E0 221 Discrete Structures / August-December 2012

(ME, MSc. Ph. D. Programmes)

Tel : +91-(0)80-2293 2239/(Maths Dept. 3212) **E-mails :** dppatil@csa.iisc.ernet.in / patil@math.iisc.ernet.in

Lectures : Monday and Wednesday ; 11:30–13:00 **Venue:** CSA, Lecture Hall (Room No. 117)

1-st Midterm : Saturday, September 22, 2012; 14:00 -16:30 **2-nd Midterm :** Sunday, October 14, 2012; 10:00 -12:00
Final Examination : Wednesday, December 05, 2012, 09:00 -12:00

Evaluation Weightage : Midterms (Two) : 50% **Final Examination :** 50%

Range of Marks for Grades (Total 100 Marks)						
	Grade S	**Grade A**	**Grade B**	**Grade C**	**Grade D**	**Grade F**
Marks-Range	>90	76–90	61–75	46–60	35–45	<35

5. The Natural Numbers — The Fundamental Theorem of Arithmetic

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

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

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

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

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

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

[1] **Recursion formula for binomial coefficients:** $\binom{n+1}{k}=\binom{n}{k}+\binom{n-1}{k-1}+\cdots+\binom{n-k+1}{1}+\binom{n-k}{0}$. This follows from the equality $\binom{n+1}{m}=\binom{n}{m}+\binom{n}{m-1}$.

(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 w o r d s over the a l p h a b e t A - into the set $\mathbb{N}^*$ of positive natural numbers. (**Remark :** Such a coding of the words over A is called a G ö d e l i s a t i o n (due to K. Gödel[2]). The natural number associated to a word is called the G ö d e l n u m b e r 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 Gœdelisation. (**Remark :** This is a variant of the g-adic expansion (see Test-Exercise T5.21).)

5.3 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 Test-Exercise T5.21.)

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

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

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

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

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

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

Then $n \equiv W \bmod d$. In particular, d divides the number n if and only if d divides the alternating sum W. (**Remark :** With the help of this exercise one can find criterion, which one can decide on the basis the digit-sequence of the natural number n in the decimal system whether d is a divisor of n with $2 \leq d \leq 16$. (with $d = 3$ and $d = 9$ one uses the simple check-sum, with $d = 11$ the simple alternating sum. The divisibility by $7, 11$ and 13 at the same time can be tested with the alternating sum of the 3-grouped together in view of the part (c). See Test-Exercise T5.21-(d) for details.)

5.4 **(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 $b \geq f$ can 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 do not 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.)

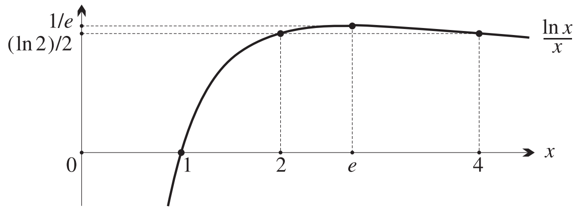
(c) Let $a, b \in \mathbb{N}^*$ and $d := \gcd(a, b) = sa + tb$ with $s, t \in \mathbb{Z}$. Then $d = s'a + t'b$ for $s', t' \in \mathbb{Z}$ if and only if there exists $k \in \mathbb{Z}$ such that $s' = s - k\left(\dfrac{b}{d}\right)$, $t' = t + k \cdot \left(\dfrac{a}{d}\right)$.

5.5 **(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

[2] K u r t G ö d e l (1906-1978) was born on 28 April 1906 in Brünn, Austria-Hungary (now Brno, Czech Republic) and died on 14 Jan 1978 in Princeton, New Jersey, USA. Gödel proved fundamental results about axiomatic systems showing in any axiomatic mathematical system there are propositions that cannot be proved or disproved within the axioms of the system.

$\gcd(c,d)=1$. 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 *integers* numbers with $x<y$ and $x^y=y^x$. The pairs of *rational* numbers (x,y) with $x<y$ and $x^y=y^x$ are precisely the pairs: $\big((1+\frac{1}{n})^n,(1+\frac{1}{n})^{n+1}\big)$, $n\in\mathbb{N}^*$. (**Hint :** Prove that for each *real* positive number of x with $1<x<e$ there exists exactly one real number $y>x$ such that $x^y=y^x$. (observe that necessarily $y>e$.) For the proof of the above assertion : note that $x^y=y^x$ if and only if $(\ln x)/x=(\ln y)/y$ and consider the function $(\ln x)/x$ on $\mathbb{R}_+^\times$.)



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

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

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

5.6 **(a)** (Perfect numbers) A natural number $n\in\mathbb{N}^*$ is called perfect if $\sigma(n)=2n$, where $\sigma(n):=\sum_{d|n} d$ denote the sum of positive divisors of n.
(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 $\sigma(b=2^{s+1}c$, $b=(2^{s+1}-1)c$, $\sigma(b)=b+c$.)

(b) (Mersenne Numbers) Let $a,n\in\mathbb{N}$ with $a,n\geq 2$. If a^n-1 is prime, then $a=2$ and n is prime. (**Hint :** Use geometric series $a^n-1=(a-1)(a^{n-1}+a^{n-2}+\cdots+a+1)$ to conclude that $a=2$; if $n=rs$ with $r>1,s>1$, then $2^n-1=(2^r)^s-1=(2^r-1)(1+2^r+2^{2r}+\cdots+(2^r)^{s-1})$. — The natural numbers of the form a^p-1, $p\in\mathbb{P}$ prime, are called Mersenne numbers. For $p=2,3,5,7$ the corresponding Mersenne numbers $3,7,31,127$ are prime, but corresponding to $p=11$, it is $M_{11}=2^{11}-1=2047=23\cdot 89$ which is not prime. — **Remarks :** It was asserted by Mersenne[3] in 1644 that : $M_p=2^p-1$ *is prime for* $2,3,5,7,13,17,19,31,61,89,107,127$, *and composite for the other remaining* 44 *values of* $p\leq 257$. For example, $47\,|\,M_{23}$, $233\,|\,M_{29}$, $223\,|\,M_{37}$, $431\,|\,M_{43}$ and $167\,|\,M_{83}$. The first mistake was found in 1886 by Perusin and Seelhoff that M_{61} is prime. Subsequently four further mistakes were found and it need no longer be taken seriously. In 1876 Lucas found a method for testing whether M_p is prime and used it to prove that M_{127} is prime. This remained the largest known prime until 1951. The problem of Mersenne's numbers is connected with that of "perfect" numbers which are defined in the part (a) above. 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[4] prime is the Mersenne number M_p corresponding to

[3] Marin Mersenne (1588-1648) was a French monk who is best known for his role as a clearing house for correspondence between eminent philosophers and scientists and for his work in number theory.

[4] The largest known prime, as of 2009 (update), was discovered 23 August 2008 by the distributed computing project Great Internet Mersenne Prime Search (This discovery was part of the Great Internet Mersenne Prime Search (GIMPS)): $2^{43,112,609}-1$. This number has $12,978,189$ digits and is the 47-th known Mersenne prime by size as of June 2009 (update). Just a few weeks later, on 6 September 2008 a smaller Mersenne prime was discovered, $2^{37,156,667}-1$, also by GIMPS. This was the second largest known prime at the time, until $2^{42,643,801}-1$ was found

$p = 43,112,609$; this prime number has $[\log_{10}((2^{43,112,609})] + 1 = [43,112,609 \cdot \log_{10} 2] + 1 = 12,978,189$ digits!)

(c) (Fermat Numbers) Let $a, n \in \mathbb{N}^*$ with $a \geq 2$. If $a^n + 1$ is prime, then a is even and n is a power of 2. (**Hint :** If a is odd then $a^n + 1$ is even and if $n = 2^t \cdot m$ with $t, m \in \mathbb{N}$ and m odd, then (put $k := 2^t$) $2^n + 1 = 1 - (-2^k)^m = (1 + 2^k)(1 - 2^k + 2^{2k} - \cdots + 2^{(m-1)k})$ and if $m > 1$, then $k < n$ and hence $1 < 1 + 2^k < 1 + 2^n$. Therefore $m = 1$. – **Remarks :** The natural number of the form $2^{2^n} + 1$, $n \in \mathbb{N}$ is called the n-th Fermat number and is denoted by $F_n := 2^{2^n} + 1$, $n \in \mathbb{N}$. The Fermat numbers corresponding to $n = 0, 1, 2, 3, 4$ are $F_0 = 2, F_1 = 5, F_2 = 17, F_3 = 257, F_4 = 65537$ are prime (already discovered by Fermat[5] himself) and hence conjectured that all were prime, but in 1732 Euler proved that : $F_5 = 2^{2^5} + 1 = 2^{32} + 1 = 641 \cdot 6700417$, since $641 = 5^4 + 2^4 = 5 \cdot 2^7 + 1$ divides $5^4 \cdot 2^{28} + 2^{32}$ and $5^4 \cdot 2^{28} - 1$ and hence the difference $2^{32} + 1 = F_5$. In 1880 Landry proved that $F_6 = 2^{2^6} + 1 = 274177 \cdot 67280412310721$. More recently it is proved that F_n is composite for $7 \leq n \leq 16$ $n = 18, 19, 23, 36, 38, 39, 55, 63, 73$ and many larger values of n. Morehead and Western proved that F_7 and F_8 are composite without determining a factor. No factor is known for F_{13} or for F_{14}, but in all the other cases proved to be composite a factor is known. No prime F_n has been found beyond F_4, so that Fermat's conjecture has not proved a very happy one. There are practical "primality tests" for Mersenne and Fermat numbers developed by Lucas and Pepin, see Test-Exercise T5.38 for more details. It is perhaps more probable that the number of Fermat primes F_n is finite. Fermat numbers are of great interest in many ways, for example, it was proved by Gauss[6] that : *if $F_n = p$ is a prime, then a regular polygon of p sides can be inscribed in a circle by Euclidean methods* (constructions by ruler and compass). The property of the Fermat numbers which is relevant here is : *No two Fermat numbers have a common divisor greater than* 1, i.e., $\gcd(F_n, F_m) = 1$, $n \neq m$. For, suppose that d divides both the Fermat numbers F_n and F_{n+k}, $k > 0$. Then putting $x = 2^{2^n}$, we have

$$\frac{F_{n+k} - 2}{F_n} = \frac{2^{2^{n+k}} - 1}{2^{2^n} + 1} = \frac{x^{2^k} - 1}{x + 1} = x^{2^k - 1} - x^{2^k - 2} + \cdots - 1$$

and so $F_n \big| F_{n+k} - 2$. This proves that $d \big| F_{n+k}$ and $d \big| F_{n+k} - 2$ and therefore $d \big| 2$. But F_n is odd and so $d = 1$. Therefore each of the Fermat numbers $F_0, F_1, \ldots, F_n$ is divisible by an odd prime number which does not divide any of the others and hence there are at least n odd primes not exceeding F_n. This proves (proof due to George Pólya[7]) Euclid's theorem (see Test-Exercise T5.24-(b)). Moreover, we have the inequality $p_{n+1} \leq F_n = 2^{2^n} + 1$ which is little stronger than the inequality in Test-Exercise T5.25-(a).))

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

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

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

---

to be prime by GIMPS in April 2009. The predecessor as largest known prime, $2^{32,582,657} - 1$, was first shown to be prime on 4 September 2006 by GIMPS also. GIMPS found the 11 latest records on ordinary computers operated by participants around the world. Such huge prime numbers are used in problems related to Cryptography.

[5] Pierre de Fermat (1601-1665) was a French lawyer and government official most remembered for his work in number theory; in particular for Fermat's Last Theorem. He is also important in the foundations of the calculus.

[6] What no one suspected before Gauss (see Footnote No.[30]) was that a regular 17-gon can be constructed by ruler and compass. Gauss was so proud of his discovery that he requested that a regular polygon of 17 sides be engraved on his tombstone; for some reason, this wish was never fulfilled, but such a polygon is inscribed on the side of a monument to Gauss erected in Brunswick, Germany, his birthplace.

[7] George Pólya (1888-1985) was a Hungarian Jewish mathematician. He was a professor of mathematics from 1914 to 1940 at ETH Zürich and from 1940 to 1953 at Stanford University. He made fundamental contributions to combinatorics, number theory, numerical analysis and probability theory. He is also noted for his work in heuristics and mathematics education.

(c) From the part (a) deduce that $\sum_{i=0}^{\infty} \frac{m^i}{a_i} = \frac{m+1}{n}$.

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

5.8 (Periodic Sequences) Let us fix the terminology for periodic sequences which is used at many places: For an arbitrary sequence $(x_i)_{i\in\mathbb{N}}$ of elements of a set X, a pair $(m_0, n) \in \mathbb{N}\times\mathbb{N}^*$ is called a pair of periodicity for (x_i) if $x_{i+n} = x_i$ for all $i \geq m_0$. In this case m_0 is called a pre-period length and n a period length of (x_i). If no such pair of periodicity for (x_i) exists, then (x_i) is called aperiodic, otherwise (x_i) is called periodic.

(a) Show that for a periodic sequence $(x_i)_{i\in\mathbb{N}}$, there exists a *unique* pair of periodicity $(k_0, \ell) \in \mathbb{N}\times\mathbb{N}^*$ with the following property: Any pair of periodicity for (x_i) is of the form $(m_0, m\ell)$ with $m_0 \geq k_0$ and $m \in \mathbb{N}^*$. (**Hint :** The main point to show is the following: If $r, s \in \mathbb{N}^*$ are period lengths of (x_i), then $\operatorname{GCD}(r,s)$ is also a period length of (x_i).) – The natural number k_0 is called *the* pre-period length of (x_i) and the natural number ℓ is called *the* period length. The pair (k_0, ℓ) itself is called the (periodicity) type of (x_i). The (finite) subsequence $(x_0, \ldots, x_{k_0-1})$ is called *the* pre-period of (x_i) and the (finite) subsequence $(x_{k_0}, \ldots, x_{k_0+\ell-1})$ is called *the* period of (x_i). In this case we simply write $(x_i)_{i\in\mathbb{N}} = (x_0, \ldots, x_{k_0-1}, \overline{x_{k_0}, \ldots, x_{k_0+\ell-1}})$. If $k_0 = 0$ then (x_i) is called purely periodic. The periodicity type of an aperiodic sequence is often denoted by $(\infty, 0)$. In particular, by definition, the period length of an aperiodic sequence is 0.

(b) If x is an element of a group, the sequence $(x^i)_{i\in\mathbb{N}}$ of its powers has period length $\operatorname{ord} x$ and is purely periodic if $\operatorname{ord} x > 0$. For an element x of a monoid the periodicity type of the sequence $(x^i)_{i\in\mathbb{N}}$ characterizes the cyclic monoid generated by x up to isomorphism and any type in $\mathbb{N}\times\mathbb{N}^* \cup \{(\infty, 0)\}$ may occur.

(c) For an integer $r \in \mathbb{N}^*$, compute the periodicity type of the sequence $(x_{ri})_{i\in\mathbb{N}}$ in terms of the periodicity type (k_0, ℓ) of $(x_i)_{i\in\mathbb{N}}$.

5.9 (The Sieve of Eratosthenes[8]) The so-called *sieve of Eratosthenes* is an alogrithm for singling out the prime from among the set of natural numbers $\leq N$ for arbitrary natural number N. It depends on the fact that if a natural number $n > 1$ has no division d with $1 < d \leq \sqrt{n}$, then n must be a prime number (See Test-Exercise T5.19-(d)). Let N be a positive natural number and let $\pi(N)$ denote the number of prime numbers $\leq N$. Let $p_1, \ldots, p_r$ be all distinct prime numbers $\leq \sqrt{N}$, i.e, $r = \pi(\sqrt{N})$. Prove the following well-known formula :

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

(**Proof :** For each $i = 1, \ldots, r$, let $M_i := \{n \in \mathbb{N}^* \mid n \leq N \text{ and } p_i | n\} = \{p_i, 2p_i, \ldots, \left[\frac{N}{pi}\right]\cdot p_i\}$ and hence $|M_i| = \left[\frac{N}{p_i}\right]$. For an index ν-tuple $(i_1, \ldots, i_\nu)$ with $1 \leq i_1 < i_2 < \cdots < i_\nu \leq r$, we have $M_{i_1}\cap\cdots\cap M_{i_\nu} = \{n \in \mathbb{N}^* \mid n \leq N \text{ and } p_{i1}|n, \ldots, p_{i_nu}|n \text{ equivalently } p_{i_1}\cdots p_{i_\nu}|n\}$ and so $|M_{i_1}\cap\cdots\cap M_{i_\nu}| = \left[\frac{N}{p_{i_1}\cdots p_{i_\nu}}\right]$. This proves that $\pi(N) = N - 1 - |\cup_{i=1}^r M_i| + r$. Now use the Sylvester's sieve formula, see Exercise 4.3.)

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

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

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

In particular, (L e g e n d r e ' s f o r m u l a [9]) : $n! = \prod_{p\leq n} p^{\sum_{r\geq 1}[n/p^r]}$.

(**Proof :** Note that $\left[\frac{n}{p^r}\right] = 0$ if $p^r > n$ and hence the sum on the RHS is really a finite sum. The assertion is proved by induction. It is trivial for $1!$. Assume $n > 1$ and the assertion is true for $(n-1)!$ and let $j = v_p(n)$, i.e., $p^j | n$ but $p^{j+1} \nmid n$. Since $n! = n\cdot(n-1)!$, it is enough to prove that $\sum\left[\frac{n}{p^i}\right] - \sum\left[\frac{(n-1)}{p^i}\right] = j$. But $\left[\frac{n}{p^i}\right] = \left[\frac{(n-1)}{p^i}\right] = \begin{cases} 1, & \text{if} \quad p^i | n, \\ 0, & \text{if} \quad p^i | n, \end{cases}$ and hence $\sum\left[\frac{n}{p^i}\right] = \sum\left[\frac{(n-1)}{p^i}\right] = j$. This proof is rather short and artificial.

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

(b) Show that $(2n)!/(n!)^2$ is an even integer. Further, show that

$$v_p((2n)!/(n!)^2) = \sum_{k\geq 1}\left(\left[\frac{2n}{p^k}\right] - 2\left[\frac{n}{p^k}\right]\right)$$

and if $n < p < 2n$, then show that $v_p((2n)!/(n!)^2) = 1$.

(c) Let $n = (r_t, \ldots, r_0)_p$ be the p-adic expansion of n, where $0 \leq r_i < p$ for all $i = 0, \ldots, t$. Then show that

$$v_p(n!) = \big(n - \sum_{i\geq 0} r_i\big)/(p-1).$$

(**Hint:** The sum on the right hand side of part (a) can be easily computed by recursion :

$$\sum_{i\geq 1}\left[\frac{n}{p^i}\right] = \big(n - \sum_{i\geq 0} r_i\big)/(p-1).)$$

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

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

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

(g) Let $n, k\in\mathbb{N}^*$, $k\leq n$. Every prime power p^r that divides $\binom{n}{k}$ is $\leq n$. (**Hint :** Use the part (a).)

---

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

(h) For each prime power $p^\alpha > 1$ and every $k \in \mathbb{N}^*$, $1 \leq k \leq p^\alpha$, show that

$$v_p\left(\binom{p^\alpha}{k}\right) = p^{\alpha - v_p(k)}.$$

5.11 (a) Compute the canonical prime decomposition of:

(i) $50!$. (ii) the product $1\cdot 3\cdot 5\cdots 99$ of the first 50 odd natural numbers.

(iii) the least common multiple $\mathrm{lcm}(1,2,3,\ldots,50)$ the first 50 positive natural numbers.

(b) The product of two relatively prime natural numbers a and b is the n-th power of a natural number $n \in \mathbb{N}^*$ if and only if this hold separately for a and b as well.

***5.12** Congruences are often used to append extra check digit to identification numbers, in order to recognize transmission errors or forgeries. Personal identification numbers of some kind on passports, credit cards, bank accounts and other variety of settings.

(a) Some banks use eight digit identification number $a_1a_2\cdots a_8$ together with a final check digit a_9. The check digit is the weighted sum of the eight modulo 10, i. e. $a_9 \equiv \sum_{i=1}^{8} x_i a_i \pmod{10}$.
Suppose that $a_9 \equiv 7a_1 + 3a_2 + 9a_3 + 7a_4 + 3a_5 + 9a_6 + 7a_7 + 3a_8 \equiv \pmod{10}$. Then:

(i) Verify that the identification number 815042169 have the check digit 9. Obtain the check digits that should be appended to the numbers 55382006 and 81372439.

(ii) The weighting scheme for assigning check digit detects any single-digit error[10] in the identification number. For example, suppose that the digit a_i is replaced by a different digit a_i', then the difference between the correct a_9 and the new check digit a_9' is $a_9 - a_9' \equiv k(a_i - a_i') \pmod{10}$, where $k = 7, 3$, or 9 depending position of a_i'. If the valid number is 81504216 were incorrectly entered as 81504316, then the check digit 8 would come up rather than the expected 9.

(iii) The bank identification number $237a_418538$ has an illegible fourth digit. Determine the value of the obscured digit.

(b) The International Standard Book Number (ISBN) used in many libraries consist of none digits $a_1a_2\cdots a_8a_9$ followed by a tenth check digit a_{10} which satisfies $a_{10} \equiv \sum_{i=1}^{9} i\cdot a_i \pmod{10}$. Determine whether each of the ISBNs below correct:
(i) 0-07-232569-0 (United States) (ii) 91-7643-497-5 (Sweden) (iii) 1-56947-3034-10 (England).
When printing the ISBN $a_1a_2\cdots a_8a_9$ two unequal digits were transposed. Show that the check digits detected this error.

5.13 Let $n \in \mathbb{N}^*$ and let $+_n$, $\cdot_n$ denote the binary operations on the quotient set $\mathbb{Z}_n$ under the equivalence relation congruence modulo n, see Test-Exercise T5.35.

(a) We characterize the invertible elements in the multiplicative monoid $(\mathbb{Z}_n, \cdot_n)$ as follows: For $a \in \mathbb{Z}$, show that the following statements are equivalent:

(i) a and n, are relatively prime, i. e. $\gcd(a,n) = 1$.

(ii) The element $[a] \in (\mathbb{Z}_n, \cdot_n)$ is cancelative (or non-zero divisor in the ring $(\mathbb{Z}_n, +_n, \cdot_n)$), i. e. the left multiplication map $\lambda_{[a]} : \mathbb{Z}_n \to \mathbb{Z}_n$, $[x] \mapsto [a]\cdot_n [x] = [ax]$ is injective.

(iii) The element $[a] \in (\mathbb{Z}_n, \cdot_n)$ is invertible (with respect to $\cdot_n$), i. e. there exists $[b] \in \mathbb{Z}_n$ such that $[a]\cdot_n [b] = [b]\cdot_n [a] = [1]$.

(**Hint :** Use Bezout's Lemma, see Test-Exercise T5.16-(a) and also T5.19-(a). — **Remark:** The cardinality of the unit group $\#(\mathbb{Z}_n, \cdot_n)^\times = \#\{r \in \mathbb{N} \mid 0 \leq r \leq n \text{ with } \gcd(r,n) = 1\}$ is usually denoted by $\varphi(n)$. This defined a function $\varphi : \mathbb{N}^* \to \mathbb{N}$, $n \mapsto \varphi(n)$ called the *Euler's totient function*.)

---

[10] The modulo 10 approach is not entirely effective. For, it does not always detect the common error of transposing distinct adjacent entries a and b within the string of digits. For example, the identification numbers 81504216 and 81504261 have the same check digit 9. The problem occurs when $|a-b| = 5$. More sophisticated methods are available with larger moduli and different weights that would prevent this error.

(b) Show that the commutative ring $(\mathbb{Z}_n, +_n, \cdot_n)$ is a field (i. e. every non-zero element $[a] \in \mathbb{Z}_n$ is invertible (with respect to the multiplication $\cdot_n$) if and only if n is a prime number.

5.14 Let p be a prime number.

(a) Let $r, k \in \mathbb{N}$ with $r < k < p$. show that p divides $\binom{p+r}{k}$. In particular, p divides $\binom{p}{k}$ for all $0 < k < p$. (**Hint :** p divides the numerator $(p+r)\cdots(p+r-k+1)$, since $p+r-k+1 < p < p+r$ and p does not divide the denominator k.)

(b) (Fermat's Little Theorem) For every natural number n, p divides $n^p - n$, i. e. $n^p \equiv n$ modulo p. (**Hint :** Use induction and the above part (b). Another proof can be given by using Test-Exercise T5.35-(d).)

(c) Let p and q be distinct prime numbers and let a be an integer with $a^p \equiv a \,(\mathrm{mod}\ q)$ and $a^q \equiv a \,(\mathrm{mod}\ p)$. Show that $a^{pq} \equiv a \,(\mathrm{mod}\ pq)$.

(d) Let p and q be two distinct prime numbers. For every integer a, prove that

$a^{pq} - a^p - a^q + a \equiv 0 \,(\mathrm{mod}\ pq)$. (**Hint :** Use the Fermat's Little Theorem, see the part (b).)

5.15 **(a)** (Wilson's Theorem[11]) *If p is a prime number, then* $(p-1)! \equiv -1 \,(\mathrm{mod}\ p)$.

(b) The converse of Wilson's Theorem is also true: *If $(n-1)! \equiv -1 \,(\mathrm{mod}\ n)$, then n must be a prime number.* (**Hint :** If n is not prime, then n has a factor d with $1 < d < n$. Further, $d|(n-1)!$ and hence d divides $(n-1)!+1$ too, a contradiction.)

(c) Prove that:

(i) An integer $n > 1$ is prime if and only if $(n-2)! \equiv 1 \,(\mathrm{mod}\ n)$.

(ii) If n is a composite number, then $(n-1)! \equiv 0 \,(\mathrm{mod}\ n)$ except when $n = 4$.

(d) For a prime number p, prove the congruence $(p-1)! \equiv p-1 \,(\mathrm{mod}\ (1+2+\cdots+(p-1)))$.

(e) Let p be a prime number. For any integer a, prove the congruences

(i) $a^p + (p-1)! \cdot a \equiv 0 \,(\mathrm{mod}\ p)$. (ii) $(p-1)! \cdot a^p + a \equiv 0 \,(\mathrm{mod}\ p)$.

(**Hint :** By Wilson's Theorem (see the part (a)) $a^p + (p-1)! \cdot a \equiv a^p - a \,(\mathrm{mod}\ p)$.)

(f) Prove that the quadratic congruence $X^2 + 1 \equiv 0 \,(\mathrm{mod}\ p)$, where p is an odd prime, has a solution if and only if $p \equiv 1 \,(\mathrm{mod}\ 4)$.

Below one can see auxiliary results and (simple) Test-Exercises.

[11] The English mathematician Edward Waring (1743-1798) announced an interesting property of prime numbers in his *Mediationes Algebraicae*, Cambridge, 1770, which was reported to him by his student John Wilson (1741-1793): *If p is a prime number, then p divides* $(p-1)!+1$. It appears that neither Wilson nor Waring knew how to prove it. Confessing this inability, Waring wrote "Theorems of this kind will be very hard to prove because of absence of a notations to express prime numbers." reading this passage, Gauss uttered his comment on "notationes versus notiones", implying that it was the notion that really mattered, not the notation. Soon afterward in 1771, Lagrange[12] gave a proof of what in literature is called "Wilson's Theorem" and observed that the converse also holds.

Auxiliary Results/Test-Exercises

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[13] and his disciples.

Plato[14] said "God is a geometer" – Jacobi[15] changed this to "God is a arithmatician". Then came Kronecker[16] and fashioned the memorable expression "God created the natural numbers and all the rest is the work of man". Felix Klein[17] (1849-1925)

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

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 $M = \mathbb{N}$.

---

[13] Pythagoras of Samos (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.

[14] Plato (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.

[15] Carl Gustav Jacob Jacobi (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.

[16] Leopold Kronecker (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.

[17] Felix Christian Klein (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.

(**Remark :** These axioms are known as Peano's axioms and were introduced by Giuseppe Peano[18] 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, see the Footnote No.[19]) :

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 unique ness is precisely formulated in Test-Exercise T5.8.

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 $\ldots$ $n := \{0, 1, 2, \ldots, n-1\} = (n-1)^+$.

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 Test-Exercise T5.2 -(b), 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)

(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*

[18] 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.

$n \geq n_0$, $\mathrm{S}(n+1)$ *is true whenever* $\mathrm{S}(n)$ *is true. Then* $\mathrm{S}(n)$ *is true for all* $n \geq n_0$. For the proof consider the set $M := \{n \in \mathbb{N} \mid n < n_0\} \cup \{n \in \mathbb{N} \mid n \geq n_0$ and $\mathrm{S}(n)$ is true $\}$.)

(b) (Minimum 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 $\mathrm{S}(n)$ 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 $\mathrm{S}(n)$ 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 $M \subset \mathbb{N}$ 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 Test-Exercise T5.7-(d). 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 $\mathrm{S}(n)$. Assume that for every $n \in \mathbb{N}$, if the $\mathrm{S}(m)$ is true for all $m < n$, then $\mathrm{S}(n)$ is also true. Then $\mathrm{S}(n)$ is true for all $n \in \mathbb{N}$.* (**Hint :** Let $M := \{n \in \mathbb{N} \mid \mathrm{S}(n)$ 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)** $\prod_{k=0}^{n}(1+q^{2^k}) = \frac{q^{2^{n+1}}-1}{q-1}$. **(c)** $\sum_{k=1}^{n} kq^k = \frac{nq^{n+2}-(n+1)q^{n+1}+q}{(q-1)^2}$.

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[19] :

(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.*

$$\begin{tikzcd} \mathbb{N} \arrow[r, "s"] \arrow[d, "f"'] & \mathbb{N} \arrow[d, "f"] \\ X \arrow[r, "F"] & X \end{tikzcd}$$

(**Hint :** Uniqueness of f is clear by induction. For existence, put $I_n := \{0,1,\dots,n\}$. 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 $f : \mathbb{N} \to X^X$ 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) Show that the 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, verify the standard properties $+$ and $\cdot$,

[19] 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.

e.g., 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 b)) $s^m = \underbrace{s \circ s \circ \cdots \circ s}_{m\text{-times}}$ of the successor map s. For $m, n \in \mathbb{N}$, define the multiplication $m \cdot n := s_n^m(0) = (s^n)^m(0)$.)

(e) Show that 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, 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 $m^n := p_m^n(1)$.)

(f) 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 (Uniqueness of the model $(\mathbb{N}, 0, s)$) Use Recursion Theorem (see Test- Exercise T5.7-(a)) to show that the model $(\mathbb{N}, 0, s)$ of a set natural numbers (defined in Test-Exercise 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

$$\begin{tikzcd} \widetilde{\mathbb{N}} \arrow[r, "\widetilde{s}"] \arrow[d, "\widetilde{f}"'] & \widetilde{\mathbb{N}} \arrow[d, "\widetilde{f}"] \\ X \arrow[r, "F"] & X \end{tikzcd}$$

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 diagramm

$$\begin{tikzcd} \mathbb{N} \arrow[r, "s"] \arrow[d, "\Phi"'] & \mathbb{N} \arrow[d, "\Phi"] \\ \widetilde{\mathbb{N}} \arrow[r, "\widetilde{s}"] & \widetilde{\mathbb{N}} \end{tikzcd}$$

is commutative.

T5.9 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 $g((0,0)) = a$,

$$g((0, n+1)) = F(g(0,n)) \quad \text{for all} \quad n \in \mathbb{N} \quad \text{and} \quad g((m+1, n)) = G(g(m,n)) \quad \text{for all} \quad m, n \in \mathbb{N}.$$

Use double recursion to obtain directly the operations of addition $+$ and $\cdot$ on $\mathbb{N}$.
(**Hint :** By Recursion Theorem (Test-Exercise 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 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) 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 $n!$.)

T5.10 (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 $f_1 \circ f_2 \circ \cdot \circ f_n$. 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 Test-Exercise T5.7-(c)).)

T5.11 (Fibonacci[20] Sequence) The sequence f_n, $n \in \mathbb{N}$, defined recursively by $f_0 = 0$, $f_1 = 1$ and $f_{n+1} = f_n + f_{n-1}$ for all $n \geq 1$, is called the Fibonacci Sequence[21] and its n-th term f_n is called the n-th Fibonacci number. The first few terms of the Fibonacci Sequence are $0, 1, 2, 3, 5, 8, 13, 21, 34, 55, \ldots$. (**Remark :** The Recursion Theorem (see Test-Exercise T5.7-(a)) cannot directly justify its existence, for the value f_{n+1} for $n \geq 1$ depend not only on f_n, but upon f_{n-1} as well. However, we can justify the simultaneous existence of the two sequences f_n and g_n satisfying :

$$\begin{cases} f_0 = 0, f_{n+1} = f_n + g_n, & \text{for} \quad n \geq 0, \\ g_0 = 1, g_{n+1} = f_n, & \text{for} \quad n \geq 0. \end{cases}$$

[20] Leonard of Pisa or Fibonacci (1170-1250) an Italian Salesman who wrote a book on “Liber Abaci” in 1209 and introduced the Hindu-Arabic place-valued decimal system and the use of Arabic numerals into Europe. Fibonacci played an important role in reviving ancient mathematics and made significant contributions of his own.

[21] In 1844 Gabriel Lamé observed that if n division steps are required in the Euclidean algorithm to compute $\gcd(a,b)$, $a, b \in \mathbb{N}^*$, then $a \geq f_{n+2}$ and $b \geq f_{n+1}$. Therefore the sequence was called the *Lamé sequence*. But Lucas discovered that Fibonacci had been aware of these numbers six centuries earlier.

For this we can use the Simultaneous Recursion (see Test-Exercise T5.9-(b)) by taking $(a,b)=(0,1)$, $H:\mathbb{N}\times\mathbb{N}\to\mathbb{N}$ is the addition on $\mathbb{N}$ and $K:\mathbb{N}\times\mathbb{N}\to\mathbb{N}$ is the first projection.)

(a) For the n-th Fibonacci number f_n, prove the following explicit (Binet's Formula[22]):

$$f_n=\frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^n-\left(\frac{1-\sqrt{5}}{2}\right)^n\right)$$

(b) Prove the following equalities by induction :

(i) $f_{n+m}=f_{n-1}f_m+f_nf_{m+1}$ for all $m\geq 0$ and all $n\geq 1$.
In particular, $f_{2n}=f_n(f_{n-1}+f_{n+1})=f_{n+1}^2-f_{n-1}^2$ for all $n\geq 1$.

(ii) $f_n^2=f_{n-1}f_{n+1}+(-1)^{n+1}$ for all $n\geq 1$.

(iii) $\varphi^n=f_{n-1}+f_n\varphi$, for all $n\in\mathbb{N}^*$, where $\varphi:=(1+\sqrt{5})/2$. (**Remark :** Using this equality we can define the Fibonacci-numbers f_n for all $n\in\mathbb{Z}$. We then have $f_n=f_{n-1}+f_{n-2}$ for all $n\in\mathbb{Z}$.)

(iv) $f_n+f_{n+1}+f_{n+3}=f_{n+4}$. (v) $f_2+f_4+\cdots+f_{2n}=f_{2n+1}-1$.

(vi) $f_1+f_3+\cdots+f_{2n-1}=f_{2n}$. (vii) $f_1-f_2+f_3-\cdots+(-1)^nf_{n+1}=(-1)^nf_n+1$.

(viii) $f_n<(5/3)^n$. (ix) $2^nf_n<(\sqrt{5}+1)^n$.

(c) $f_n=(a^n-b^n)/\sqrt{5}$, where a and b are the positive and negative zeros of the quadratic equation $X^2-X-1=0$. (**Hint :** Use Binet's Formula.)

(d) (Lucas ; 1876) prove the following formula for the Fibonacci numbers in terms of binomial coefficients:

$$f_n=\binom{n-1}{0}+\binom{n-2}{1}+\cdots+\binom{n-[\frac{n-1}{2}]}{[\frac{n-1}{2}]-1}+\binom{n-[\frac{n-1}{2}]-1}{[\frac{n-1}{2}]}.$$

(**Hint :** Use induction with $f_n=f_{n-1}+f_{n-2}$ and $\binom{m}{k}=\binom{m-1}{k}+\binom{m-1}{k-1}$.)

(e) For $n\geq$, prove the formulas:

$$f_{2n}=\binom{n}{1}\cdot f_1+\binom{n}{2}\cdot f_2+\cdots+\binom{n}{n}\cdot f_n \ \text{ and } \ -f_n=-\binom{n}{1}\cdot f_1+\binom{n}{2}\cdot f_2+\cdots+(-1)^n\binom{n}{n}\cdot f_n$$

(**Hint :** Use the Binet's formula and the Binomial Theorem $(1+X)^n=\sum_{k=0}^n\binom{n}{k}X^k$.)

(f) $\mathfrak{A}^n=\begin{pmatrix} f_{n+1} & f_n\\ f_n & f_{n-1}\end{pmatrix}$, where $\mathfrak{A}:=\begin{pmatrix}1&1\\1&0\end{pmatrix}$

(g) $\#(\mathfrak{F}_n)=f_{n+2}$, where $\mathfrak{F}_n:=\{A\in\mathfrak{P}(\{1,2,\ldots,n\})\mid\{i,i+1\}\not\subseteq A$ for every $1\leq i\leq n-1\}$.

T5.12 Let X be a non-empty set.

(a) If X is not finite, then show that there exists an injective map $\mathbb{N}\to X$. (**Hint :** Consider the set $\mathfrak{P}_{\mathrm{f}}(X):=\{A\in\mathfrak{P}(X)\mid A$ is finite$\}$ of all finite subsets of X. Then for every $A\in\mathfrak{P}_{\mathrm{f}}(X)$, the complement $X\setminus A$ is a non-empty subset of X and by the *axiom of choice* there exists a *choice function* $g:\mathfrak{P}_{\mathrm{f}}(X)\to\bigcup_{A\in\mathfrak{P}_{\mathrm{f}}(X)}(X\setminus A)$, i.e., $g(A)\in X\setminus A$ for every $A\in\mathfrak{P}_{\mathrm{f}}(X)$. Now, apply recursion theorem to the map $F:\mathfrak{P}_{\mathrm{f}}(X)\to\mathfrak{P}_{\mathrm{f}}(X)$ defined by $A\mapsto A\cup\{g(A)\}$, to get a sequence $f:\mathbb{N}\to\mathfrak{P}_{\mathrm{f}}(X)$ in $\mathfrak{P}_{\mathrm{f}}(X)$ such that $f(0)=\emptyset$ and $f(n+1)=F(f(n))$ for all $n\geq 1$. Then $x_n:=g(f(n))\notin f(n)\subseteq\{x_0,\ldots,x_{n-1}\}$. Therefore the map $\mathbb{N}\to X$, $n\mapsto x_n$ is injective.)

(b) Show that the following statements are equivalent:

(i) X is not finite. (ii) There exists a proper subset $Y\subsetneq X$ with a bijective map $Y\to X$.

(**Hint :** Use part (a). – **Remark:** Dedekind defined infinite sets using the condition (ii).)

[22] Binet Jacques Philippe (1786-1856) was a French mathematician who discovered this formula (in 1843) expressing f_n in terms of the integer n.

T5.13 For the recursively defined sequences (a_n) in the parts (a) ,(b) ,(c) below, prove the given explicit representations.

(a) $a_0 = 2$, $a_n = 2 - a_{n-1}^{-1}$, $n \geq 1$. Then $a_n = (n+2)/(n+1)$ for all $n \in \mathbb{N}$.

(b) $a_0 = 0$, $a_1 = 1$, $a_n = \frac{1}{2}(a_{n-1} + a_{n-2})$, $n \geq 2$. Then $a_n = \frac{2}{3}\left(1 - (-1)^n \frac{1}{2^n}\right)$ for all $n \in \mathbb{N}$.

(c) $a_0 = 1$, $a_n = 1 + a_{n-1}^{-1}$, $n \geq 1$. Then $a_n = f_{n+2}/f_{n+1}$ for all $n \in \mathbb{N}$, where for $k \in \mathbb{N}$, f_k is the k-th Fibonacci-number (see Test-Exercise T5.11).

(d) $a_0 = 1$, $a_n = \sum_{k=0}^{n-1} a_k$, $n \geq 1$. Then $a_n = 2^{n-1}$ for all $n \geq 1$.

T5.14 (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 $b \mid (r - r')$. But since $0 \leq r, r' \leq b$ we have $-b \leq r - r' \leq b$ and hence $r - r' = 0$, i.e., $r' = r$. Now from $(q' - q)b = 0$ and $b \neq 0$, it follows that $q' = q$.)

T5.15 (Divisibility) An integer d is called a divisor of $a \in \mathbb{Z}$ in $\mathbb{Z}$, and is denoted by $d \mid a$, if there exists $v \in \mathbb{Z}$ such that $a = dv$. In this case we also say that d divides a or a is a multiple of d (in $\mathbb{Z}$). If d is not a divisor of a, then we write $d \nmid a$. If $0 \neq d$ is a divisor of a, then $v \in \mathbb{Z}$ in the equation $a = dv$ is uniquely determined by the cancelation law. An integer $a, \in \mathbb{Z}$ is called even (respectively odd) if $2 \mid a$ (respectively, $2 \nmid a$), i. e., a is of the form $2v$ (respectively, $2v + 1$).

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

(i) (Reflexivity) $a \mid a$.

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

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

(iv) If $a \mid b$ and $a \mid c$, then $a \mid (xb + yc)$ for all $x, y \in \mathbb{Z}$.

(**Remarks :** The rule (iii) does not hold if one replaces ac (respectively, bd) by $a + c$ (respectively, $b + d$). The number 0 is divisible by every integer $d \in \mathbb{Z}$, since $0 = d \cdot 0$; this is the only case of an integer which has infinitely many distinct divisors. This is proved in the part b) below which is an important connection between divisibility relation $\mid$ and the (standard) order $\leq$ 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 $d \mid a$ and $a \mid d$ then $d = a$. (**Remarks :** Every integer a has the four (distinct) divisors $a, -a, 1, -1$; these are called the trivial divisors of a; other divisors are called proper divisors of a. Therefore from b) it follows that : *If* d *is a proper divisor of* $a \neq 0$, *then* $1 < |d| < |a|$. Since $a = dv$ if and only if $-a = d(-v)$, the integers a and $-a$ 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, $\tau(n)$ and $\sigma(n)$, $n \in \mathbb{N}^*$ in Test-Exercise T5.32)

T5.16 (G C D) 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[23]) 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 $M := \{ua + vb \mid u, v \in \mathbb{Z}$ and $ua + vb \in \mathbb{N}^*\}$ be 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 Test-Exercise T5.19-(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 $a \big| c$ and $b | c$ with $\gcd(a,b) = 1$, then $ab \big| c$. (**Hint :** Use Bezout's Lemma.)

(iv) (Euclid's Lemma) If $a, b, c \in \mathbb{Z}$ and $a \big| bc$ and $\gcd(a,b) = 1$, then $a \big| c$. (**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 Test-Exercise T5.19-(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) $d \big| a$ and $d \big| b$ and (ii) whenever a positive integer c divides both a and b, then $c \big| d$. (**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) $a \big| b \iff a = \gcd(a,b)$.

(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) $a \big| b \iff a = a \sqcap b$;

[23] 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 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.

(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) $\gcd(a, a+n) \big| n$ and hence $\gcd(a, a+1) = 1$.
(iii) If $\gcd(a,b) = 1$ and $\gcd(a,c) = 1$, then $\gcd(a,bc) = 1$. (**Hint :** $1 = sa + tb = ua + vc$ for some $s,t,u,v \in \mathbb{Z}$. Then $1 = (sa+tb)(ua+vc) = (aus + cvs + btu)a + (tv)bc$.)
(iv) If $\gcd(a,b) = 1$, then $\gcd(a^m, b^n) = 1$. (**Hint :** Use the above part (iii).)
(v) The relation $a^n | b^n$ implies that $a|b$. (**Hint :** Let $d := \gcd(a,b)$ and write $a = rd$ and $b = sd$. Then $\gcd(r,s) = 1$ and hence $\gcd(r^n, s^n) = 1$ by (ii). Now show that $r = 1$, whence $a = d$, i.e, $a\big|b$.)
(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 $\gcd(n! + 1, (n+1)! + 1) = 1$.

T5.17 (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 $q,r \in \mathbb{Z}$, $0 \le r < t$. 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 $\mathrm{M}(a) \cap \mathrm{M}(b) = \mathrm{M}(\mathrm{lcm}(a,b))$.

T5.18 The notion of greatest common divisor can be extended to more than two integers in an obvious way. Let $a_1,\ldots,a_n \in \mathbb{N}$, $n \ge 1$, not all zero. Then $\gcd(a_1,\ldots,a_n)$ is defined to be the positive integer d satisfying the following two properties :

(i) $d\big|a_i$ for every $i = 1,\ldots,n$; (ii) if c is a positive integer with $c\big|a_i$ for every $i = 1,\ldots,n$, then $c\big|d$ (equivalently $c \le d$).

Note that $\gcd(a_1,\ldots,a_{n-1},a_n) = \gcd(\gcd(a_1,\ldots,a_{n-1}),a_n) = \cdots = \gcd(a_1,\gcd(a_2,\ldots,a_n))$ by Test-Exercise T5.22-(b)-(iv) and hence the gcd depends only on $a_1,\ldots,a_n$ and not on the order in which they are written.

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

(i) $a_1,\ldots,a_n$ are pairwise relatively prime.

(ii) If each $a_1,\ldots,a_n$ divide the natural number c, then a also divide the number c.

(iii) $\mathrm{lcm}(a_1,\ldots,a_n) = a$.

(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 $\dfrac{1}{a} = \dfrac{s_1}{a_1} + \cdots + \dfrac{s_n}{a_n}$.

(**Remark :** lcm 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 r e l a t i v e l y p r i m e. Note that this concept is different from that of pairwise relatively prime.)

(b) For $a_1,\ldots,a_n \in \mathbb{N}^*$, $n \ge 1$, show that there exist $u_1,\ldots,u_n \in \mathbb{Z}$ such that $\gcd(a_1,\ldots,a_n) = u_1a_1 + \cdots + u_na_n$. In particular, $a_1,\ldots,a_n$ are relatively prime if and only if there exist integers $u_1,\ldots,u_n$ such that $1 = u_1a_1 + \cdots + u_na_n$. (**Remark :** One can find the coefficients $u_1,\ldots,u_n$ algorithmically by successive use of the lemma of Bezout (see Test-Exercise T5.22-(a)). This algorithm supplies frequently disproportionately large coefficients $u_1,\ldots,u_n$. It is better to proceed as follows : First by renumbering assume that a_1 is minimal in $\{a_1,\ldots,a_n\}$, and goes then to tuple $(a_1,r_2,\ldots,r_n)$, where r_j the remainder of a_j after dividing by a_1, after removing the zeros among r_j, consider the new tuple as at the beginning. One has to control, how the coefficients of the tuple constructed are represented as linear combinations of the $a_1,\ldots,a_n$, beginning with $a_i = \sum_{k=1}^n \delta_{ik}a_k$.) Find integers u_1,u_2,u_3 such that $1 = u_1 \cdot 88 + u_2 \cdot 152 + u_3 \cdot 209$.

T5.19 (E u c l i d e a n a l g o r i t h m[24]) Let $a,b \in \mathbb{N}^*$ with $a \ge b$.

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

[24] 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 E u c l i d e a n a l g o r i t h m. The French mathematician G a b r i e l L a m é (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.

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

Then :

(a) $\gcd(a,b) = r_{k+1}$. (**Hint :** By repeated use of the Test-Exercise T5.16-(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 Test-Exercise T5.16-(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) (Euclid's Lemma) (see also Test-Exercise T5.16-(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.)

T5.20 Let $(f_n)_{n\in\mathbb{N}}$ denote the Fibonacci sequence (see Test-Exercise T5.11).

(a) For $m,n \in \mathbb{N}^*$, show that f_{mn} divides f_m. (**Hint :** Use test-Exercise T5.11-(b)-(i) and induction on n.)

(b) $\gcd(f_{n+2}, f_{n+1}) = 1$. (**Hint:** The Euclidean Algorithm for obtaining the gcd leads to the system of n equations: $f_{n+2} = 1\cdot f_{n+1} + f_n\,;\quad f_{n+1} = 1\cdot f_n + f_{n-1}\,;\quad \cdots \quad f_4 = 1\cdot f_3 + f_2 \quad f_3 = 2\cdot f_2\,.$)

(c) $\gcd(f_m, f_n) = f_{\gcd(m,n)}$. (**Hint :** If $m = qn + r$, then $gcd(f_m, f_n) = \gcd(f_{qn-1}f_r + f_{qn}f_{r+1}, f_n)$ by Test-Exercise T5.11-(b)-(i). Further, since f_{mn} divides f_m by (a), it follows (by using $\gcd(a+c,b) = \gcd(a,b)$ if $b|c$) that $\gcd(f_{qn-1}f_r + f_{qn}f_{r+1}, f_n) = \gcd(f_{qn-1}f_r, f_n) = 1$. For the last equality use parts (a) and (b).)

(d) Let $p > 5$ be a prime number. Show that either p divides f_{p-1} or p divides f_{p+1}, but not both. (**Hint :** By Test-Exercise T5.11-(c) $f_p = (a^n - b^n)/\sqrt{5}$, where a (respectively b) is a positive (respectively, negative) root of $X^2-X-1=0$. Expanding a^p and b^p by the Binomial theorem and reading modulo p (using $\binom{p}{k}\equiv 0\,(\text{mod } p)$ and $2^{p-1}\equiv 1\,(\text{mod } p)$), we get $f_p\equiv 5^{(p-1)/2}\equiv \pm 1\,(\text{mod } p)$. Therefore $f_p^2\equiv 1\,(\text{mod } p)$, i. e. p divides f_p^2-1. Finally by Test-Exercise T5.11-(b)-(ii) $f_{p-1}f_{p+1}\equiv 0\,(\text{mod } p)$ and hence one of f_{p-1} and f_{p+1} is divisible by p. Further, since $\gcd(f_{p-1},f_{p+1})=f_{\gcd(p-1,p+1)}=f_2=1$ by (b), the last assertion is clear.)

T5.21 (g-adic-Expansion) Let g be natural number ≥ 2. For every natural number $n\geq 1$, there exist uniquely determined natural numbers r and $a_0,\dots,a_r$ with $a_r\neq 0$ and $0\leq a_i<g$ such that

$$n=a_0+a_1g+\cdots+a_rg^r=\sum_{i=0}^r a_ig^i\ .$$

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 $q_0:=n$:

$$\begin{aligned} q_0&=q_1g+a_0\,, && 0\leq a_0<g\,,\\ q_1&=q_2g+a_1\,, && 0\leq a_1<g\,,\\ &\cdots\cdots && \cdots\cdots\\ q_{r-1}&=q_rg+a_{r-1}\,, && 0\leq a_{r-1}<g\,,\\ q_r&=a_r\,, && 0<a_r<g\,. \end{aligned}$$

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 $n=a_0+a_1g+\cdots+a_rg^r$ one can compute the number n rapidly by using the recursion[25] :

$$\begin{aligned} n_0&=a_r\ ,\\ n_1&=n_0g+a_{r-1}\ (=a_rg+a_{r-1})\ ,\\ &\cdots\cdots\cdots\\ n_{r-1}&=n_{r-2}g+a_1\ (=a_rg^{r-1}+a_{r-1}g^{r-2}+\cdots+a_2g+a_1)\ ,\\ n_r&=n_{r-1}g+a_0=n\ . \end{aligned}$$

Let $n\in\mathbb{N}^*$ and let $n=a_mg^m+a_{m-1}g^{m-1}+\cdots+a_1g+a_0$, $m\in\mathbb{N}$ 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 $Q'_g(n):=a_0-a_1+\cdots+(-1)^ma_m$. Then:

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

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

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

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

(i) $3|n\iff 3|(a_0+a_1+\cdots+a_m)$; $5|n\iff 5|a_0$; $6|n\iff 6|(a_0+4a_1+4a_2+\cdots+4a_m)$; $9|n\iff 9|(a_0+a_1+\cdots+a_m)$; $11|n\iff 11|(a_0-a_1+\cdots+(-1)^ma_m)$. More generally, if $n=a_mg^m+a_{m-1}g^{m-1}+\cdots+a_1g+a_0$, $m\in\mathbb{N}$ 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.

[25] 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.

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

†(**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: $a_n \geq g-1$ 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 5.8), 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 $x=(a_0,a_1a_2\cdots a_n\cdots)_g$ and $(a_0;a_1a_2\cdots a_r,\overline{a_{r+1}\cdots a_{r+s}})_g$.

(e) 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 $x=(a_0;a_1a_2\cdots a_r,\overline{a_{r+1}\cdots a_{r+s}})_g$.

(f) 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 5.8), 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, $\frac{1}{g^n-1}=(0;\overline{00\cdots 01})_g$.

(g) 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 $y=(0;a_1a_2\cdots a_n\cdots)_g$, where $a_n=1$ if n is prime and 0 otherwise.

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

(h) 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.)

T5.22 (Linear Diophantine Equation) The ancient Greek mathematician Diophantus [26] had initiated the study of solutions (in integers) of equations in one or more indeterminate with 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 $t \geq \mathrm{Max}\,(|x_0|/b,|y_0|/a)$ are positive solutions of the given equation.)

[26] Diophantus of Alexandria (A.D. 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.

(c) The contents of the *Mathematical classic* of Chang Ch'iu-chien[27] (6th century) 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) (Mahaviracharya, 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 $100y+x-68=2(100x+y)$.

T5.23 (Continued Fractions[28]) (see the book[29]) A finite continued fraction is a fraction of the form

$$a_0+\cfrac{1}{a_1+\cfrac{1}{a_2+\cfrac{1}{a_3+\cfrac{1}{\ddots\, \cfrac{1}{a_{n-1}+\cfrac{1}{a_n}}}}}}\,,$$

where $a_0,a_1,\ldots,a_n$ are real numbers with $a_1,\ldots,a_n$ are positive. The numbers $a_1,\ldots,a_n$ are called *partial denominators* of this fraction. Such a fraction is called *simple* if all $a_0,a_1,\ldots,a_n$ are integers.

(a) Every rational number can be can be written as a finite simple continued fraction. (**Hint:** Let $x=a/b$, $a,b\in\mathbb{Z}$, $b\neq 0$, be an arbitrary rational number. Then the Euclidean algorithm for finding $\gcd(a,b)$ gives the equations:

$a=ba_0+r_1\,,\, 0<r_1<b\,;\; b=r_1a_1+r_2\,,\, 0<r_2<r_1\,;\;\cdots\;;\; r_{n-2}=r_{n-1}a_{n-1}+r_n\,,\, 0<r_n<r_{n-1}\,;\; r_{n-1}=r_na_n\,.$

Since each remainder $r_k\in\mathbb{N}^*$, $a_1,\ldots,a_n$ are all positive integers. rewriting the above equations as:

$a/b=a_0+\dfrac{r_1}{b}=a_0+\dfrac{1}{b/r_1}\,;\quad \dfrac{b}{r_1}=a_1+\dfrac{r_2}{r_1}=a_1+\dfrac{1}{r_1/r_2}\,;\;\cdots\;;\quad \dfrac{r_{n-2}}{r_{n-1}}=a_{n-1}+\dfrac{r_n}{r_{n-1}}\,;\quad \dfrac{r_{n-1}}{r_n}=a_n\,.$

Now substituting the values r_i/r_{i+1}, $i=n,\ldots 2,1$ successively from later equations into earlier equations, we get the required multi-decked expression.)

Because continued fractions are unwieldy to print or write, we adopt the convention to denote a continued fraction by a symbol $[a_0;a_1,\ldots,a_n]$. It is a good practice to express the rational numbers $\frac{-19}{51}$ and $\frac{118}{303}$

[27] Zhang Qiujian (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*.

[28] In *Liber Abaci* Fibonacci (see Footnote 20) introduced "continued fractions" – a multiple-decked expressions. Although giving due credit to Fibonacci, most authorities agree that the theory of continued fractions begins with Rafael Bombelli (1526-1572) the last of the great algebraist of renaissance Italy. In his "L'Algebra Opera" (1572), Bombelli attempted to find square roots by means of infinite continued fractions – a method both ingenious and novel. It may be interesting to mention that Bombelli was the first to popularize the work of Diophantus.

[29] Perron, O. : Die Lehre von den Kettenbrüchen, Bd. 1. 3. Aufl. Stuttgart 1954.

as finite simple continued fractions. Further, determine the rational numbers which are represented by the simple continued fractions: $[-2;2,4,6,8]$ and $[0;1,2,3,4,3,2,1]$.

†(**Remarks:** One of the main use of the theory of continued fractions is finding approximate values of irrational numbers. For this the notion of infinite continued fractions is necessary. Moreover, one can prove that: *Every real number x is the value of an uniquely determined normalized simple continued fractions. Moreover, this continued fraction is finite if and only if x is rational.* Therefore $x = \lim_{n\to\infty}[a_0;a_1,\cdots,a_n]$.

(b) (i) Using continued fractions verify that the first 4 digits in the decimal expansion of the following square-roots: $\sqrt{2} = 1.4142\cdots$; $\sqrt{3} = 1.7320\cdots$; $\sqrt{5} = 2.2360\cdots$; $\sqrt{7} = 2.6457\cdots$; $\sqrt{11} = 3.3166\cdots$.

(ii) For $a,b \in \mathbb{N}^*$, show that $[a,b,a,b,a,b\cdots] = (ab+\sqrt{a^2b^2+4ab})/ab$.

(iii) For $n \in \mathbb{N}^*$, show that : $\sqrt{n^2+1} = [n,2n,2n,2n,\cdots] = [n,\overline{2n}]$;

(Euler) : $\sqrt{n^2+2} = [n,n,2n,n,2n,n,2n,\cdots] = [n,\overline{n,2n}]$;

$\sqrt{(n^2+1)^2-1} = [n,1,2n,1,2n,1,2n,\cdots] = [n,\overline{1,2n}]$;

(**Hint :** $n+\sqrt{n^2+1} = 2n+(\sqrt{n^2+1}-n) = 2n+\frac{1}{n+\sqrt{n^2+1}}$.)

(Euler) : $n \geq 2$, $\sqrt{(n^2+1)^2-2} = [n,\overline{1,n-1,1,,2n}]$;

(iv) Let $q,n \in \mathbb{N}$ with $1 \leq q \leq n-q \leq n$ and $\dfrac{n}{n-q} = [1,b_1,b_2,\ldots b_m]$ be the continued fraction expansion of $n/(n-q)$. Show that $\dfrac{n}{q} = [1+b_1,b_2,\ldots b_m]$ is the continued fraction expansion of n/q.

(v) If $x \in \mathbb{R}\setminus\mathbb{Q}$, $x > 1$, is represented by the (infinite) continued fraction $[a_0;a_1,a_2,\cdots,a_n,\cdots]$, then show that $\dfrac{1}{x} = [a_0;a_1,a_2,\cdots,a_n,\cdots]$ is the continued fraction expansion of $1/x$.

(c) The Fibonacci sequence $f_0,f_1,\ldots,f_n,\ldots$ gives the continued fraction expansion of the golden-ratio (see Test-Exercise T5.11) $\varphi := \dfrac{1+\sqrt{5}}{2}$; i. e. $\varphi = [1,1,1,\cdots]$.

(d) The beginning of the continued fraction expansion of the number π is:

$$\pi = [3;7,15,1,292,1,1,1,2,1,3,1,14,2,1,1,2,2,2,2,1,84,\cdots].$$

Note that $[3] = \frac{3}{1} < [3;7,5] = \frac{333}{106} < \pi < [3;7,15,1] = \frac{355}{113} < [3,7] = \frac{22}{7}$, this was already known to Archimedes.

(e) The beginning of the continued fraction expansion of the number e which was found by Euler is:

$$e = [2;1,2,1,1,4,1,1,6,1,1,8,\cdots].$$

(f) It is interesting to ask the question: Which numbers have periodic continued fractions? (see Exercise 5.8). For example, the golden-ratio $\varphi = \frac{1+\sqrt{5}}{2} = [\overline{1}]$. In 1737 Euler proved that: *All irrational numbers x with periodic continued fraction expansion are quadratic irrationalities*, i. e. *are irrational roots of a quadratic equation of the form $X^2+\beta X+\gamma = 0$*, or equivalently, of $aX^2+bX+c = 0$, $a,b \in \mathbb{Z}, b \neq 0$. Moreover, in 1770 Lagrange proved that: *Quadratic irrationalities are exactly the ones which have periodic continued fraction expansion.*

(g) Similar to the Question in the part (c) one can also ask: Which quadratic irrational numbers have pure periodic continued fraction expansion? This was answered by Galois in 1828/29.

T5.24 (Prime numbers) A natural number p is called a prime number or an irreducible (in $\mathbb{N}$) if $p > 1$ and $p = ab$ with $a,b \in \mathbb{N}$, then either $a = 1$ or $b = 1$. A natural number $n > 1$ is called composite or reducible if it is not a prime number. The set of all prime numbers is denoted by $\mathbb{P}$. Then by definition $1 \notin \mathbb{P}$. For a natural number $p > 1$, the following statements are equivalent :

(i) $p \in \mathbb{P}$.

(ii) 1 and p are the only positive divisors of p.

(iii) p has no proper divisor. (**Remark :** On the basis of the property (iii) prime numbers are also called *irreducible*.)

(a) (Existence Theorem) Every natural number $a > 1$ has a smallest (positive) divisor $t > 1$. Moreover, this divisor t is a prime number. (**Proof :** The set $T = \{d \in \mathbb{N}^* \mid d \big| a \text{ and } d > 1\}$ is non-empty, since $a \in T$. Therefore by the Minimum Principle (see Test-Exercise 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) (Euclid's Theorem[30]) There are infinitely many prime numbers, i. e., the set $\mathbb{P}$ is infinite. (**Proof :** In the text of Euclid the word "infinite" is not mentioned; this theorem was formulated as : *Given any finite set of prime numbers, one can always find a prime number which does not belong to the given set.* Show that : *Let $q_1, \ldots, q_n$ be finite set of prime numbers. Then the smallest (positive) divisor $t > 1$ of the natural number $a := q_1 \cdot q_2 \cdots q_n + 1$ is a prime number which is different from all the prime numbers $q_1, \ldots, q_n$.* — Since $a > 1$, 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 Test-Exercise 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 ???.)

T5.25 Let $\mathbb{P}$ denote the set of all prime numbers. Let p_n denote the n-th prime (in the natural order $\le$ on $\mathbb{N}^*$, i. e. starting with $n = 1, 2, \ldots,$). Then show that :

(a) $p_n > 2n - 1$ for $n \ge 5$ and $p_n \le 2^{2^{n-1}}$ for all $n \in \mathbb{N}^*$. (**Hint :** Note that $p_{n+1} \le p_1 \cdot p_2 \cdots p_n + 1$.)

(b) 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 $4m + 3$.)

(c) The sum $\dfrac{1}{p_1} + \dfrac{1}{p_2} + \cdots + \dfrac{1}{p_n}$ is never an integer.

---

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

(d) Another proof of infiniteness of $\mathbb{P}$: Suppose that there are only finitely many primes, say, $p_1, \ldots, p_n$. Now, use the natural number $N = p_2 \cdot p_3 \cdots p_n + p_1 \cdot p_3 \cdots p_n + \cdots + p_2 \cdot p_3 \cdots p_{n-1}$.

T5.26 Let $n \in \mathbb{N}^*$. Show that :

(a) If $n > 1$ and if n divides $(n-1)! + 1$, then n must be a prime number.

(b) If $n > 2$, then there exists a prime number p with $n < p < n!$. (**Hint :** Consider a prime divisor p of $n! - 1$.)

(c) If $n > 1$, then every prime divisor of $n! + 1$ is an odd integer $> n$. (**Remark :** This shows again that there are infinitely many prime numbers. It is unknown whether infinitely many of $n! + 1$ are prime.)

(d) 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.)

(e) 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.

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

T5.27 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[31] 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 $q < n$.

T5.28 (Fundamental Theorem of Arithmetic[32]) 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.*

[31] 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.

[32] 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.

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 Test-Exercise T5.16-(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 Test-Exercise T5.16-(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 example given in the Test-Exercise T5.30. 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 Test-exercise T5.29). This can also be seen in the examples in the Test-Exercises T5.30 and T5.31.

(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

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 $p \in \mathbb{P}$.

T5.29 (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.)

T5.30 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 $(3n_1+1)(3n_2+1) = 3(3n_1 n_2 + n_1 + n_2) + 1$. 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 $4 \big| 100 = 10 \cdot 10$ in M, but $4 \not| 10$ in M, i.e., the element 4 is irreducible in M, but does not have the prime property in M. In this example what is missing is that the set M is not additively closed, for example, $4 \in M$, but $8 = 4 + 4 \notin M$ or more generally, $3n_1 = 1 \in M$ and $3n_2 + 1 \in M$, but $(3n_1+1) + (3n_2+1) = 3(n_1+n_2) + 2 \notin M$. We further note that gcd of 40 and 100 does not exists in M and lcm of 4 and 10 does not exits in M (since $4 \not| 10$ in M).

T5.31 Let $q \in \mathbb{N}^*$ be an arbitrary prime number (e. g. $q := 2$ or $q := 1234567891$ [33]) and $N := \mathbb{N}^* - \{q\}$. Then N is a multiplicatively closed and every element in N is a product of irreducible elements of N; such a decomposition is not any more, in general unique. More precisely, prove that: The irreducible elements in N are usual prime numbers $p \neq q$ and their products pq with q and both the elements $q_2 := q^2$ and $q_3 := q^3$. The element $n := q^6 \in N$ has two essentially different decompositions $n = q_2 \cdot q_2 \cdot q_2 = q_3 \cdot q_3$ as product of irreducible elements of N. The irreducible element q_3 divides (in N) the product $q_2 \cdot q_2 \cdot q_2$, but none of its factor. Similarly, q_2 divides (in N) the product $q_3 \cdot q_3$, but not q_3. Similarly, $m := pq^3 = (pq)q^2$ has (in N) two essentially different decompositions (p prime number $\neq q$).

T5.32 **(a)** Let $n, k \in \mathbb{N}^*$ be relatively prime natural numbers. Show that n divides $\binom{n}{k}$ and k divides $\binom{n-1}{k-1}$. (**Hint :** Think about the formula $k\binom{n}{k} = n\binom{n-1}{k-1}$.)

(b) For every natural number n, show that $4 \cdot 7 \cdot 9 = 252$ divides $n^8 - n^2$.

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

(c) Let $r \in \mathbb{N}^*$, $m = (m_1, \ldots, m_r) \in \mathbb{N}^r$ and $n := \sum_{i=1}^r m_i$. Let p be a prime number with $\text{Max}\,(m_1, \ldots, m_r) < p \le n$. Show that p divides $\binom{n}{m} = n!/m_1! \cdots m_r!$.

(d) Find the canonical prime decomposition of the natural number 81 057 226 635 000. (**Ans :** $2^3 \cdot 3^3 \cdot 5^4 \cdot 7^3 \cdot 11^2 \cdot 17 \cdot 23 \cdot 37$.)

(e) If $n = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ is the prime decomposition of the positive natural number n with pairwise distinct prime numbers $p_1, \ldots, p_r$, then show that:

(i) $T(n) := (\alpha_1 + 1) \cdots (\alpha_r + 1)$ is the number of positive divisors of n in $\mathbb{N}^*$.

(ii) $\sigma(n) := \prod_{i=1}^{r} \frac{(p_i^{\alpha_i+1} - 1)}{(p_i - 1)}$ is the sum of all positive divisors of n in $\mathbb{N}^*$.

(f) How many divisors are there for the number given in the part (d)? and what is their sum?

T5.33 **(a)** Let $a \in \mathbb{N}^*$, For how many natural numbers $x \in \mathbb{N}^*$, $x(x+a)$ is a (perfect) square? Compute these x for $a \in \{15, 30, 60, 120\}$. (**Hint :** You may need *Pythagorean triples*, see Test-Exercise T5.38.)

(b) For every $s \ge 2$, a pair $(m_s, n_s) := \big(2(2^{s-1} - 1), 2^{s+1}(2^{s-1} - 1)\big)$ is a pair (m, n) of positive natural numbers such that $m < n$ and m and n as well as $m+1$ and $n+1$ have the same prime divisors. (**Remark :** There are other such pairs (m, n), for example, $(75, 1215)$ is such a pair. See Makowski: Ens. Math. **14**, 193 (1968) .)

T5.34 (Irrational numbers[34]) 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 $a_n \ne 0$, $n \ge 1$, 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 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)[35] $\sqrt{3}, \sqrt{5}, \ldots, \sqrt{p}$, 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.

---

[34] 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".

[35] 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.

(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[36], 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 $[(k!)z]=(k!)z$.

(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. Fourier (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[37] (for $x=1/(Q+1) \leq 1/2$).
– **Remark:** The proof of irrationality of the number π is not quite so easy!)

T5.35 (Congruences) In the first chapter of *Disquisitiones Arithmaticae*[38] Gauss introduced the concept of *congruence*. 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 congruent modulo n, denoted by $a \equiv b (\bmod n)$ if n divides the difference $a-b$, i. e. $a-b=kn$ for some integer $k \in \mathbb{Z}$.

---

[36] 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 B. C.). 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: $223/71 < \pi < 22/7$.

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

[38] This monumental work of the German mathematician Carl Friedrich Gauss (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 [32]

Given an integer $a \in \mathbb{Z}$, let q and r denote the quotient and remainder upon division by n, so that $a = qn + r,\ \ 0 \le r < n$. then $a \equiv r\,(\mathrm{mod}\ n)$. Therefore every integer is congruent modulo n to exactly one of $0, 1, \ldots, n-1$; in particular, $a \equiv 0\,(\mathrm{mod}\ n)$ if and only if n divides a. Further, note that $a \equiv b\,(\mathrm{mod}\ n)$ 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. Some of the elementary properties of equality that carry over to $\equiv$ are:

(i) $a \equiv a\,(\mathrm{mod}\ n)$. (ii) If $a \equiv b\,(\mathrm{mod}\ n)$, then $b \equiv a\,(\mathrm{mod}\ n)$.

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

(**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 congruence classes modulo n: $[r] := r + \mathbb{Z} \cdot n := \{r + kn \mid k \in \mathbb{Z}\}$, $r = 0, \ldots, n-1$. Therefore the quotient set $\mathbb{Z}/\!\equiv\, = \{[r] \mid 0 \le r < n-1\}$; this quotient set is usually denoted by $\mathbb{Z}_n$ and its elements are also called the residue classes modulo n. The system $0, 1, \ldots, n-1$ form a complete representative system for the quotient set $\mathbb{Z}/\!\equiv$.)

(iv) If $a \equiv b\,(\mathrm{mod}\ n)$ and if $c \equiv d\,(\mathrm{mod}\ n)$, then $a + c \equiv b + d\,(\mathrm{mod}\ n)$ and $a \cdot c \equiv b \cdot d\,(\mathrm{mod}\ n)$.

(v) If $a \equiv b\,(\mathrm{mod}\ n)$, then $a + c \equiv b + c\,(\mathrm{mod}\ n)$ and $a \cdot c \equiv b \cdot c\,(\mathrm{mod}\ n)$.

(**Remark :** It follows from (iv) that the binary operations $+_n$ (called the addition modulo n) and $\cdot_n$ (called the multiplication modulo 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 cancellation can be allowed:

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

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

(b) 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 $a_0, \ldots, a_d \in \mathbb{Z}$. If $a \equiv b\ (\mathrm{mod}\ n)$ then show that $P(a) \equiv P(b)\ (\mathrm{mod}\ n)$. Deduce that if a is a solution of the congruence $P(a) \equiv 0\ (\mathrm{mod}\ n)$ and if $a \equiv b\ (\mathrm{mod}\ n)$, then b is also a solution.

(c) (i) Find the remainder when 4444^{4444} is divided by 9. (**Hint :** Use $2^3 \equiv -1 (\mathrm{mod}\ 9)$.)

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

(d) Let $a \in \mathbb{Z}$ be an integer relatively prime to n. Then:

(i) For every $c \in \mathbb{Z}$, the integers $c, c+1, \ldots, c+(n-1)a$ form a complete representative system for $\mathbb{Z}_n$. In particular, any n consecutive integers form a complete representative system for $\mathbb{Z}_n$.

(ii) If $a_1, \ldots, a_n \in \mathbb{Z}$ is a complete representative system for $\mathbb{Z}_n$, then $a \cdot a_1, \ldots, a \cdot a_n$ also form a complete representative system for $\mathbb{Z}_n$.

(iii) 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.

(e) Find the remainders when

(i) $15!$ is divided by 17. (ii) $2 \cdot (26!)$ is divided by 29. (iii) $4 \cdot (29!) + 5!$ is divided by 31.

(f) 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 $(10^{n-1}+2\cdot 10^{n-2}+3\cdot 10^{n-3}+\cdots+n)\cdot(10-1)+(n+1)=\dfrac{10^{n+1}-1}{9}$.)

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

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

(i) 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 $10^{n+1}\cdot m+1$, $m\in\mathbb{N}^*$.)

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

T5.36 **(a)** Faliure of the converse of Fermat's Little Theorem: show that if $n\in\mathbb{N}^*$ and if the congruence $a^n\equiv a\,(\mathrm{mod}\ n)$ holds for some integer which is relatively prime to n, then n need not be prime. (**Hint :** $2^{340}\equiv 1\,(\mathrm{mod}\ 341)$, but $341=11\cdot 31$ is not prime.)

(b) Use Fermat's Little Theorem to:

(i) Verify that 17 divides $11^{104}+1$. (ii) verify that 13 divides $11^{12n+6}+1$ for every $n\in\mathbb{N}$.

(iii) Let p be a prime number and let a be an integer with $\gcd(a,p)=1$. Verify that $x\equiv a^{p-1}b\,(\mathrm{mod}\ p)$ is the unique solution of the linear congruence $aX\equiv b\,(\mathrm{mod}\ p)$.

(iv) Solve the congruence $2X\equiv 1\,(\mathrm{mod}\ 31)$; $6X\equiv 5\,(\mathrm{mod}\ 11)$ and $3X\equiv 17\,(\mathrm{mod}\ 29)$.

(c) The three most recent appearances of Halley's comet were in the years 1835, 1910 and 1986; the next appearance will be in 2061. Prove that $1835^{1910}+1986^{2061}\equiv 0\,(\mathrm{mod}\ 7)$.

(d) Verify the congruence $2222^{5555}+5555^{2222}\equiv 0\,(\mathrm{mod}\ 7)$.

T5.37 Let p be a prime number.

(a) If a and b are integers with $\gcd(a,p=1\gcd(b,p)$ and if $a^p\equiv b^p\,(\mathrm{mod}\ p)$, then $a\equiv b\,(\mathrm{mod}\ p)$.

(b) If p is an odd prime number, then

(i) $1^{p-1}+2^{p-1}+\cdots+(p-1)^{p-1}\equiv -1\,(\mathrm{mod}\ p)$.

(ii) $1^p+2^p+\cdots+(p-1)^p\equiv 0\,(\mathrm{mod}\ p)$.

(iii) $\dbinom{p-1}{k}\equiv(-1)^k\,(\mathrm{mod}\ p)$ for every $1\leq k\leq p-1$.

(c) Let p and q be two distinct odd prime numbers such that $p-1\,\big|\,q-1$ and let a be an integer with $\gcd(a,pq)=1$. Show that $a^{q-1}\equiv 1\,(\mathrm{mod}\ pq)$.

(d) Let p and q be two distinct prime numbers. Show that $p^{q-1}+q^{p-1}\equiv 1\,(\mathrm{mod}\ pq)$.

(e) Verify that $2^{561}\equiv 2\,(\mathrm{mod}\ 561)$ and $3^{561}\equiv 3\,(\mathrm{mod}\ 561)$. (**Remark :** It is an unanswered question whether that exist infinitely many composite numbers n such that n divides both 2^n-2 and 3^n-3.)

T5.38 In this test-Exercise we undertake the task of finding all solutions of the Pythagorean equation $X^2+Y^2=Z^2$ in the positive integers.

(a) (Pythagorean Triples) A triple $(x,y,z)\in\mathbb{Z}^3$ is called a Pythagorean triple if $x^2+y^2=z^2$; the triple is said to be primitive if $\gcd(x,yz)=1$. The characterization of all primitive Pythagorean triples is fairly straight forward: $(x,y,z)\in\mathbb{Z}^3$, $\gcd(x,y,z)=1$, $2|x$, $x>0$, $y>0$, $z>0$ are given by the formulas: $x=2st$, $y=s^2-t^2$, $z=s^2+t^2$ for integers $s>t>0$, $\gcd(s,t)=1$ and $s\not\equiv t\,(\mathrm{mod}\ 2)$. (**Proof:**)

(b) (Pythagorean Triangles) A right angled triangle is called a Pythagorean triangle if all its sides are of integral lengths. An interesting geometric fact concerning Pythagorean triangles is: *The radius of the inscribed circle of a Pythagorean triangle is always an integer.* (**Proof:**)

(c) Let $n\in\mathbb{N}^*$. Show that

(i) There are at least n Pythagorean triples having the same first member. (**Hint :** Let $y_k=2^k(2^{2n-2k}-1)$ and $z_k=2^k(2^{2n-2k}+1)$, $k=0,1,\ldots,n-1$. Then $(2^{n+1},y_k,z_k)$ are all Pythagorean triples.)

(ii) There exists a Pythagorean triangle the radius of whose inscribed circle is n. (**Hint :** If r denotes the radius of the circle inscribed in the Pythagorean triangle having sides a and b and hypotenuse c, then $r=\frac{1}{2}(a+b-c)$. Consider the triple $(2n+1,2n^2+2n,2n^2+2n=1)$.)

†**T5.39** (Primality Tests[39]) Let $n\in\mathbb{N}^*$.

(a) (Lucas's Test) If there exists $a\in\mathbb{Z}$ such that $a^{n-1}\equiv 1\,(\mathrm{mod}\ n)$ and $a^{(n-1)/p}\not\equiv 1\,(\mathrm{mod}\ n)$ for all prime numebrs p which divide $n-1$, then n is a prime number.

(b) (Pepin's Test[40]) The Fermat number $F_n=2^{2^n}+1$ is prime if and only if $3^{(F_n-1)/2}\equiv -1\,(\mathrm{mod}\ F_n)$.

†**T5.40** (Fermat's Last Theorem) [41]

(a)

(b) (Fermat's Method of Infinite Decent)

(c) (Some History) Some highlights of the 19-th century work on FLT are:

- In 1816 – The French Academy announces a first prize for a solution to FLT.
- in 1820s – Sophie Germain shows that if p and $2p+1$ are prime, then $x^p+y^p=z^p$ has no solution with $p\not| xyz$. (This is called the Case I of FLT; the Case II is where $p|xyz$ and is usually much harder.)
- In 1825 – Drichlet and Legendre prove FLT for $n=5$.
- In 1832 – Drichlet attempts to prove FLT for $n=7$ and proves FLT for $n=14$.
- In 1839 – Lamé proves FLT for $n=7$.
- In 1847 – Lamé and Cauchy presents faulty proof of FLT for general n.
- In 1844-1847 – Kummer's work on FLT:

[39] Lucas Edouard (1842-1891) a French number theorist was the first to device an effieint "primality test" that is, a procedure that guarantees whether a number is prime or composite without revealing its factors. His primality criteria for Mersenne and Fermat numbers were developed in a series of 13 papers published between 1876 and 1878. By imposing further restrictions on the base in Fermat's congruence $a^{n-1}\equiv 1\,(\mathrm{mod}\ n)$, it is possible to obtain a definite guarantee of primality of n. This result which was proved in 1876 is known as Lucas's converse of of Fermat's Little Theorem. See also Lucas's book *Théorie des Nombres* (1891).

[40] In 1877, the Jesuit Priest Théophile Pepin (1826-1904) devised the practical test for determining the primality of the Fermant Number F_n.

[41] By the early 1800s, all of Fermat Problems were solved except for FLT, thus justifying the name "Fermat's Last Theorem".

  - In 1847 – **Theorem**: FLT holds for p if $p \not| h$ (such prime are called regular primes).
  - In 1847 – **Theorem**: p is regular if and only if p does not divide the numerators of the Bernoulli-numbers[42] $B_2, B_4, \ldots B_{p-3}$. – As a consequence of this for $p < 100$ only $37, 59, 67$ are irregular primes.

- In 1850 – The French Academy offers a second prize for a solution to FLT.
- In 1856 – at Cauchy's suggestion, the French Academy withdraws the prize and then awards a medal to Kummer.
- In 1857 – Kummer develops a complicated criteria for proving FLT for certain irregular primes. – Some gaps in his proof which are later filled by Vandiver in 1920s. These result establish FLT for $p < 100$.
- Some highlights of the history of FLT after Kummer:

[42]Bernoulli-numbers are defined by the power series expansion of the function $\dfrac{x}{e^x - 1} = \sum_{n=1}^{\infty} \dfrac{B_n}{n!}\, x^n$.