Lecture Notes

To understand and appreciate the text which is (in dark-violet colour) marked with the symbol † one may possibly require more mathematical maturity than one has! These are steps towards applications to various other branches of mathematics, especially to Analysis and Number Theory.

There is a dictum that anyone who desires to get at the roots of the subject should study its history. Endorsing this, the pain is taken to fit historical remarks in the text whenever possible.

The *Theory of Numbers* is concerned with properties on integers and more particularly with the positive integers (also known as the positive *natural numbers*) $1, 2, 3, \ldots$. The origin of this misnomer harks back to the early Greeks for whom the *number* meant positive integer and nothing else. Far from being a gift from Heaven, number theory has had a long and sometimes painful evolution.

– Few words about the origin of number theory: The Theory of Numbers is one of the oldest branches of mathematics; its roots goes back to remote date. The Greeks were largely indebted to the Babylonians and ancient Egyptians for a core of information about the properties of natural numbers, the first rudiments of this theory are generally credited to Pythagoras[10] and his disciples.

P l a t o[11] said "God is a geometer" – J a c o b i[12] changed this to "God is a arithmatician". Then came K r o n e c k e r[13] and fashioned the memorable expression "God created the natural numbers and all the rest is the work of man". **F e l i x K l e i n[14] (1849-1925)**

T5.1 (The set of Natural numbers -- Peano's axioms Natural numbers cane be defined axiomatically as follows:

[10] P y t h a g o r a s o f S a m o s (born between 580 BC and 562 BC) was an Ionian Greek philosopher, mathematician, and founder of the religious movement called *Pythagoreanism*. Most of the information about Pythagoras was written down centuries after he lived, so very little reliable information is known about him. He was born on the island of Samos, and might have traveled widely in his youth, visiting Egypt and other places seeking knowledge. Around 530 BC, he moved to Croton, a Greek colony in southern Italy, and there set up a religious sect. The school concentrated on four *mathemata* or subjects of stud: *arithmetica* (arithmetic – Number theory rather than the art of calculating), *harmonia* (music), *geometria* (geometry) and *astrology* (astronomy). This fourfold division of knowledge became known in the Middle Ages as the *quadrivium* to which was added the *trivium* of logic, grammar and rhetoric. These seven liberal arts came to be looked upon as the necessary course of study of an educated person.

Pythagoras made influential contributions to philosophy and religious teaching in the late 6-th century BC. He is often revered as a great mathematician, mystic and scientist, but he is best known for the Pythagorean theorem which bears his name. The society took an active role in the politics of Croton, but this eventually led to their downfall. The Pythagorean meeting-places were burned, and Pythagoras was forced to flee the city. He is said to have ended his days in Metapontum.

[11] P l a t o (427 BC-347 BC) is one of the most important Greek philosophers. He founded the Academy in Athens, an institution devoted to research and instruction in philosophy and the sciences. His works on philosophy, politics and mathematics were very influencial and laid the foundations for Euclid's systematic approach to mathematics.

[12] C a r l G u s t a v J a c o b J a c o b i (1804-1851) made basic contributions to the theory of elliptic functions. He carried out important research in partial differential equations of the first order and applied them to the differential equations of dynamics.

[13] L e o p o l d K r o n e c k e r (1823-1891) was a German mathematician. His primary contributions were in the theory of equations. He made major contributions in elliptic functions and the theory of algebraic numbers.

[14] F e l i x C h r i s t i a n K l e i n (1849-1925) was a German mathematician. Felix Klein's synthesis of geometry as the study of the properties of a space that are invariant under a given group of transformations, known as the Erlanger Programm, profoundly influenced mathematical development.

A set of natural numbers $\mathbb{N}$ is a set with special element 0 and there is a map $s : \mathbb{N} \to \mathbb{N} \setminus \{0\}$ satisfying the following properties:

(P_1) s is injective.

(P_2) (Induction-Axiom) Suppose that $M \subseteq \mathbb{N}$ is a subset such that $0 \in M$ and if $n \in M$, then $s(n) \in M$. Then $M = \mathbb{N}$.

(**Remark :** These axioms are known as Peano's axioms and were introduced by Giuseppe Peano[15] in the "*Arithmetices Principia*", Torino, 1889. Peano also showed how one can derive the entire arithmetic using these axioms.)

The axiom P_2 is called the axiom of induction or induction-axiom. From this axiom it follows that the map $s : \mathbb{N} \to \mathbb{N} \setminus \{0\}$ is surjective and hence it is bijective. Instead of $0, s(0), s(s(0)), s(s(s(0))), \ldots,$, one can simply write $0, 1, 2, 3, \ldots,$.

With this one can immediately ask the following two fundamental questions:

(1) Does there exists such a system $(\mathbb{N}, 0, s)$ which satisfy the axioms P_1 and P_2, i. e. a model for natural numbers.

(2) If answer to the question (1) is yes, then ow many such models are there?

For these questions we consider the following concept (due to Dedekind) :

A set X is called (simple) infinite if there exists an injective map $f : X \to X$ which is not surjective. Then clearly (if it exists!) the set $\mathbb{N}$ of natural numbers is a "smallest" simple infinite set. More deeper is the following theorem due to Dedekind: *There exists a unique simple infinite set which is a model* $(\mathbb{N}, 0, s)$ *for the set of natural numbers.* We shall indicate the existence here and the uniqueness is precisely formulated in T5.9.

Start with the emptyset $\emptyset$ and put:

$0 := \emptyset,$
$1 := \{\emptyset\} = \{0\} = 0^+,$
$2 := \{\emptyset\} \cup \{\{\emptyset\}\} = \{0, 1\} = 1^+,$
$3 := \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\} = \{0, 1, 2\} = 2^+$
and so on ... $n := \{0, 1, 2, \ldots, n-1\} = (n-1)^+.$

Now, take $\mathbb{N} := \{0, 1, 2, \ldots\}$ and define $s : \mathbb{N} \to \mathbb{N}$ by $s(n) := n^+ = n \cup \{n\} = \{0, 1, 2, \ldots, n\}$. It is easy to check that $(\mathbb{N}, 0, s)$ satisfies the Peano's axioms P_1 and P_2.

In terms of *immediate successors* the above can be written as: 1 is the immediate successor of 0, 2 is the immediate successor of 1, ..., n^+ is the immediate successor of n for every $n \in \mathbb{N}$. Moreover, there is a unique relation $\leq$ on $\mathbb{N}$ (actually it is the inclusion relation $\subseteq$) which a total order on $\mathbb{N}$ with the smallest element 0. (**Remark :** This unique order $\leq$ on $\mathbb{N}$ is called the standard or usual order on $\mathbb{N}$. In T5.2-(b) below, we shall prove that the ordered set $(\mathbb{N}, \leq)$ is well-ordered, i. e. every non-empty subset $M \subseteq \mathbb{N}$ has the smallest element (in M).)

T5.2 We use the Induction-axiom to prove its following consequences:

(a) (First principle of induction) Using the third axiom of Peano prove the following : *Suppose that for each natural number* $n \in \mathbb{N}$*, we have associated a statement* $S(n)$*. Assume that the following conditions are satisfied* :

(i) $S(0)$ *is true.* The (Basis of Induction)

[15] Giuseppe Peano (1858-1932) was an Italian mathematician born on 27 August 1858 and died on 20 April 1932, whose work was of exceptional philosophical value. The author of over 200 books and papers, he was a founder of mathematical logic and set theory, to which he contributed much notation. The standard axiomatization of the natural numbers is named in his honor. As part of this axiomatization effort, he made key contributions to the modern rigorous and systematic treatment of the method of mathematical induction. He spent most of his career teaching mathematics at the University of Turin, Italy.

(ii) *For every* $n \in \mathbb{N}$, $S(n+1)$ *is true whenever* $S(n)$ *is true.* The (Inductive step) *Then* $S(n)$ *is true for all* $n \in \mathbb{N}$. (**Hint :** Let $M := \{n \in \mathbb{N} \mid S(n) \text{ is true}\} \subseteq \mathbb{N}$. Then $0 \in M$ by the hypothesis (i). Furher, by hypothesis (ii) if $n \in M$, then $n+1 \in M$. Therefore $M = \mathbb{N}$ by the induction-axiom. – **Remark:** The following variant is also used very often: *Let* $n_0 \in \mathbb{N}$. *Suppose that for every natural number* $n \geq n_0$, *we have associated a statement* $S(n)$. *Assume that* $S(n_0)$ *is true and for every* $n \geq n_0$, $S(n+1)$ *is true whenever* $S(n)$ *is true. Then* $S(n)$ *is true for all* $n \geq n_0$. For the proof consider the set $M := \{n \in \mathbb{N} \mid n < n_0\} \cup \{n \in \mathbb{N} \mid n \geq n_0 \text{ and } S(n) \text{ is true }\}$.)

(b) (Minimum Principle or well Ordering Principle) *Every non-empty subset* M *of* $\mathbb{N}$ *has a smallest element*, i.e., *there exists an element* $m_0 \in M$ *such that* $m_0 \leq m$ *for all* $m \in M$. (**Hint :** For $n \in \mathbb{N}$, let $S(n)$ be the following statement: *If* M *contains a natural number* m *with* $m \leq n$, *then* M *has a smallest element.* By using induction show that the statement $S(n)$ is true for all n. – **Remark:** The minimum principle for $\mathbb{N}$ is also known as the well-ordering property of $\mathbb{N}$. Moreover, well-ordering property of $\mathbb{N}$ is equivalent to the induction-axiom, see the part (c) below.)

(c) Deduce the induction-axiom from the well-ordering property of $\mathbb{N}$. (**Hint :** Suppose that $M \subseteq \mathbb{N}$ such that $0 \in M$ and if $n \in M$, then $n+1 \in M$. To prove that $M = \mathbb{N}$ or equivalently to prove that the complement $\mathbb{N} \setminus M = \emptyset$. If $\mathbb{N} \setminus M \neq \emptyset$, then by the minimal principle, it has a smallest element say n_0, i. e. $n_0 \in \mathbb{N} \setminus M$ and $n_0 \leq n$ for every $\mathbb{N} \setminus M$. But then $n_0 - 1 \in M$ and $n_0 \notin M$ a contradiction to the hypothesis in the induction-axiom.)

(d) (Archimedean Property) For every pair of positive natural numbers a and b, there exists a positive natural number $n \in \mathbb{N}^*$ such that $n \cdot b \geq b$. (**Remark :** Note that we have assumed that the binary operations $+$, $\cdot$ and the order relation $\leq$ are defined on $\mathbb{N}$, see T5.8. Further, for $x, y \in \mathbb{N}$, note that $x \leq y$ if $y = x + z$ for some $z \in \mathbb{N}$. – **Hint:** Suppose that $b < n \cdot a$ for every $n \in \mathbb{N}$. Then $M := \{b - na \mid n \in \mathbb{N}\} \subseteq \mathbb{N}$ and clearly $b \in M$. Therefore by the Minimum Principle M has a smallest element, say $b - m \cdot a$. But then $b - (m+1) \cdot a \in M$ also and $b - (m+1) \cdot a = b - m \cdot a - a < b - m \cdot a$ a contradiction to the minimality of $b - m \cdot a$.)

(e) (Second principle of induction) *Suppose that for each natural number* $n \in \mathbb{N}$, *we have associated a statement* $S(n)$. *Assume that for every* $n \in \mathbb{N}$, *if the* $S(m)$ *is true for all* $m < n$, *then* $S(n)$ *is also true. Then* $S(n)$ *is true for all* $n \in \mathbb{N}$. (**Hint :** Let $M := \{n \in \mathbb{N} \mid S(n) \text{ is NOT true}\} \subseteq \mathbb{N}$. Then show that $M = \emptyset$.)

T5.3 (Some Arithmetic series) For all $n \in \mathbb{N}$, prove the following formulas by induction :

(a) $\displaystyle\sum_{k=1}^{n} k = \frac{n(n+1)}{2}$. **(b)** $\displaystyle\sum_{k=1}^{n} k^2 = \frac{n(n+1)(2n+1)}{6}$. **(c)** $\displaystyle\sum_{k=1}^{n} k^3 = \Big(\frac{n(n+1)}{2}\Big)^2 = \Big(\sum_{k=1}^{n} k\Big)^2$.

(d) $\displaystyle\sum_{k=1}^{n} (-1)^{k-1} k = \frac{1}{4}\big(1 + (-1)^{n-1}(2n+1)\big)$. **(e)** $\displaystyle\sum_{k=1}^{n} (-1)^{k-1} k^2 = (-1)^{n+1} \cdot \frac{n(n+1)}{2}$.

(f) $\displaystyle\sum_{k=1}^{n} (2k-1) = n^2$. **(g)** $\displaystyle\sum_{k=1}^{n} (2k-1)^2 = \frac{n}{3}(4n^2 - 1)$. **(h)** $\displaystyle\sum_{k=1}^{n} k(k+1) = \frac{1}{3} n(n+1)(n+2)$.

(i) $\displaystyle\sum_{k=1}^{n} \frac{1}{k(k+1)} = 1 - \frac{1}{n+1}$. **(j)** $\displaystyle\sum_{k=1}^{n} \frac{1}{4k^2 - 1} = \frac{1}{2}\Big(1 - \frac{1}{2n+1}\Big)$.

(k) $\displaystyle\sum_{k=1}^{n} \frac{1}{k(k+1)(k+2)} = \frac{1}{4} - \frac{1}{2(n+1)(n+2)}$. **(l)** $\displaystyle\sum_{k=1}^{n} \frac{k-1}{k(k+1)(k+2)} = \frac{1}{4} - \frac{2n+1}{2(n+1)(n+2)}$.

T5.4 For all $n \geq 1$ prove:

(a) $\displaystyle\prod_{k=2}^{n} \Big(1 - \frac{1}{k^2}\Big) = \frac{1}{2}\Big(1 + \frac{1}{n}\Big)$. **(b)** $\displaystyle\prod_{k=2}^{n} \Big(1 - \frac{2}{k(k+1)}\Big) = \frac{1}{3}\Big(1 + \frac{2}{n}\Big)$.

(c) $\displaystyle\prod_{k=2}^{n}\frac{k^3-1}{k^3+1}=\frac{2}{3}\Big(1+\frac{1}{n(n+1)}\Big)$.

T5.5 (Finite geometric series) For every real (or complex) number $q\neq 1$ and every $n\in\mathbb{N}$, prove that : **(a)** $\sum_{k=0}^{n}q^k=\frac{q^{n+1}-1}{q-1}$ **(b)** $\displaystyle\prod_{k=0}^{n}(1+q^{2^k})=\frac{q^{2^{n+1}}-1}{q-1}$. **(c)** $\displaystyle\sum_{k=1}^{n}kq^k=\frac{nq^{n+2}-(n+1)q^{n+1}+q}{(q-1)^2}$.

T5.6 For all $n\geq 1$ prove:

(a) 5 divides $2^{n+1}+3\cdot 7^n$. **(b)** 3 divides n^3+2n. **(c)** 6 divides n^3-n.

(d) 7 divides $5^{2n+1}+2^{2n+1}$. **(e)** 30 divides n^5-n. **(f)** 3 divides $2^{2n}-1$.

(g) 15 divides $3n^5+5n^3+7n$. **(h)** 133 divides $11^{n+2}+12^{2n+1}$. **(i)** 5 divides $3^{n+1}+2^{3n+1}$.

T5.7 Proofs by induction are very common in Mathematics and are undoubtedly familiar to the reader. One also encounters quite frequently – without being conscious of it – definitions by induction or recursion. For example, powers of a non-zero real number a^n are defined by $a^0=1, a^{r+1}=a^r a$. Definition by induction is not as trivial as it may appear at first glance. This can be made precise by the following well-known recursion theorem proved by Dedekind[16] :

(a) (Recursion Theorem) *Let X be a non-empty set and let $F:X\to X$ be a map. For $a\in X$, there exists a unique (sequence in X) map $f:\mathbb{N}\longrightarrow X$ such that* (i) $f(0)=a$ *and* (ii) $f(s(n))=F(f(n))$ *for all $n\in\mathbb{N}$, i.e., the following diagram is commutative.*

$$\begin{array}{ccc}\mathbb{N} & \xrightarrow{\ s\ } & \mathbb{N}\\ {\scriptstyle f}\downarrow & & \downarrow{\scriptstyle f}\\ X & \xrightarrow{\ F\ } & X\end{array}$$

(**Hint :** Uniqueness of f is clear by induction. For existence, put $I_n:=\{0,1,\ldots,n\}$. By induction show that the following statement $\mathrm{S}(n)$ is true for all $n\in\mathbb{N}$. $\mathrm{S}(n)$: *There exists a unique map $f_n:I_n\to X$ such that $f_n(0)=a$ and $f_n(r+1)=F(f_n(r))$ for every $r\in\mathbb{N}$ with $r<n$.* For arbitrary natural numbers $m,n\in\mathbb{N}$ with $m\leq n$, we then have $f_m=f_n|I_m$. Therefore $f_n(n)=F(f_n(n-1))=F(f_{n-1}(n-1))$ for all $n\geq 1$. Now, define f by $n\mapsto f_n(n)$.) (**Remark :** One might be tempted to say that one can *define* inductively by conditions (i) and (ii). However, this does not make sense since in talking about a function on $\mathbb{N}$ we must have an à priori definition of $f(n)$ for every $n\in\mathbb{N}$. A proof of the existence of f must use *all* of Peano's axioms. See the example illustrating this in the part (b) below.)

(b) (Henkin) Let $N=\{0,1\}$ and define the map $s_N:N\to N$ by $s_N(0):=1$ and $s_N(1):=1$. Show that (N,s_N) satisfies Peano's axioms P_2 but not P_1. Show that the recursion theorem breaks down for (N,s_N). (**Hint :** Let $F:N\to N$ be the map defined by $F(0)=1$ and $F(1)=0$. Show that there is no map $f:N\to N$ satisfying $f(0)=0$ and $f(s_N(a))=F(f(a))$ for all $a\in N$.)

(c) (Iteration of maps) Let X be a set, $\Phi:X\to X$ be a map, i.e., $\Phi\in X^X$. and let $F:X^X\to X^X$ be the map defined by $\Psi\mapsto\Phi\circ\Psi$. Then there exists a sequence $f:\mathbb{N}\to X^X$

[16] Julius Wilhelm Richard Dedekind (October 6, 1831 - February 12, 1916) was a German mathematician who did important work in abstract algebra (particularly ring theory), algebraic number theory and the foundations of the real numbers. Dedekind was one of the greatest mathematicians of the nineteenth-century, as well as one of the most important contributors to number theory and algebra of all time. Any comprehensive history of mathematics will mention him for his invention of the theory of ideals and his investigation of the notions of algebraic number, field, module, lattice, etc. Often acknowledged are: his analysis of the notion of continuity, his introduction of the real numbers by means of Dedekind cuts, his formulation of the Dedekind-Peano axioms for the natural numbers, his proof of the categoricity of these axioms, and his contributions to the early development of set theory.

in X^X such that $f(0) = \mathrm{id}_X$ and $f(n+1) = F(f(n)) = \Phi \circ f(n)$ for all $n \in \mathbb{N}$. For $n \in \mathbb{N}$ the map $f(n) : X \to X$ is called the n-th iterate of Φ and is denoted by Φ^n. Note that $\Phi^0 = \mathrm{id}_X, \Phi^{n+1} = \Phi^n \circ \Phi$ for all $n \in \mathbb{N}$. Further, $(\mathrm{id}_X)^n = \mathrm{id}_X$ for $n \in \mathbb{N}$.

(d) Let X be a set, $a \in X$, $Y := \bigcup_{n\in\mathbb{N}} X^n$ and let $G : Y \to X$ be a map. Then there exists a unique sequence $g : \mathbb{N} \to X$ such that $, g(0) = a$ and $g(n+1) = G(g(0), g(1), \ldots, g(n))$ for all $n \in \mathbb{N}$. (**Hint :** Define the map $F : Y \to Y$ be $(x_1, \ldots, x_n) \mapsto (x_1, \ldots, x_n, G((x_1, \ldots, x_n)))$. Then by recursion theorem there exists a unique map $f : \mathbb{N} \to Y$ such that $f(0) = a$ and $f(n+1) = F(f(n))$ for all $n \in \mathbb{N}$. Now, define $g : \mathbb{N} \to X$ by $n \mapsto f(n)(n)$.)

T5.8 (Addition, Multiplication and Exponentiation in $\mathbb{N}$) Let $(\mathbb{N}, 0, s)$ of a set natural numbers (defined in T5.1).

(a) The binary operations addition $+ : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ and the multiplication $\cdot : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ on $\mathbb{N}$ can be defined by using the recursion theorem. Further, one can verify the standard properties $+$ and $\cdot$. For example, existence of identity element, associativity, commutativity, distributive laws, cancelation laws, monotonicity (with respect to the standard order $\leq$ etc. (**Hint :** For $+$ apply recursion theorem to $X = \mathbb{N}$ $F = s$ and $a = m \in \mathbb{N}$ to get the unique map $s_m : \mathbb{N} \to \mathbb{N}$ such that $s_m(0) = m$ and $s_m(s(n)) = s(s_m(n)$ for all $n \in \mathbb{N}$. Now, define $m + n := s_m(n)$. Note that $m + 0 = s_m(0) = m$ and $m + s(n) = s_m(s(n)) = s(s_m(n))$. Further, note that for $m \in \mathbb{N}$, the map $s_m : \mathbb{N} \to \mathbb{N}$ is the m-th iterate (see T5.7-(c)) $s^m = \underbrace{s \circ s \circ \cdots \circ s}_{m\text{-times}}$ of the successor map s. For $m, n \in \mathbb{N}$, define the multiplication $m \cdot n := s_n^m(0) = (s^n)^m(0)$.)

(b) There exists a binary operation of exponentiation (or n-th power of m) $\mathbb{N} \times \mathbb{N} \to \mathbb{N}$, $(m, n) \mapsto m^n$. Further, one can state and verify the standard laws of exponents. (**Hint :** For $m \in \mathbb{N}$, let $p_m : \mathbb{N} \to \mathbb{N}$ be the multiplication by m. Define $m^n := p_m^n(1)$.)

T5.9 (Uniqueness of the model $(\mathbb{N}, 0, s)$) Use Recursion Theorem (see T5.7-(a)) to show that the model $(\mathbb{N}, 0, s)$ of a set natural numbers (defined in T5.1) is essentially unique. More precisely: Let $\widetilde{\mathbb{N}}$ be a non-empty set, $\widetilde{0} \in \widetilde{\mathbb{N}}$ and let $\widetilde{s} : \widetilde{\mathbb{N}} \to \widetilde{\mathbb{N}}$ be a map. Suppose that for each map $F : X \to X$ and each $a \in X$, there exists a unique map $\widetilde{f} : \widetilde{\mathbb{N}} \to X$ such that (i) $\widetilde{f}(\widetilde{0}) = a$ and (ii) $\widetilde{f}(\widetilde{s}(n)) = F(\widetilde{f}(n))$ for all $n \in \mathbb{N}$, i.e., the diagram

$$\begin{array}{ccc} \widetilde{\mathbb{N}} & \xrightarrow{\widetilde{s}} & \widetilde{\mathbb{N}} \\ {\scriptstyle \widetilde{f}}\downarrow & & \downarrow{\scriptstyle \widetilde{f}} \\ X & \xrightarrow{F} & X \end{array}$$

is commutative. Then there exists a unique bijective map $\Phi : \mathbb{N} \to \widetilde{\mathbb{N}}$ such that $\Phi(0) = \widetilde{0}$ and $\Phi(s(n)) = \widetilde{s}(\Phi(n))$ for all $n \in \mathbb{N}$, i.e., the diagram

$$\begin{array}{ccc} \mathbb{N} & \xrightarrow{s} & \mathbb{N} \\ {\scriptstyle \Phi}\downarrow & & \downarrow{\scriptstyle \Phi} \\ \widetilde{\mathbb{N}} & \xrightarrow{\widetilde{s}} & \widetilde{\mathbb{N}} \end{array}$$

is commutative.

T5.10 In this exercise we list some more useful formulations of recursions: Let X and Y be sets.

(a) (Double Recursion) Let $a \in X$ and let $F, G : X \to X$ be two maps. Then there exists a unique map $g : \mathbb{N} \times \mathbb{N} \to X$ such that $g((0,0)) = a$, $g((0, n+1)) = F(g(0,n))$ for all $n \in \mathbb{N}$ and $g((m+1, n)) = G(g(m,n))$ for all $m, n \in \mathbb{N}$. Use double recursion to obtain directly the operations of addition $+$ and $\cdot$ on $\mathbb{N}$.

(**Hint :** By Recursion Theorem T5.7-(a) there exists a map $\Psi_0 : \mathbb{N} \to X$ such that $\Psi_0(0) = 0$ and $\Psi_0(n+1) = F(\Psi_0(n))$ for all $n \in \mathbb{N}$. Now, apply once again the Recursion Theorem to the map $\Phi : X^{\mathbb{N}} \to X^{\mathbb{N}}$, $\varphi \mapsto G \circ \varphi$ and $\Psi_0 \in \mathbb{X}^{\mathbb{N}}$, to get the map $\Psi : \mathbb{N} \to X^{\mathbb{N}}$ such that $\Psi(0) = \Psi_0$ and $\Psi(m+1) = \Phi(\Psi(m))$. Finally, define the map $g : \mathbb{N} \times \mathbb{N} \to X$ by $g(m,n) := \Psi(m)(n)$.)

(b) (Simultaneous Recursion) Let $H : X \times Y \to X$, $K : X \times Y \to Y$ be given maps. For $(a,b) \in X \times Y$, there exist a unique maps $f : \mathbb{N} \to X$ and $g : \mathbb{N} \to Y$ such that $f(0) = a$, $g(0) = b$ and $f(n+1) = H(f(n), g(n))$, $g(n+1) = K(f(n), g(n))$ for all $n \in \mathbb{N}$. (**Hint :** Apply Recursion Theorem T5.7-(a) to the set $X \times Y$, the map $F := H \times K : X \times Y \to X \times Y$, $(x,y) \mapsto (H(x,y), K(x,y))$ and $(a,b) \in X \times Y$, to get the map $G : \mathbb{N} \to X \times Y$ such that $G(0) = (a,b)$ and $G(n+1) = F(G(n))$ for all $n \in \mathbb{N}$. Now, take $f = p \circ G$ and $q \circ G$, where $p : X \times Y \to X$ (resp. $q : X \times Y \to Y$) is the first (resp. second) projection. Using the properties of G check that f and g have the required properties.)

(c) (Primitive Recursion) Let $a \in X$ and let $H : X \times \mathbb{N} \to X$ be a given map. Show that there exists a unique map $f : \mathbb{N} \to X$ such that $f(0) = a$ and $f(n+1) = H(f(n), n)$ for all $n \in \mathbb{N}$. (**Hint :** Apply the Simultaneous Recursion to $Y = \mathbb{N}$, $b = 0$ and the map $K : X \times \mathbb{N} \to \mathbb{N}$ defined by $(x,n) \mapsto n+1$.)

(d) (Factorials) Construct a map $f : \mathbb{N} \to \mathbb{N}$ such that $f(0) = 1$ and $f(n) = 1 \cdot 2 \cdots (n-1) \cdot n$ (the product of the first n non-zero natural numbers) for each $n > 0$. (**Hint :** Use the primitive recursion to $X = \mathbb{N}$, $a = 1$ and $H : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ the map defined by $H(m,n) = (n+1) \cdot m$. – **Remark:** For each $n \in \mathbb{N}$, the natural number $F(n)$ is called factorial n and is denoted by $n!$.)

T5.11 (n-ary operations – generalized sums and products) Let $n \in \mathbb{N}$ and let $X^{\{1,\ldots,n\}} := X^n := \underbrace{X \times \cdots \times X}_{n\text{- times}}$. A map $f : X^n \to X$ is called an n-ary operation on X.

Let $* : X \times X \to X$ be a binary operation on X. Then there exists a unique family $f_n : X^n \to X$, $n \in \mathbb{N}^*$ of n-ary operation on X such that : $f_1 = \mathrm{id}_X$, $f_2 = *$ and

$f_{n+1}((x_1,\ldots,x_n,x_{n+1})) = f_n((x_1,\ldots,x_n)) * x_{n+1}$ for all $(x_1,\ldots,x_n,x_{n+1}) \in X^{n+1}$ and for all $n \geq 1$.

(a) Applying the above result to the binary operation of addition $+$ on $\mathbb{N}$, we have a unique family $f_n : \mathbb{N}^n \to X$, $n \in \mathbb{N}^*$ of n-ary operation on $\mathbb{N}$.
For $n \in \mathbb{N}$ and $(x_1,\ldots,x_n) \in \mathbb{N}^n$, $f_n((x_1,\ldots,x_n))$ is denoted by $\sum_{i=1}^n x_i$. Therefore $\sum_{i=1}^0 x_i = 0$ and $\sum_{i=1}^{n+1} x_i = (\sum_{i=1}^n x_i) + x_{n+1}$ for all $(x_1,\ldots,x_n,x_{n+1}) \in \mathbb{N}^{n+1}$ and for all $n \geq 1$.

(b) Applying the above result to the binary operation of multiplication $\cdot$ on $\mathbb{N}$, we have a unique family $p_n : \mathbb{N}^n \to X$, $n \in \mathbb{N}^*$ of n-ary operation on $\mathbb{N}$.
For $n \in \mathbb{N}$ and $(x_1,\ldots,x_n) \in \mathbb{N}^n$, $p_n((x_1,\ldots,x_n))$ is denoted by $\prod_{i=1}^n x_i$. Therefore $\prod_{i=1}^0 x_i = 1$ and $\prod_{i=1}^{n+1} x_i = (\prod_{i=1}^n x_i) + x_{n+1}$ for all $(x_1,\ldots,x_n,x_{n+1}) \in \mathbb{N}^{n+1}$ and for all $n \geq 1$.

(c) For $n \in \mathbb{N}$, $(x_1,\ldots,x_n) \in \mathbb{N}^n$ and any permutation σ of $\{1,\ldots,n\}$, prove that $\sum_{i=1}^n x_i = \sum_{i=1}^n x_{\sigma(i)}$ and $\prod_{i=1}^n x_i = \prod_{i=1}^n x_{\sigma(i)}$.

(d) Applying the above result to the binary operation of composition X^X, we have a unique family $\Phi_n : (X^X)^n \to X^X$, $n \in \mathbb{N}^*$ of n-ary operation on X^X. For $n \in \mathbb{N}$ and $(f_1,\ldots,f_n) \in (X^X)^n$, $\Phi_n((f_1,\ldots,f_n))$ is denoted by $f_1 \circ f_2 \circ \circ f_n$. In particular, if $f_i = f$ for every $i \geq 1$, then for $n \geq 1$ $\Phi_n((f,f,\ldots,f)) = f^n$ is the n-th iterate of f (see also T5.7-(c)).)

T5.12 (Division Algorithm) 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 Minimum

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 $b\big|(r-r')$. 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 $q' = q$.)

T5.13 (Divisibility) An integer d is called a divisor of $a \in \mathbb{Z}$ in $\mathbb{Z}$, and is denoted by $d\big|a$, 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 $d \not| a$. If $0 \neq d$ is a divisor of a, then $v \in \mathbb{Z}$ in the equation $a = dv$ is uniquely determined by the cancelation law. An integer $a, \in \mathbb{Z}$ is called even (respectively odd) if $2\big|a$ (respectively, $2 \not| a$), i. e., a is of the form $2v$ (respectively, $2v+1$).

(a) The *divisibility* defines a relation on $\mathbb{Z}$ and it satisfies the following basic rules : For all $a,b,c,d \in \mathbb{Z}$, we have :

(i) (Reflexivity) $a\big|a$.

(ii) (Transitivity) If $a\big|b$ and $b\big|c$, then $a\big|c$.

(iii) If $a\big|b$ and $c\big|d$, then $ac\big|bd$.

(iv) If $a\big|b$ and $a\big|c$, then $a\big|(xb+yc)$ 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 $\big|$ and the (standard) order $\leq$ on $\mathbb{N}$.)

(b) Let $a \in \mathbb{Z}$, $a \neq 0$ and let $d \in \mathbb{Z}$ be a divisor 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 $d\big|a$ and $a\big|d$ 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 $-a$ have 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 one knows *all divisors of an integer a* if one knows *all positive divisors of $|a|$*. On this basis many considerations in number theory can be reduced to the set $\mathbb{N}^*$ of positive integers. See for example, the numerical functions $\tau(n)$ and $\sigma(n)$, $n \in \mathbb{N}^*$.)

T5.14 (GCD) For an integer $a \in \mathbb{Z}$, let $\mathrm{D}(a)$ denote the set of all positive divisors of a. Then 1 and $a \in \mathrm{D}(a)$; $\mathrm{D}(a) = \mathbb{N} \iff a = 0$; 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) $d\big|a$ and $d\big|b$; (ii) if c is a positive integer with $c\big|a$ and $c\big|b$, then $c \leq d$.
We put $\gcd(0,0) := 0$.

(a) (Bezout's Lemma [17]) For integers $a,b \in \mathbb{Z}$ with $(a,b) \neq (0,0)$ there exists integers $s,t \in \mathbb{Z}$ such that $\gcd(a,b) = sa+tb$. (**Hint :** Let $M := \{ua+vb \mid u,v \in \mathbb{Z} \text{ and } ua+vb \in \mathbb{N}^*\}$ be

[17] Étienne Bézout (1730-1783) was a French mathematician who is best known for his theorem on the number of solutions of polynomial equations. In 1758 Bézout was elected an adjoint in mechanics of the French Academy

the set of all positive linear combinations of a and b. Then both $|a|, |b| \in M$ and hence by the Minimum Principle T5.2-(b), M contains a smallest element, say $d = sa+tb$, $s,t \in \mathbb{Z}$. Show that $a = \gcd(a,b)$. See also T5.16-(b).)

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 $d = \gcd(a,b)$.

Two integers $a,b \in \mathbb{Z}$ with $(a,b) \neq (0,0)$ are said to be relatively prime if $\gcd(a,b) = 1$, equivalently, there exist integers $s,t \in \mathbb{Z}$ such that $1 = sa+tb$.

(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 $a \mid c$ and $b \mid c$ with $\gcd(a,b) = 1$, then $ab \mid c$. (**Hint :** Use Bezout's Lemma.)

(iv) (Euclid's Lemma) If $a,b,c \in \mathbb{Z}$ and $a \mid bc$ and $\gcd(a,b) = 1$, then $a \mid c$. (**Hint :** By Bezout's Lemma, there exist integers $s,t \in \mathbb{Z}$ such that $1 = sa+tb$ and hence a divides $sac+tbc = c$. See also T5.16-(d).)

(v) 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) $d \mid a$ and $d \mid b$ and (ii) whenever a positive integer c divides both a and b, then $c \mid d$. (**Hint:** Use the part (ii). – **Remark :** The assertion (vi) often serves as a definition of $\gcd(a,b)$. The advantage is the order relationship $\leq$ is not involved.)

(vi) $\mathrm{D}(a) \cap \mathrm{D}(b) = \mathrm{D}(\gcd(a,b))$.

(vii) 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) $a \mid b \iff a = \gcd(a,b)$.

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

(v) (Distributivity) $\gcd(ca,cb) = |c|\gcd(a,b)$. (vi) (Product formula) $\gcd(ab,c) = \gcd(\gcd(a,c)b,c)$.

(**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 elegant symbol, for example, $a \sqcap b := \gcd(a,b)$, then these rules are more suggestive :

(i) $a \sqcap a = |a|$; (ii) $a \mid b \iff a = a \sqcap b$;

(iii) (Commutativity) $a \sqcap b = b \sqcap a$; (iv) (Associativity) $(a \sqcap b) \sqcap c = a \sqcap (b \sqcap c)$;

(v) (Distributivity) $(c \cdot a) \sqcap (c \cdot b) = |c| \cdot (a \sqcap b)$; (vi) (Product formula) $(a \cdot b) \sqcap c = ((a \sqcap c) \cdot b) \sqcap c$;

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 traditional notation $\gcd(a,b)$.)

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

(i) $\gcd(a,1) = 1$. (ii) $\gcd(a,a+n) \mid n$ 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 $a^n \mid b^n$ implies that $a \mid b$. (**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 (iv). Now show that $r = 1$, whence $a = d$, i.e, $a \mid b$.)

---

of Sciences. Besides numerous minor works, wrote a *Théorie générale des équations algébriques*, published at Paris in 1779, which in particular contained much new and valuable matter on the theory of elimination and symmetrical functions of the roots of an equation: he used determinants in a paper in the Histoire de l'acadé mie royale, 1764, but did not treat the general theory.

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

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

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

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

(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 :** $a^{2^n}+1\big|a^{2^{n+1}}-1$. 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 $\gcd(n!+1,(n+1)!+1)=1$.

T5.15 (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 $\mathrm{M}(a)=\mathbb{N}\cdot a\uplus(-\mathbb{N}^+)\cdot a$. 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) $a\big|m$ and $b\big|m$; (ii) if c is a positive integer with $a\big|c$ and $b\big|c$, then $m\big|c$ (equivalently, $m\leq c$). 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 $\mathrm{lcm}(a,b)\leq|ab|$.

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

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

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

(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) $a\big|m$ and $b\big|m$ and (ii) whenever a positive integer c is a multiple of both a and b, then $m\big|c$. (**Hint :** Put $v=\mathrm{lcm}(a,b)$ and use division algorithm to write $m=qt+r$ with $q,r\in\mathbb{Z}$, $0\leq r<t$. Then r is common multiple of a and b. – **Remark :** This assertion often serves as a definition of $\mathrm{lcm}(a,b)$. The advantage is the order relationship is not involved.)

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

T5.16 (Euclidean algorithm[18]) Let $a,b\in\mathbb{N}^*$ with $a\geq b$.

[18] 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.

We put: $r_0 := a$ and $r_1 := b$ and consider the system of equations obtained by the repeated use of division algorithm :

$$\begin{aligned} r_0 &= q_1 r_1 + r_2\,, & 0 < r_2 < r_1\,;\\ r_1 &= q_2 r_2 + r_3\,, & 0 < r_3 < r_2\,;\\ &\cdots \qquad \cdots & \\ r_{k-1} &= q_k r_k + r_{k+1}\,, & 0 < r_{k+1} < r_k\\ r_k &= q_{k+1} r_{k+1}\,. & \end{aligned}$$

Then :

(a) $\gcd(a,b) = r_{k+1}$. (**Hint :** By repeated use of the T5.14-(a)-(vii), we have $\gcd(a,b) = \gcd(r_0,r_1) = \gcd(r_1,r_2) = \cdots = \gcd(r_k,r_{k+1}) = \gcd(r_{k+1},0) = r_{k+1}$.)

(b) For $i = 0,\ldots,k+1$, define s_i and t_i recursively by :

$$\begin{aligned} s_0 &= 1\,, t_0 = 0\,;\\ s_1 &= 0\,, t_1 = 1\,;\\ s_{i+1} &= s_{i-1} - q_i s_i\,, & i = 1,\ldots,k\\ t_{i+1} &= t_{i-1} - q_i t_i\,, & i = 1,\ldots,k \end{aligned}$$

Then:

$a = r_0 = s_0 a + t_0 b$, $r_1 = s_1 a + t_1 b$, $r_{i+1} = r_{i-1} - q_i r_i = s_{i-1}a + t_{i-1}b - q_i s_i a - q_i t_i b = s_{i+1}a + t_{i+1}b$, for all $i = 1,\ldots,k$. In particular, $\gcd(a,b) = r_{k+1} = s_{k+1}a + t_{k+1}b$. (**Remark :** This proves once again the Bezout's Lemma T5.14-(a).) **(c)** Let $a := 36667$ and $b := 12247$. Then we have:

$$\begin{aligned} 36667 &= 2 \cdot 12247 + 12173\\ 12247 &= 1 \cdot 12173 + 74\\ 12173 &= 164 \cdot 74 + 37\\ 74 &= 2 \cdot 37\,. \end{aligned}$$

The integers s_i and t_i can be computed using the following table:

i	0	1	2	3	4
q_i		2	1	164	
s_i	1	0	1	-1	165
t_i	0	1	-2	3	-494

.

Therefore $37 = \gcd(36667,12247) = 165 \cdot 36667 - 494 \cdot 12247$.

(d) (E u c l i d ' s L e m m a) (see also T5.14-(a)-(iv)): *If a prime number p divides a product $a_1 \cdots a_r$ of positive natural numbers, then p divides at least one of the factors a_i.* (**Hint :** We may assume that $r = 2$ (Induction on r). By hypothesis $a_1 a_2 = pc$ with $c \in \mathbb{N}^*$. Suppose that p does not divide b_1. Then p and b_1 are relatively prime and by Bezout's Lemma there exist integers $s,t \in \mathbb{Z}$ such that $1 = sp + tb_1$. Then $b_2 = spb_2 + tb_1b_2 = p(sb_2 + tc)$, i. e. p divides b_2.)

T5.17 (L i n e a r D i o p h a n t i n e E q u a t i o n) The ancient Greek mathematician Diophantus [19] had initiated the study of solutions (in integers) of equations in one or more indeterminate with

[19] D i o p h a n t u s o f A l e x a n d r i a (AD 200 and 214 - between 284 and 298 at age 84), sometimes called "the father of algebra", was an Alexandrian Greek mathematician and the author of a series of books called *Arithmetica*. These texts deal with solving algebraic equations, many of which are now lost. In studying *Arithmetica*, Fermat concluded that a certain equation considered by Diophantus had no solutions, and noted without elaboration that he had found "a truly marvelous proof of this proposition," now referred to as *Fermat's Last Theorem*. This led to tremendous advances in number theory, and the study of Diophantine equations ("Diophantine geometry") and of Diophantine approximations remain important areas of mathematical research. Diophantus was the first Greek mathematician who recognized fractions as numbers; thus he allowed positive rational numbers for the coefficients and solutions. In modern use, Diophantine equations are usually algebraic equations with integer coefficients, for which integer solutions are sought. Diophantus also made advances in mathematical notation.

integer coefficients.

(a) The linear Diophantine equation $aX + bY = c$, $ab, c \in \mathbb{Z}$, has a solution if and only if $d := \gcd(a,b)$ divides c. Moreover, if (x_0, y_0) is a particular solution of this equation, then all other solutions are given by $(x,y) = (x_0,y_0) + (b/d, -a/d)t$, $t \in \mathbb{Z}$.

(b) Let a and b be relatively prime positive integers. Prove that the Diophantine equation $aX - bY = c$ has infinitely many solutions in the positive integers. (**Hint :** There exists integers x_0, y_0 such that $ax_0 + by_0 = c$. Then $(x,y) = (x_0, -y_0) + (b,a)t$, $t \in \mathbb{Z}$ with $t \geq \text{Max}\,(|x_0|/b, |y_0|/a)$ are positive solutions of the given equation.)

(c) The contents of the *Mathematical classic* of C h a n g C h' i u-c h i e n[20] (6th century AD) attest to the algebraic abilities of the Chinese scholars contains the following famous problem: If an Apple costs Rs. 5, an Orange Rs. 3 and three Bananas together Rs. 1, how many Apples, Oranges and Bananas, totaling 100 , can be bought for Rs. 100? (**Hint :** Solve the Diophantine equations $5X + 3Y + \frac{1}{3}Z = 100$ and $X + Y + Z = 100$ simultaneously by eliminating one unknown (for example, Z).)

(d) (M a h a v i r a c h a r y a, 850) There were 63 equal piles of plantain fruit put together and 7 single fruits. They were divided evenly among 23 travelers. What is the number of fruits in each pile? (**Hint :** Solve the Diophantine equation $63X + 7 = 23Y$.)

(e) When Mr. Dey cashed a check at his bank, the teller mistook the number of paise for the number of rupees and vice versa. Unaware of this, Mr. Dey spent 68 paise and then noticed to his surprise that he had twice the amount of the original check. Determine the smallest value for which the check could have been written. HintIf x denotes the number of rupees and y the number of paise in the check, then $100y + x - 68 = 2(100x + y)$.

T5.18 (P r i m e n u m b e r s) A natural number p is called a p r i m e n u m b e r or an i r r e d u c i b l e (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 c o m p o s i t e or r e d u c i b l e 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) (E x i s t e n c e T h e o r e m) Every natural number $a > 1$ has a smallest (positive) divisor $t > 1$. Moreover, this divisor t is a prime number. (**Proof :** The set $T = \{d \in \mathbb{N}^* \mid d \big| a \text{ and } d > 1\}$ is non-empty, since $a \in T$. Therefore by the Minimum Principle (see T5.2-(b)) 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 $t' \big| t$ and $t \big| a$ and hence $t' \big| a$ a contradiction to the minimality of t in T.)

(b) (E u c l i d ' s T h e o r e m[21]) 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*

[20] Z h a n g Q i u j i a n (about 430-about 490) was a Chinese mathematician who wrote the text *Zhang Qiujian suanjing* (Zhang Qiujian's Mathematical Manual) This is a work of historical significance not only because existing treatises of very early mathematics are scarce, but also because it provides a rare insight into the early development of arithmetic – an arithmetic which was built on a numeral system that had the same concept as Hindu-Arabic numeral system – *Jiu zhang suanshu*.

[21] Proved in the "Elements (Book IX, Theorem 20)" of Euclid. Euclid's argument is universally regarded as a model of mathematical elegance. – E u c l i d o f A l e x a n d r i a (325 BC-265 BC) was a Greek mathematician best known for his treatise on mathematics (especially Geometry) – *The Elements*. This influenced the development of Western mathematics for more than 2000 years. 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. 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. As a final personal note let me add that my

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

(c) (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.* More generally, *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 $1\le i\le n$.* (**Proof :** The set $A:=\{x\in\mathbb{N}^*\mid p\big|ax\}$ contains p and b and hence by the Minimum Principle (see T5.2-(b)) it has a smallest element c. We claim that $c\big|y$ for every $y\in A$. For, by division algorithm $y=qc+r$ with $q,r\in\mathbb{N}$ and $0\le r<c$. Then, since $p\big|ay$ and $p\big|ac$, $p\big|ay-q(ac)=ar$. This proves that $r=0$; otherwise $r\in A$ and $r<c$ a contradiction to the minimality of c in A. Therefore $c\big|y$ for every $y\in A$; in particular, $c\big|p$ and hence $c=1$ or $c=p$. If $c=1$, then $p\big|ac=a$. If $c=p$, then (since $b\in A$) by the above claim $p\big|b$. – The last part follows from the first by induction.)

(d) For a natural number p 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 $p\big|a$ or $p\big|b$.

(**Proof :** We may assume that a and b are both positive. The implication (i)⇒(ii) is proved in (c). 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 $p\big|dd'$ and hence by (ii) either $p\big|d$ or $p\big|d'$. But since $1\le d\le p$ and $1\le d'\le p$ 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 number. — **Remark :** The property (ii) is (usually distinguished from the irreducibility property of p) called the prime property. Therefore we can reformulate the part (d) as : *A natural number $p>1$ is irreducible if and only if p has the prime property.* See also ???.)

T5.19 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 :** These are very special cases of a remarkable theorem of Dirichlet[22] on primes in arithmetic progressions established in 1837. The proof is much too difficult to include here, so that we must content ourselves with the mere statement: *If a,b are relatively prime positive natural numbers, then there are infinitely many prime numbers of the form $an+b$, $n\in\mathbb{N}$.* — **Remarks:** For example, (by Dirichelt's Theorem), there are infinitely many primes ending 999 such as 1999, 100999, 1000999, ..., for these appear in the arithmetic progression determined by $1000n+999$, where $\gcd(1000,999)=1$.)

(a) There is no arithmetic progression $a+n\cdot b$, $n\in\mathbb{N}$ that consists of only of prime numbers. (**Hint :** Suppose that $p=a+n\cdot b$ is a prime number. Then the $n+kp$-th term of the arithmetic progression is $a+(n+kp)\cdot b=(a+n\cdot b)+kp\cdot b=p(1+kb)$. This shows that the arithmetic progression must contain infinitely many composite numbers.)

(b) If all the $n>2$ terms of the arithmetic progression $p,p+d,\ldots,p+(n-1)d$ are prime numbers, then the common difference d is divisible by every prime $q<n$.

---

own introduction to mathematics at school in the 1970s was from an edition of part of Euclid's Elements and the work provided a logical basis for mathematics and the concept of proof which seem to be lacking in school mathematics today.

[22] Peter Gustav Lejeune Dirichlet (1805-1859) was a German mathematician with deep contributions to number theory (including creating the field of analytic number theory), and to the theory of Fourier series and other topics in mathematical analysis; he is credited with being one of the first mathematicians to give the modern formal definition of a function. Dirichelt's doctoral advisers were Simeon Poisson and Joseph Fourier. Doctoral students of Drichelts were Gotthold Eisenstein, Leopold Kronecker, Rudolf Lipschitz, Carl Wilhelm Borchardt. Other notable students were Richard Dedekind, Eduard Heine, Bernhard Riemann, Wilhelm Weber.

T5.20 (Fundamental Theorem of Arithmetic[23]) Proposition 14 of Book IX of Euclid's "Elements" embodies the result which later became known as:

Fundamental Theorem of Arithmetic : *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.*

More precisely, the existence and uniqueness parts are stated as:

(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 of a.* (**Proof :** Either a is prime or composite.; in the former case there is nothing to prove. If a is composite, then by T5.18-(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 $\rho \in \mathfrak{S}_n$ such that $q_i = p_{\rho(i)}$ 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 T5.18-(d) $p_1 \big| q_j$ for some j, $1 \leq j \leq m$. Renumbering 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 canceling 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 $\rho' \in \mathfrak{S}(\{2, \ldots, n\})$ such that $q_{\rho(i)} = p_i$ for all $i = 2, \ldots, n$. Now, define $\rho \in \mathfrak{S}_n$ by $\rho(1) = 1$ and $\rho(i) = \rho'(i)$ for all $i = 2, \ldots, n$. — **Remarks :** The above proof for uniqueness use the Euclid's lemma on the prime property (see Test-Exercise T5-16-(a)-(iv)) 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 examples given in T5.22 and T5.23. 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 (see also Zermelo's proof given in the T5.21). This can also be seen in the examples in the Examples T5.22 and T5.23.

(c) (Canonical Prime Decomposition) Let $n \in \mathbb{N}^*$. Collecting the equal prime factors in the prime decomposition of n, we get the canonical prime decomposition $n = \prod_{p \in \mathbb{P}} p^{\alpha_p}$. In this product $\mathbb{P}$ denote the set of all prime numbers and the p-exponents or multiplicities $\alpha_p \in \mathbb{N}$ are non-zero only for finitely many prime numbers $p \in \mathbb{P}$, so that the above product has only finitely many factors $\neq 1$. For example, $1001 = 7 \cdot 11 \cdot 13$ and $10200 = 2^3 \cdot 3 \cdot 5^2 \cdot 17$. Therefore, for every prime number $p \in \mathbb{P}$, we define a map $v_p : \mathbb{N}^* \to \mathbb{N}$ by $n \mapsto v_p(n) := \alpha_p$. The map v_p is called the p-adic valuation. It is clear that $v_p(n) = 0$ for almost all $p \in \mathbb{P}$.

If $m, n \in \mathbb{N}^*$ and $m = \prod_{p \in \mathbb{P}} p^{v_p(m)}$, $n = \prod_{p \in \mathbb{P}} p^{v_p(n)}$ are the canonical prime decompositions of m and n respectively. Then:

(i) m divides n if and only if $v_p(m) \leq v_p(n)$ for all $p \in \mathbb{P}$.

(ii) $\gcd(m,n) = \prod_{p \in \mathbb{P}} p^{\mathrm{Min}(v_p(m), v_p(n))}$ and $\mathrm{lcm}(m,n) = \prod_{p \in \mathbb{P}} p^{\mathrm{Max}(v_p(m), v_p(n))}$ and

[23] The Fundamental Theorem of Arithmetic does not seem to have been stated explicitly in Euclid's 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), see also Footnote 27. It was, of course, familiar to earlier mathematicians; but GAUSS was the first to develop arithmetic as a systematic science.

For an integer $a \in \mathbb{Z}$, $a \neq 0$, the canonical prime decomposition is $a = (-1)^{\varepsilon} \prod_{p \in \mathbb{P}} p^{v_p(|a|)}$, where $\varepsilon \in \{0,1\}$ (and hence $(-1)^{\varepsilon}$ is the sign of a and $|a|$ is the absolute value of a. Moreover, for every non-zero rational number $x = a/b$ with $a,b \in \mathbb{Z} \setminus \{0\}$, combining the canonical prime decompositions of a and b, we get the canonical prime decomposition of x: $x = (-1)^{\varepsilon} \prod_{p \in \mathbb{P}} p^{v_p(x)}$, where the p-exponents $v_p(x)$, $p \in \mathbb{P}$ are integers (and not just the natural numbers) and are non-zero only for finitely many prime numbers $p \in \mathbb{P}$. Note that x is uniquely determined by the p-exponents $v_p(x)$, $p \in \mathbb{P}$ and its sign $(-1)^{\varepsilon}$. Further, note that a rational number $x \in \mathbb{Q} \setminus \{0\}$ is an integer if and only if $v_p(x) \geq 0$ for all $p \in \mathbb{P}$.

T5.21 (Zermelo's proof of uniqueness of irreducible decomposition) In this proof we recall that a natural number $p \in \mathbb{N}^*$ is called an irreducible number if $p > 1$ and the only divisors of p in $\mathbb{N}^*$ are 1 and p itself. Let $n \in \mathbb{N}^*$. We shall prove the uniqueness of irreducible decomposition by induction on n. If $n = 1$ or $n = p$ is a (irreducible) prime number, then the assertion is clear by the definition of prime (irreducible) number. Now, suppose that $n = p-1 \cdots p_r = q_1 \cdots q_s$ where $p_1, \ldots, p_r$; $q-1, \ldots, q_s$ are irreducible numbers with $r,s \geq 2$. We may assume that $p_1 \leq p_2 \leq \cdots \leq p_r$; $q_1 \leq q_2 \leq \cdots \leq q_s$ and $p_1 \leq q_1$. If $p_1 = q_1$, then $n' := p_2 \cdots p_r = q_2 \cdots q_s < n$ and hence the uniqueness assertion follows from the induction hypothesis. If $p_1 < q_1$, then we must lead to a contradiction (of the irreducibility of q_1). Put $m := n - p_1 q_2 \cdots q_s = (q_1 - p_1) q_2 \cdots q_s = p_1(p_2 \cdots p_r - q_2 \cdots q_s)$. Then $1 < m < n$. Therefore by induction hypothesis it follows from the uniqueness assertion for $m = p_1(p_2 \cdots p_r - q_2 \cdots q_s)$ that p_1 must occur in every irreducible decomposition of m. In particular, p_1 must occur in the product $m = (q_1 - p_1) q_2 \cdots q_s$, where $q_2, \ldots, q_s$ are irreducible numbers and $p_1 \neq q_j$ for every $j = 1, \ldots, s$. This shows that p_1 must occur in $q_1 - p_1$, i. e. p_1 divides $q_1 - p_1$ in $\mathbb{N}^*$, or equivalently, $q_1 - p_1 = b p_1$ with $b \in \mathbb{N}^*$, i. e. $q_1 = (b+1) p_1$ which contradicts the irreduciblity of q_1. •

(**Remark :** Zermelo's indirect method of proof is psycological and less convincing. However, this proof is elegant and didactically difficult to present in the class room. Moreover, the Euclid's Lemma is not in this proof. In fact we can now deduce the Euclid's Lemma as a corollary of the Fundamental Theorem of Arithmetic.)

T5.22 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 this, 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 $\mathbb{N}$, 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 $\mathbb{N}$) also define divisibility and prime property in M, with these definitions $4 \mid 100 = 10 \cdot 10$ in M, but $4 \not\mid 10$ 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 $4 \not\mid 10$ in M).

T5.23 Let $q \in \mathbb{N}^*$ be an arbitrary prime number (e. g. $q := 2$ or $q := 1234567891$ [24]) 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

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

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 essentially different decompositions (p prime number $\neq q$).

T5.24 (C o n g r u e n c e s) In the first chapter of *Disquisitiones Arithmaticae*[25] Gauss introduced the concept of *congruence* and the notation that makes it such a powerful technique for computations. He was induced to adopt the symbol $\equiv$ because of the close analogy with the (algebraic) equality $=$.

Let $n \in \mathbb{N}^*$ be a fixed positive natural number. Two integers a and $b \in \mathbb{Z}$ are said to be c o n g r u e n t m o d u l o n, denoted by $a \equiv b \pmod{n}$ if n divides the difference $a-b$, i. e. $a-b=kn$ for some integer $k \in \mathbb{Z}$.

Given an integer $a \in \mathbb{Z}$, let q and r denote the quotient and remainder upon division by n, so that $a = qn+r$, $0 \leq r < n$. then $a \equiv r \pmod{n}$. Therefore every integer is congruent modulo n to exactly one of $0, 1, \ldots, n-1$; in particular, $a \equiv 0 \pmod{n}$ if and only if n divides a. Further, note that $a \equiv b \pmod{n}$ if and only if a and b have the same remainder upon division by n.

(a) The behavior of $\equiv$ with respect to the addition and multiplication is reminiscent of the ordinary equality. For a (fixed) natural number $n > 1$ and arbitrary integers $a, b, c, d \in \mathbb{Z}$, some of the elementary properties of equality that carry over to $\equiv$ are:

(i) $a \equiv a \pmod{n}$.

(ii) If $a \equiv b \pmod{n}$, then $b \equiv a \pmod{n}$.

(iii) If $a \equiv b \pmod{n}$ and if $b \equiv c \pmod{n}$, then $a \equiv c \pmod{n}$.

(**Remark :** The above three properties show that $\equiv$ is an equivalence relation on the set of integers. The equivalence classes of $\equiv$ are precisely the c o n g r u e n c e c l a s s e s m o d u l o n: $[r] := r + \mathbb{Z} \cdot n := \{r + kn \mid k \in \mathbb{Z}\}$, $r = 0, \ldots, n-1$. Therefore the quotient set $\mathbb{Z}/\equiv = \{[r] \mid 0 \leq r < n-1\}$; this quotient set is usually denoted by $\mathbb{Z}_n$ and its elements are also called the r e s i d u e c l a s s e s m o d u l o n. The system $0, 1, \ldots, n-1$ form a complete representative system for the quotient set $\mathbb{Z}/\equiv$.)

(iv) If $a \equiv b \pmod{n}$ and if $c \equiv d \pmod{n}$, then $a + c \equiv b + d \pmod{n}$ and $a \cdot c \equiv b \cdot d \pmod{n}$. In particular, if $a \equiv b \pmod{n}$, then $a^m \equiv b^m \pmod{n}$ for every $m \in \mathbb{N}$ and $a + c \equiv b + c \pmod{n}$ and $a \cdot c \equiv b \cdot c \pmod{n}$.

(**Remark :** It follows from (iv) that the binary operations $+_n$ (called the a d d i t i o n m o d u l o n) and $\cdot_n$ (called the m u l t i p l i c a t i o n m o d u l o n) defined on the quotient set $\mathbb{Z}_n$ by $([r],[s]) \mapsto [r+s]$ and $([r],[s]) \mapsto [r \cdot s]$ are well-defined. Both these binary operations are associative, commutative and $[0]$ (respectively, $[1]$) is the identity element for $+_n$ (respectively, $\cdot_n$). Therefore $(\mathbb{Z}_n, +_n)$ *and* $(\mathbb{Z}_n, \cdot_n)$ *are commutative monoids. Moreover, the monoid* $(\mathbb{Z}_n, +_n)$ *is a group.* Further, the binary operations $+n$ and $cdot_n$ are connected by the distributive laws: $([r] +_n [s]) \cdot_n [t] = [r] \cdot_n [t] +_n [s] \cdot_n [t]$ and $[r] \cdot_n ([s] +_n [t]) = [r] \cdot_n [s] +_n [r] \cdot_n [t]$ for all $r, s, t \in \{0, 1, \ldots, n-1\}$. Therefore $(\mathbb{Z}_n, +_n, \cdot_n)$ *is a commutative ring with the* (multiplicative) *identity* $[1]$. All the above assertions are immediate from the definitions of $+_n$, $\cdot_n$ and the standard associativity, commutativity and the distributive laws of the standard addition and multiplication on the set $\mathbb{Z}$ of integers.)

One cannot unrestrictedly cancel common factor in the arithmetic of congruences. With suitable precautions cancelation can be allowed:

(v) If $ca \equiv cb \pmod{n}$, then $a \equiv b \pmod{n/d}$, where $d = \gcd(c, n)$. (**Hint :** Use Euclid's lemma.)

(vi) If $ca \equiv cb \pmod{n}$ and if $\gcd(c, n) = 1$, then $a \equiv b \pmod{n}$. In particular, if p is a prime number which does not divide c and if $ca \equiv cb \pmod{p}$, then $a \equiv b \pmod{n}$.

---

[25] This monumental work of the German mathematician C a r l F r i e d r i c h G a u s s (1777-1855) appeared in 1801 when he was 24 years old. In this work Gauss laid the foundations of modern number theory, see also the Footnote [23]

(b) For a (fixed) natural number $n > 1$ and arbitrary integers $a, b, c, d \in \mathbb{Z}$, prove that:

(i) If $a \equiv b \pmod{n}$ and if $m \mid n$, then $a \equiv b \pmod{m}$.

(ii) If $a \equiv b \pmod{n}$ and if $c > 0$, then $ca \equiv cb \pmod{cn}$.

(iii) If $a \equiv b \pmod{n}$ and if each a, b, n is divisible by $d > 0$, then $a/d \equiv b/d \pmod{n/d}$.

(iv) If $a \equiv b \pmod{n}$, then $\gcd(a,n) = \gcd(a,b)$.

(c) Find the remainders : (i) when 2^{50}, 41^{65}, 111^{333} and 333^{111} are divided by 7.

(ii) when 53^{103} and 103^{53} are divided by 39.

(iii) when 4444^{4444} is divided by 9. (**Hint :** Use $2^3 \equiv -1 \pmod 9$.)

(iv) when $15!$ is divided by 17.

(v) when $2 \cdot (26!)$ is divided by 29.

(vi) when $4 \cdot (29!) + 5!$ is divided by 31.

(d) For $n \in \mathbb{N}^*$, show that :

(i) 7 divides $5^{2n} + 3 \cdot 2^{5n-2}$; 13 divides $3^{n+1} + 4^{2n+1}$; 27 divides $2^{5n+1} + 5^{n+2}$; 43 divides $6^{n+2} + 7^{2n+1}$.

(ii) For $n \geq 1$, show that $(-13)^{n+1} \equiv (-13)^n + (-13)^{n-1} \pmod{181}$. (**Hint :** Note that $(-13)^2 \equiv -13 + 1 \pmod{181}$ and use induction on n.)

(iii) 89 divides $2^{44} - 1$ and 97 divides $2^{48} - 1$.

(e) Show that :

(i) If $a_1, \ldots, a_n \in \mathbb{Z}$ is a complete representative system for $\mathbb{Z}_n$ and if $a \in \mathbb{Z}$ is relatively prime to n, then $a \cdot a_1, \ldots, a \cdot a_n$ also form a complete representative system for $\mathbb{Z}_n$.

(ii) Verify that $0, 1, 2, 2^2, \ldots, 2^9$ form a complete representative system for $\mathbb{Z}_{11}$, but that $0, 1^2, 2^2, 3^2, \ldots, 10^2$ do not.

(iii) If $a \in \mathbb{Z}$ is relatively prime to n and if $c \in \mathbb{Z}$ is arbitrary, then the integers $c, c+a, \ldots, c+(n-1)a$ form a complete representative system for $\mathbb{Z}_n$. In particular, any n consecutive integers form a complete representative system for $\mathbb{Z}_n$. Deduce that the product of any set of n consecutive integers is divisible by n.

(f) If $a \in \mathbb{Z}$ is an odd integer, then show that $a^{2^n} \equiv 1 \pmod{2^{n+2}}$ for every $n \in \mathbb{N}^*$. (**Hint :** Use induction on n.)

(g) For a natural number $n > 1$ and arbitrary integers $a, b, c, d \in \mathbb{Z}$ with $\gcd(b,n) = 1$, prove that: if $ab \equiv cd \pmod{n}$ and $b \equiv d \pmod{n}$, then $a \equiv c \pmod{n}$.

(h) For natural numbers $m, n \in \mathbb{N}^*$ and arbitrary integers $a, b, c \in \mathbb{Z}$, prove that: if $a \equiv b \pmod{m}$ and $a \equiv c \pmod{n}$, then $b \equiv c \pmod{\gcd(m,n)}$.

T5.25 (g-adic-Expansion) Let g be natural number ≥ 2. For every natural number $n \geq 1$, there exist uniquely determined natural numbers r and $a_0, \ldots, a_r$ with $a_r \neq 0$ and $0 \leq a_i < g$ such that

$$n = a_0 + a_1 g + \cdots + a_r g^r = \sum_{i=0}^{r} a_i g^i \ .$$

The digits a_i of this g-adic-expansion of n recursively by repeated use of division with remainder by using the following scheme, with $q_0 := n$:

$$\begin{aligned}
q_0 &= q_1 g + a_0 , & 0 \leq a_0 < g \ , \\
q_1 &= q_2 g + a_1 , & 0 \leq a_1 < g \ , \\
&\cdots\cdots\cdots & \cdots\cdots\cdots\cdots \\
q_{r-1} &= q_r g + a_{r-1} , & 0 \leq a_{r-1} < g \ , \\
q_r &= a_r , & 0 < a_r < g \ .
\end{aligned}$$

The uniqueness of these digits follows immediately follows from the uniqueness of the divison with remainder. We also write shortly $n = (a_r \dots a_0)_g$. For $g = 2$ respectively, $g = 3$, $g = 10$, $g = 16$, then we also use the terms the dual- respectively ternary- decimal- hexa- or sedecimal expansion of n. In the last system the digits $10, \dots, 15$ denoted by the letters A,...,F. Conversely, from the g-adic expansion $n = a_0 + a_1 g + \cdots + a_r g^r$ one can compute the number n rapidly by using the recursion[26] :

$$\begin{aligned} n_0 &= a_r \ , \\ n_1 &= n_0 g + a_{r-1} \ (= a_r g + a_{r-1}) \ , \\ &\cdots\cdots\cdots\cdots\cdots\cdots \\ n_{r-1} &= n_{r-2} g + a_1 \ (= a_r g^{r-1} + a_{r-1} g^{r-2} + \cdots + a_2 g + a_1) \ , \\ n_r &= n_{r-1} g + a_0 = n \ . \end{aligned}$$

Let $n \in \mathbb{N}^*$ and let $n = a_m g^m + a_{m-1} g^{m-1} + \cdots + a_1 g + a_0$, $m \in \mathbb{N}$ and $a_j \in \{0, 1, \dots, g-1\}$ be the g-adic expansion of n. Put $Q_g(n) := a_0 + \cdots + a_m$ and $Q'_g(n) := a_0 - a_1 + \cdots + (-1)^m a_m$. Then:

(a) $n \equiv Q_g(n) \pmod{(g-1)}$ and $n \equiv Q'_g(n) \pmod{(g+1)}$.
In particular, $g-1 \mid n \iff g-1 \mid Q_g(n)$ and $g+1 \mid n \iff g+1 \mid Q'_g(n)$.

(b) $Q_g(n+n') \equiv Q_g(n) + Q_g(n') \pmod{g-1}$ and $Q'_g(n+n') \equiv Q'_g(n) + Q'_g(n') \pmod{g+1}$.

(c) $Q_g(n \cdot n') \equiv Q_g(n) \cdot Q_g(n') \pmod{g-1}$ and $Q'_g(n \cdot n') \equiv Q'_g(n) \cdot Q'_g(n') \pmod{g+1}$.

(d) Let $n \in \mathbb{N}^*$ and let $n = a_m 10^m + a_{m-1} 10^{m-1} + \cdots + a_1 10 + a_0$, $m \in \mathbb{N}$ and $a_j \in \{0, 1, \dots, 9\}$ be the decimal expansion of n. Then
(i) $3|n \iff 3|(a_0 + a_1 + \cdots + a_m)$; $5|n \iff 5|a_0$; $6|n \iff 6|(a_0 + 4a_1 + 4a_2 + \cdots + 4a_m)$; $9|n \iff 9|(a_0 + a_1 + \cdots + a_m)$; $11|n \iff 11|(a_0 - a_1 + \cdots + (-1)^m a_m)$. More generally, if $n = a_m g^m + a_{m-1} g^{m-1} + \cdots + a_1 g + a_0$, $m \in \mathbb{N}$ and $a_j \in \{0, 1, \dots, g-1\}$ is the g-adic expansion of n. Then $g-1$ divides n if and only if $g-1$ divides the sum $a_m + \cdots + a_0$ of the digits of n.
(ii) $7|n \iff 7|(a_2, a_1, a_0)_{10} - (a_5, a_4, a_3)_{10} + \cdots$; $11|n \iff 11|(a_2, a_1, a_0)_{10} - (a_5, a_4, a_3)_{10} + \cdots$; $13|n \iff 13|(a_0 + 2a_1 + \cdots + 2^m a_m)$.

†(**Remarks:** More generally, one can also prove that: *Every non-negative real number $x \geq 0$ can be represented uniquely by a infinite convergent series $x = \sum_{\nu=0}^{\infty} a_\nu / g^\nu$, where the g-digit sequence of natural numbers $(a_n)_{n \in \mathbb{N}}$ is obtained by the g-adic algorithm and satisfy the following inequalities: $a_n \leq g-1$ for all $n \geq 1$ and $a_n \leq g-2$ for infinitely many n.*

Moreover, such a sequence of natural numbers comes as a g-adic digit sequence of a non-negative real number. The g-adic algorithm of a non-negative real number $x \geq 0$ gives a simple criterion to test whether or not x is rational. More precisely:

A non-negative real number $x \geq 0$ is a rational number if and only if the sequence $(a_n)_{n \in \mathbb{N}}$ is periodic (see Exercise 5.9), i. e. *there exist $r \in \mathbb{N}$ and $s \in \mathbb{N}^*$ such that $a_{r+\nu} = a_{r+\nu+s}$ for all $\nu \in \mathbb{N}^*$.*

We use the notation $x = (a_0, a_1 a_2 \cdots a_n \cdots)_g$ and $(a_0; a_1 a_2 \cdots a_r, \overline{a_{r+1} \cdots a_{r+s}})_g$.

(a) For a rational number $x \in [0, 1)$ and natural numbers r, s, the following statements are equivalent:
(i) $g^r(g^s - 1) \cdot x \in \mathbb{Z}$. (ii) x has the g-adic expansion of the form $x = (a_0; a_1 a_2 \cdots a_r, \overline{a_{r+1} \cdots a_{r+s}})_g$.

(b) For a rational number $x = a/b \in [0, 1)$ with $\gcd(a, b) = 1$, show that $\gcd(b, g) = 1$ if and only if the g-adic expansion of x is purely periodic (see Exercise 5.9), i. e. it is of the form $x = (0, \overline{a_1 \cdots a_s})_g$. In particular, the g-adic expansion of reduced fractions $x = \frac{a}{g^n - 1}$ is purely periodic with period n. for example, $\frac{1}{g^n - 1} = (0; \overline{00 \cdots 01})_g$.

---

[26] This is a special case of the well known Horner's scheme. Named after William George Horner (1786-1837), who is largely remembered only for the method, Horner's method, of solving algebraic equations ascribed to him by Augustus De Morgan and others.

(c) Which of the following (real) numbers are irrational numbers :

(i) The number x with the g-adic expansion $x = (0; 101001000100001\cdots)_g$.

(ii) The number y with the g-adic expansion $y = (0; a_1 a_2 \cdots a_n \cdots)_g$, where $a_n = 1$ if n is prime and 0 otherwise.

(iii) $u = \sum_{v=0}^{\infty} \left(\frac{1}{g}\right)^v$, $v = \sum_{v=0}^{\infty} \left(\frac{1}{g}\right)^{v(v+1)/2}$ and $w = \sum_{v=0}^{\infty} \left(\frac{1}{g}\right)^{v^2}$.

(d) Compute the g-adic exppansions of the numbers $\frac{a}{g-1}$ and $\frac{a}{g+1}$. Moreover, show that $\frac{1}{(g-1)^2} = (0; 0123\cdots(g-3)(g-1))_g$ is purely periodic.)

T5.26 Let $n \in \mathbb{N}^*$, $a, b \in \mathbb{Z}$ and let $P(X) = \sum_{i=0}^{d} a_i X^i$ be a polynomial with integer coefficients $a_0, \ldots, a_d \in \mathbb{Z}$. We say that an integer $a \in \mathbb{Z}$ is a solution of the polynomial congruence $P(X) \equiv 0 \pmod{n}$ if $P(a) \equiv 0 \pmod{n}$.

(a) If $a \equiv b \pmod{n}$ then show that $P(a) \equiv P(b) \pmod{n}$. Deduce that if a is a solution of the congruence $P(a) \equiv 0 \pmod{n}$ and if $a \equiv b \pmod{n}$, then b is also a solution.

(b) Determine the last two digits of 9^{9^9}. (**Hint :** $9^9 \equiv 9 \pmod{10}$ and hence $9^{9^9} = 9^{9+10k}$. Now use $9^9 \equiv 89 \pmod{100}$.)

(c) Is the integer $(447836)_9$ divisible by 3 and 8?

(d) Find the missing digits (by working modulo 9 or 11) in the calculations below :

(i) $51840 \cdot 273581 = 1418243x040$. (ii) $2x99561 = (3(523+x))^2$. (iii) $2784x = x \cdot 5569$.

(iv) $512 \cdot 1x53125 = 1000000000$. (v) If 495 divides $273x49y5$, then find the digits x and y.

(e) Determine the last three digits of 7^{999}. (**Hint :** $7^{4n} \equiv (1+400)^n \equiv 1+400n \pmod{1000}$.)

(f) For any $n \geq 1$, show that there exists a prime number with at least n of its digits equal to 0. (**Hint :** consider the arithmetic progression $10^{n+1} \cdot m + 1$, $m \in \mathbb{N}^*$.)

(g) Show that 2^{r+1} divides a integer n if and only if 2^r divides the number made up of the last r digits of n. (**Hint :** $10^k = 2^k \cdot 5^k \equiv 0 \pmod{2^r}$ for $k \geq r$.)

(h) Explain why the following curious calculation hold:

$$\begin{aligned}
1 \cdot 9 + 2 &= 11 \\
12 \cdot 9 + 3 &= 111 \\
123 \cdot 9 + 4 &= 1111 \\
1234 \cdot 9 + 5 &= 11111 \\
12345 \cdot 9 + 6 &= 111111 \\
123456 \cdot 9 + 7 &= 1111111 \\
1234567 \cdot 9 + 8 &= 11111111 \\
12345678 \cdot 9 + 9 &= 111111111 \\
123456789 \cdot 9 + 10 &= 1111111111
\end{aligned}$$

(**Hint:** Show that $(10^{n-1} + 2 \cdot 10^{n-2} + 3 \cdot 10^{n-3} + \cdots + n) \cdot (10-1) + (n+1) = \frac{10^{n+1}-1}{9}$.)

(i) If 792 divides the integer $(13xy45z)_{10}$, then find the digits x, y and z. (**Hint :** Use T5.25-(d)-(ii).)

(j) For any prime number $p > 3$, prove that 13 divides $10^{2p} - 10^p + 1$.

T5.27 (Irrational numbers[27]) A real number which is not rational is called an irrational number.

(a) 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.

(b) 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, $i = 1, \ldots, r$.

(c) (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 every 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)[28] $\sqrt{3}, \sqrt{5}, \ldots, \sqrt{p}$, 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.

(d) 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.

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

(f) Let t be a rational multiple of π[29], 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 $\cos t = 0, \pm 1/2, \pm 1$; $\sin t = 0, \pm 1/2, \pm 1$; $\tan t = 0, \pm 1$.

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

(h) Let z be a real number. Show that the following statements 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 $[(k!)z] = (k!)z$.

---

[27] The word "irrational" is the translation of the Greek word "$\alpha\lambda o\gamma o\zeta$ " in Latin. The Greek word probably means "not pronounceable". The misunderstanding that in Latin "ratio" is essentially the meaning of "rationality" made "irrational numbers".

[28] Phythagoras 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 rational, then there exists $k \in \mathbb{N}^*$ such that $k\sqrt{2} \in \mathbb{Z}$. By the Minimum Principle T5.2-(b) choose a minimal $k \in \mathbb{N}^*$ 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.

[29] What is the definition of the number π? Ancient Greeks defined the number π as the ratio of the circumference of a circle to its diameter. The letter π came from Greek the word *perimetros*. It was Euler's adoption of the symbol in his many popular textbooks that made it widely known and used. The first recorded scientific effort to approximate π appeared in the *Measurement of a Circle* by the Greek mathematician of ancient Syracuse, Archimedes (287-212 BC). His method was to inscribe and circumscribe regular polygon about circle, determine their perimeters and use these as lower and upper bounds on the circumference. Using a polygon of 96 sides, he obtained the inequality: $223/71 < \pi < 22/7$.

(i) Use the above part (h) 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 $[(k!)e] = k! \sum_{i=0}^{k} 1/i! < (k!)e$.) (**Proof:** (due to J . - B . F o u r i e r (1768-1830) a French mathematician and physicist) Suppose that $e = P/Q$ with $P, Q \in \mathbb{N}$, $P, Q \geq 1$. Then

$$P/Q = 1 + 1/1! + 1/2! + \cdots + 1/Q! + 1/(Q+1)! + \cdots$$

Multiplying by $Q!$, it follows that

$$(Q-1)! \cdot P = Q! + Q! + \cdots + Q + 1 + 1/(Q+1) + 1/(Q+1)(Q+2) + \cdots$$

i. e. the series

$$\sum_{\nu=1}^{\infty} \frac{1}{(Q+1)\cdots(Q+\nu)} > 0$$

has an integer value. But

$$\frac{1}{(Q+1)\cdots(Q+\nu)} < \frac{1}{(Q+1)^{\nu}} \quad \text{for all} \quad \nu \geq 2,$$

and hence

$$\frac{1}{(Q+1)\cdots(Q+\nu)} < \sum_{\nu=1}^{\infty} \frac{1}{(Q+1)^{\nu}} = \frac{1}{Q} \leq 1$$

a contradiction. For the last equality, we have used the formula[30] (for $x = 1/(Q+1) \leq 1/2$).
– **Remark:** The proof of irrationality of the number π involves Differential and Integral Calculus and is not quite so easy!)

[30] For every $x \in \mathbb{R}$ with $|x| < 1$, we have $\sum_{\nu=0}^{\infty} x^{\nu} = \frac{x}{1-x}$.