F(n) = \sum_{d|n} f(d)$ is also multiplicative. If $f = \rho$ (see the part d) above), then what down the formula for $F(n)$ in terms of the canonical prime factorisation of n.

2). For $n \in \mathbb{N}^*$, let $\tau(n)$ denote the number of positive divisors of n and let $\sigma(n)$ denote the sum of positive divisors of n. Then:

a). If $n \in \mathbb{N}^*$, $n > 1$ and $n = p_1^{m_1} \cdots p_r^{m_r}$ is the canonical prime factorisation of n, then $\tau(n) = \prod_{i=1}^{r}(m_i + 1)$ and $\sigma(n) = \displaystyle\prod_{i=1}^{r} \frac{(p^{m_i+1} - 1)}{(p_i - 1)}$. In particular, $\tau(p^m) = (m + 1)$ and $\sigma(p^m) = \dfrac{p^{m+1} - 1}{p - 1}$. Therefore both the arithmetic functions τ and σ are multiplicative.

[3] PHYTHAGORAS (569-500 B. C.) deserve the credit for being the first to classify numbers into odd and even, prime and composite.

[4] What is the definition of the number π ?,

b). For any $n \in \mathbb{N}^*$, $\tau(n) \le 2\sqrt{n}$. (**Hint:** If $d|n$ then one of d or n/d is $\le \sqrt{n}$.)

c). If $n \in \mathbb{N}^*$ is a square-free, then $\tau(n) = 2^r$, where r is the number of prime divisors of n.

d). $\tau(n)$ is and odd integer if and only if n is a perfect square.

e). $\sigma(n)$ is and odd integer if and only if n is a perfect square or twice a perfect square. (**Hint:** If p is an odd prime, then $1 + p + p^2 + \cdots + p^k$ is odd only when k is even.)

f). Find the form of all $n \in \mathbb{N}^*$ satisfying $\tau(n) = 10$ (resp. $\sigma(n) = 10$). What is the samllest positive integer n for which this is true? (**Hint:** For $n > 1$, $\sigma(n) > n$.)

g). Find the smallest natural number $n \in \mathbb{N}$ which has exatly (respectively, at least) 60 divisors.

h). Let $n \in \mathbb{N}^*$. Prove that: (i) $\sum_{d|n} 1/d = \sigma(n)/n$. (ii) If $n = p_1^{m_1} \cdots p_r^{m_r}$ is the canonical prime factorisation of n, then $1 > \dfrac{n}{\sigma(n)} > \left(1 - \dfrac{1}{p_1}\right)\left(1 - \dfrac{1}{p_2}\right)\cdots\left(1 - \dfrac{1}{p_r}\right)$. (iii) $\dfrac{\sigma(n!)}{n!} \ge 1 + \dfrac{1}{2} + \cdots + \dfrac{1}{n}$. (**Hint:** Use the part a).) (iv) If n is a composite number, then $\sigma(n) > n + \sqrt{n}$. (**Hint:** If $d|n$ with $1 < d < n$ and $d \le \sqrt{n}$, then $1 < n/d < n$ and $n/d \ge \sqrt{n}$.)

i). Given $k \in \mathbb{N}^*$, with $n > 1$, there are infinitely many $n \in \mathbb{N}^*$ for which $\tau(n) = k$, but at most finitely many $n \in \mathbb{N}^*$ with $\sigma(n) = k$. (**Hint:** Use the part b).)

j). Let f is a multiplicative arithmetic function and let F be the multiplicative (see 1)-e)) arithmetic function F defined by $F(n) = \sum_{d|n} f(d)$. Then for any $k \in \mathbb{N}^*$, we have $\sum_{n=1}^N F(n) = \sum_{k=1}^N f(k)[N/k]$.

k). If N is a positive integer, then: $\sum_{n=1}^N \tau(n) = \sum_{n=1}^N [N/n]$ and $\sum_{n=1}^N \sigma(n) = \sum_{n=1}^N n \cdot [N/n]$. (**Hint:** Use $\tau(n) = \sum_{d|n} 1$, $\sigma(n) = \sum_{d|n} d$ and the part j).)

l). If N is a positive integer, then: $N = \sum_{n=1}^{2N} \tau(n) = \sum_{n=1}^N [2N/n]$ and $\tau(N) = \sum_{n=1}^N ([N/n] - [(N-1)/n])$. (**Hint:** Use the part k).)

3). (Liouville's λ-function) Let λ be the arithmetic function defined by $\lambda(1) = 1$ and $\lambda(n) = (-1)^{m_1 + m_2 + \cdots + m_r}$, where $n \in \mathbb{N}^*$, $n > 1$ and $n = p_1^{m_1} \cdots p_r^{m_r}$ is the canonical prime factorisation of n. Then λ is multiplicative and $\sum_{d|n} \lambda(d) = \begin{cases} 1, & \text{if } n \text{ is a square, i.e., } n = m^2 \text{ for some } m \in \mathbb{N}^*, \\ 0, & \text{otherwise.} \end{cases}$

4). (Euler's φ-function) For $n \in \mathbb{N}^*$, let $\varphi(n)$ denote the number of positive natural numbers $\le n$ that are relatively prime to n, i.e., $\varphi(n) = \text{card}\,(k \in \{1, 2, , \ldots, n\} \mid \gcd(k, n) = 1\})$. Then

a). If p is prime and $m \in \mathbb{N}^*$, then $\varphi(p^m) = p^m - p^{m-1} = p^m(1 - \frac{1}{p})$.

b). φ is multiplicative.

c). If $n \in \mathbb{N}^*$, $n > 1$ and $n = p_1^{m_1} \cdots p_r^{m_r}$ is the canonical prime factorisation of n, then

$$\varphi(n) = \prod_{i=1}^r \left(p_i^{m_i} - p_i^{m_i - 1}\right) = n \cdot \left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_r}\right).$$

d). For $n \in \mathbb{N}^*$, show that: (i) if $n > 2$, then $\varphi(n)$ is an even integer.

(ii) if n is odd, then $\varphi(2n) = \varphi(n)$.

(iii) if $n > 2$ is even, then $\varphi(2n) = 2\varphi(n)$.

(iv) if $\varphi(3n) = 3\varphi(n) \iff 3|n$.

(v) if $\varphi(3n) = 2\varphi(n) \iff 3 \not| n$.

(vi) if $\varphi(n) = n/2 \iff n = 2^k$ for some $k \in \mathbb{N}^*$.

(vii) $\frac{1}{2}\sqrt{n} \le \varphi(n) \le n$.

(viii) if $n > 1$ and has r distinct prime factors, then $n/2^r \le \varphi(n)$.

(ix) if $n > 1$ is a composite number, then $\varphi(n) \le n - \sqrt{n}$. (**Hint:** If p is the smallest prime divisor of n with $p \le \sqrt{n}$, then $\varphi(n) \le n(1 - 1/p)$.)

(x) if $n > 1$ and has r distinct odd prime factors, then $2^r|\varphi(n)$.

(xi) if $m \in \mathbb{N}^*$ and every prime divisor of n also divides m, then $\varphi(nm) = n\varphi(m)$. In particular, $\varphi(n^2) = n\varphi(n)$.

[†] **Euclid of Alexandria** was born about 325 BC and died about 265 BC in Alexandria, Egypt. Euclid of Alexandria is the most prominent mathematician of antiquity best known for his treatise on mathematics The Elements. The long lasting nature of The Elements must make Euclid the leading mathematics teacher of all time. However little is known of Euclid's life except that he taught at Alexandria in Egypt. Proclus, the last major Greek philosopher, who lived around 450 AD wrote :

Not much younger than these [pupils of Plato] is Euclid, who put together the "Elements", arranging in order many of Eudoxus's theorems, perfecting many of Theaetetus's, and also bringing to irrefutable demonstration the things which had been only loosely proved by his predecessors. This man lived in the time of the first Ptolemy; for Archimedes, who followed closely upon the first Ptolemy makes mention of Euclid, and further they say that Ptolemy once asked him if there were a shorted way to study geometry than the Elements, to which he replied that there was no royal road to geometry. He is therefore younger than Plato's circle, but older than Eratosthenes and Archimedes; for these were contemporaries, as Eratosthenes somewhere says. In his aim he was a Platonist, being in sympathy with this philosophy, whence he made the end of the whole "Elements" the construction of the so-called Platonic figures.

There is other information about Euclid given by certain authors but it is not thought to be reliable. Two different types of this extra information exists. The first type of extra information is that given by Arabian authors who state that Euclid was the son of Naucrates and that he was born in Tyre. It is believed by historians of mathematics that this is entirely fictitious and was merely invented by the authors.

The second type of information is that Euclid was born at Megara. This is due to an error on the part of the authors who first gave this information. In fact there was a Euclid of Megara, who was a philosopher who lived about 100 years before the mathematician Euclid of Alexandria. It is not quite the coincidence that it might seem that there were two learned men called Euclid. In fact Euclid was a very common name around this period and this is one further complication that makes it difficult to discover information concerning Euclid of Alexandria since there are references to numerous men called Euclid in the literature of this period.

Returning to the quotation from Proclus given above, the first point to make is that there is nothing inconsistent in the dating given. However, although we do not know for certain exactly what reference to Euclid in Archimedes' work Proclus is referring to, in what has come down to us there is only one reference to Euclid and this occurs in On the sphere and the cylinder. The obvious conclusion, therefore, is that all is well with the argument of Proclus and this was assumed until challenged by Hjelmslev in [48]. He argued that the reference to Euclid was added to Archimedes book at a later stage, and indeed it is a rather surprising reference. It was not the tradition of the time to give such references, moreover there are many other places in Archimedes where it would be appropriate to refer to Euclid and there is no such reference. Despite Hjelmslev's claims that the passage has been added later, Bulmer-Thomas writes :

Although it is no longer possible to rely on this reference, a general consideration of Euclid's works ... still shows that he must have written after such pupils of Plato as Eudoxus and before Archimedes.

This is far from an end to the arguments about Euclid the mathematician. The situation is best summed up by Itard who gives three possible hypotheses.

(i) Euclid was an historical character who wrote the Elements and the other works attributed to him.

(ii) Euclid was the leader of a team of mathematicians working at Alexandria. They all contributed to writing the 'complete works of Euclid', even continuing to write books under Euclid's name after his death.

(iii) Euclid was not an historical character. The 'complete works of Euclid' were written by a team of mathematicians at Alexandria who took the name Euclid from the historical character Euclid of Megara who had lived about 100 years earlier.

It is worth remarking that Itard, who accepts Hjelmslev's claims that the passage about Euclid was added to Archimedes, favours the second of the three possibilities that we listed above. We should, however, make some comments on the three possibilities which, it is fair to say, sum up pretty well all possible current theories.

There is some strong evidence to accept (i). It was accepted without question by everyone for over 2000 years and there is little evidence which is inconsistent with this hypothesis. It is true that there are differences in style between some of the books of the Elements yet many authors vary their style. Again the fact that Euclid undoubtedly based the Elements on previous works means that it would be rather remarkable if no trace of the style of the original author remained.

Even if we accept (i) then there is little doubt that Euclid built up a vigorous school of mathematics at Alexandria. He therefore would have had some able pupils who may have helped out in writing the books. However hypothesis (ii) goes much further than this and would suggest that different books were written by different mathematicians. Other than the differences in style referred to above, there is little direct evidence of this.

Although on the face of it (iii) might seem the most fanciful of the three suggestions, nevertheless the 20th century example of Bourbaki shows that it is far from impossible. Henri Cartan, André Weil, Jean Dieudonné, Claude Chevalley, and Alexander Grothendieck wrote collectively under the name of Bourbaki and Bourbaki's Eléments de mathématiques contains more than 30 volumes. Of course if (iii) were the correct hypothesis then Apollonius, who studied with the pupils of Euclid in Alexandria, must have known there was no person 'Euclid' but the fact that he wrote : .... *Euclid did not work out the syntheses of the locus with respect to three and four lines, but only a chance portion of it ...*

certainly does not prove that Euclid was an historical character since there are many similar references to Bourbaki by mathematicians who knew perfectly well that Bourbaki was fictitious. Nevertheless the mathematicians who made up the Bourbaki team are all well known in their own right and this may be the greatest argument against hypothesis (iii) in that the 'Euclid team' would have to have consisted of outstanding mathematicians. So who were they?

We shall assume in this article that hypothesis (i) is true but, having no knowledge of Euclid, we must concentrate on his works after making a few comments on possible historical events. Euclid must have studied in Plato's Academy in Athens to have learnt of the geometry of Eudoxus and Theaetetus of which he was so familiar.

None of Euclid's works have a preface, at least none has come down to us so it is highly unlikely that any ever existed, so we cannot see any of his character, as we can of some other Greek mathematicians, from the nature of their prefaces. Pappus writes that Euclid was : *... most fair and well disposed towards all who were able in any measure to advance mathematics, careful in no way to give offence, and although an exact scholar not vaunting himself.*

Some claim these words have been added to Pappus, and certainly the point of the passage (in a continuation which we have not quoted) is to speak harshly (and almost certainly unfairly) of Apollonius. The picture of Euclid drawn by Pappus is, however, certainly in line with the evidence from his mathematical texts. Another story told by Stobaeus is the following : *... someone who had begun to learn geometry with Euclid, when he had learnt the first theorem, asked Euclid "What shall I get by learning these things?" Euclid called his slave and said "Give him threepence since he must make gain out of what he learns".*

Euclid's most famous work is his treatise on mathematics The Elements. The book was a compilation of knowledge that became the centre of mathematical teaching for 2000 years. Probably no results in The Elements were first proved by Euclid but the organisation of the material and its exposition are certainly due to him. In fact there is ample evidence that Euclid is using earlier textbooks as he writes the Elements since he introduces quite a number of definitions which are never used such as that of an oblong, a rhombus, and a rhomboid.

The Elements begins with definitions and five postulates. The first three postulates are postulates of construction, for example the first postulate states that it is possible to draw a straight line between any two points. These postulates also implicitly assume the existence of points, lines and circles and then the existence of other geometric objects are deduced from the fact that these exist. There are other assumptions in the postulates which are not explicit. For example it is assumed that there is a unique line joining any two points. Similarly postulates two and three, on producing straight lines and drawing circles, respectively, assume the uniqueness of the objects the possibility of whose construction is being postulated.

The fourth and fifth postulates are of a different nature. Postulate four states that all right angles are equal. This may seem "obvious" but it actually assumes that space in homogeneous - by this we mean that a figure will be independent of the position in space in which it is placed. The famous fifth, or parallel, postulate states that one and only one line can be drawn through a point parallel to a given line. Euclid's decision to make this a postulate led to Euclidean geometry. It was not until the 19th century that this postulate was dropped and non- euclidean geometries were studied.

There are also axioms which Euclid calls 'common notions'. These are not specific geometrical properties but rather general assumptions which allow mathematics to proceed as a deductive science. For example : Things which are equal to the same thing are equal to each other.

Zeno of Sidon, about 250 years after Euclid wrote the Elements, seems to have been the first to show that Euclid's propositions were not deduced from the postulates and axioms alone, and Euclid does make other subtle assumptions.

The Elements is divided into 13 books. Books one to six deal with plane geometry. In particular books one and two set out basic properties of triangles, parallels, parallelograms, rectangles and squares. Book three studies properties of the circle while book four deals with problems about circles and is thought largely to set out work of the followers of Pythagoras. Book five lays out the work of Eudoxus on proportion applied to commensurable and incommensurable magnitudes. Heath says : *Greek mathematics can boast no finer discovery than this theory, which put on a sound footing so much of geometry as depended on the use of proportion.*

Book six looks at applications of the results of book five to plane geometry. Books seven to nine deal with number theory. In particular book seven is a self-contained introduction to number theory and contains the Euclidean algorithm for finding the greatest common divisor of two numbers. Book eight looks at numbers in geometrical progression but van der Waerden writes that it contains : *... cumbersome enunciations, needless repetitions, and even logical fallacies. Apparently Euclid's exposition excelled only in those parts in which he had excellent sources at his disposal.*

Book ten deals with the theory of irrational numbers and is mainly the work of Theaetetus. Euclid changed the proofs of several theorems in this book so that they fitted the new definition of proportion given by Eudoxus.

Books eleven to thirteen deal with three-dimensional geometry. In book thirteen the basic definitions needed for the three books together are given. The theorems then follow a fairly similar pattern to the two- dimensional analogues previously given in books one and four. The main results of book twelve are that circles are to one another as the squares of their diameters and that spheres are to each other as the cubes of their diameters. These results are certainly due to Eudoxus. Euclid proves these theorems using the "method of exhaustion" as invented by Eudoxus. The Elements ends with book thirteen which discusses the properties of the five regular polyhedra and gives a proof that there are precisely five. This book appears to be based largely on an earlier treatise by Theaetetus.

Euclid's Elements is remarkable for the clarity with which the theorems are stated and proved. The standard of rigour was to become a goal for the inventors of the calculus centuries later. As Heath writes : *This wonderful book, with all its imperfections, which are indeed slight enough when account is taken of the date it appeared, is and will doubtless remain the greatest mathematical textbook of all time. ... Even in Greek times the most accomplished mathematicians occupied themselves with it: Heron, Pappus, Porphyry, Proclus and Simplicius wrote commentaries; Theon of Alexandria re-edited it, altering the language here and there, mostly with a view to greater clearness and consistency...*

It is a fascinating story how the Elements has survived from Euclid's time and this is told well by Fowler. He describes the earliest material relating to the Elements which has survived : *Our earliest glimpse of Euclidean material will be the most remarkable for a thousand years, six fragmentary ostraca containing text and a figure ... found on Elephantine Island* *in 1906/07 and 1907/08... These texts are early, though still more than 100 years after the death of Plato (they are dated on palaeographic grounds to the third quarter of the third century BC); advanced (they deal with the results found in the "Elements"* [book thirteen] *... on the pentagon, hexagon, decagon, and icosahedron); and they do not follow the text of the Elements. ... So they give evidence of someone in the third century BC, located more than 500 miles south of Alexandria, working through this difficult material... this may be an attempt to understand the mathematics, and not a slavish copying ...*

The next fragment that we have dates from 75 - 125 AD and again appears to be notes by someone trying to understand the material of the Elements.

More than one thousand editions of The Elements have been published since it was first printed in 1482. Heath discusses many of the editions and describes the likely changes to the text over the years.

B L van der Waerden assesses the importance of the Elements : *Almost from the time of its writing and lasting almost to the present, the Elements has exerted a continuous and major influence on human affairs. It was the primary source of geometric reasoning, theorems, and methods at least until the advent of non-Euclidean geometry in the 19th century. It is sometimes said that, next to the Bible, the "Elements" may be the most translated, published, and studied of all the books produced in the Western world.*

Euclid also wrote the following books which have survived: Data (with 94 propositions), which looks at what properties of figures can be deduced when other properties are given; On Divisions which looks at constructions to divide a figure into two parts with areas of given ratio; Optics which is the first Greek work on perspective; and Phaenomena which is an elementary introduction to mathematical astronomy and gives results on the times stars in certain positions will rise and set. Euclid's following books have all been lost: Surface Loci (two books), Porisms (a three book work with, according to Pappus, 171 theorems and 38 lemmas), Conics (four books), Book of Fallacies and Elements of Music. The Book of Fallacies is described by Proclus :

Since many things seem to conform with the truth and to follow from scientific principles, but lead astray from the principles and deceive the more superficial, [Euclid] has handed down methods for the clear- sighted understanding of these matters also ... The treatise in which he gave this machinery to us is entitled Fallacies, enumerating in order the various kinds, exercising our intelligence in each case by theorems of all sorts, setting the true side by side with the false, and combining the refutation of the error with practical illustration.

Elements of Music is a work which is attributed to Euclid by Proclus. We have two treatises on music which have survived, and have by some authors attributed to Euclid, but it is now thought that they are not the work on music referred to by Proclus.

Euclid may not have been a first class mathematician but the long lasting nature of The Elements must make him the leading mathematics teacher of antiquity or perhaps of all time.