3. Prime Numbers

(135) Using computer software, write a program
  (a) to generate all Mersenne primes up to $2^{525} - 1$;
  (b) to determine the smallest prime number larger than $10^{100} + 1$.

(136) Write a program that generates prime numbers up to a given number N. One can, of course, use Eratosthenes' sieve.

(137) Use a computer to find four consecutive integers having the same number of prime factors (allowing repetitions).

(138) (a) By reversing the digits of the prime number 1009, we obtain the number 9001, which is also prime. Write a program to find the prime numbers in [1,10000] verifying this property.
(b) By reversing the digits of the prime number 163, we obtain the number 361, which is a perfect square. Using computer software, write a program to find all prime numbers in $[1, 10000]$ with this property.

(139) Using a computer, find all prime numbers $p \leq 10\,000$ with the property that p, $p + 2$ and $p + 6$ are all primes.

(140) Let p_k be the k-th prime number. Show that $p_k < 2^k$ if $k \geq 2$.

(141) If a prime number $p_k > 5$ is equally isolated from the prime numbers appearing before and after it, that is $p_k - p_{k-1} = p_{k+1} - p_k = d$, say, show that d is a multiple of 6. Then, for each of the cases $d = 6$, 12 and 18, find, by using a computer, the smallest prime number p_k with this property.

(142) Prove that none of the numbers

$$12321,\ 1234321,\ 123454321,\ 12345654321,\ 1234567654321,$$

$$123456787654321,\ 12345678987654321$$

is prime.

(143) For each integer $k \geq 1$, let n_k be the k-th composite number, so that for instance $n_1 = 4$ and $n_{10} = 18$. Use computer software and an appropriate algorithm in order to establish the value of n_k, with $k = 10^\alpha$, for each integer $\alpha \in [2, 10]$.

(144) For each integer $k \geq 1$, let n_k be the k-th number of the form p^α, where p is prime, α a positive integer, so that for instance $n_1 = 2$ and $n_{10} = 16$. Use computer software and an appropriate algorithm in order to establish the value of n_k, with $k = 10^\alpha$, for each integer $\alpha \in [2, 10]$.

(145) Find all positive integers $n < 100$ such that $2^n + n^2$ is prime. To which class of congruence modulo 6 do these numbers n belong?

(146) Show that if the integer $n \geq 4$ is not an odd multiple of 9, then the corresponding number $a_n := 4^n + 2^n + 1$ is necessarily composite. Then, use a computer in order to find all positive integers $n < 1000$ for which a_n is prime.

(147) Consider the sequence (a_n) defined by $a_1 = a_2 = 1$ and, for $n \geq 3$, by $a_n = n! - (n-1)! + \cdots + (-1)^n 2! + (-1)^{n+1} 1!$. Use a computer in order to find the smallest number n such that a_n is a composite number.

(148) The mathematicians Minác and Willans have obtained a formula for the n-th prime number p_n which is more of a theoretical interest than of a

practical interest:

$$p_n = 1 + \sum_{m=1}^{2^n} \left\lfloor \left[\frac{n}{1 + \sum_{j=2}^{m} \left\lfloor \frac{(j-1)!+1}{j} - \left\lfloor \frac{(j-1)!}{j} \right\rfloor \right\rfloor} \right]^{1/n} \right\rfloor,$$

where as usual $[x]$ stands for the largest integer $\leq x$. Prove this formula.

(149) Develop an idea used by Paul Erdős (1913–1996) to show that, for each integer $n \geq 1$,

$$\prod_{p \leq n} p \leq 4^n.$$

His idea was to write

$$\prod_{p \leq n} p = \prod_{p \leq \frac{n+1}{2}} p \cdot \prod_{\frac{n+1}{2} < p \leq n} p$$

and to use the fact that each prime number $p > (n+1)/2$ appears in the factorization of the binomial coefficient $\binom{n}{(n+1)/2}$. Provide the details.

(150) Show that if four positive integers a, b, c, d are such that $ab = cd$, then the number $a^2 + b^2 + c^2 + d^2$ is necessarily composite.

(151) Show that, for each integer $n \geq 1$, the number $4n^3 + 6n^2 + 4n + 1$ is composite.

(152) Show that if p and q are two consecutive odd prime numbers, then $p + q$ is the product of at least three prime numbers (not necessarily distinct).

(153) Does there exist a positive integer n such that $n/2$ is a perfect square, $n/3$ a cube and $n/5$ a fifth power?

(154) Given any integer $n \geq 2$, show that $n^{42} - 27$ is never a prime number.

(155) Let $\theta(x) := \sum_{p \leq x} \log p$. Prove that Bertrand's Postulate follows from the fact that

$$c_1 x < \theta(x) < c_2 x,$$

where $c_1 = 0.73$ and $c_2 = 1.12$.

(156) Use Bertrand's Postulate to show that, for each integer $n \geq 4$,

$$p_{n+1}^2 < p_1 p_2 \cdots p_n,$$

where p_n stands for the n-th prime number.

(157) Certain integers $n \geq 3$ can be written in the form $n = p + m^2$, with p prime and $m \in \mathbb{N}$. This is the case for example for the numbers 3, 4, 6, 7, 8, 9, 11, 12, 14, 15, 16, 17, 18, 19, 20, 21. Let q^r be a prime power, where r is a positive even integer such that $2q^{r/2} - 1$ is composite. Show that q^r cannot be written as $q^r = p + m^2$, with p prime and $m \in \mathbb{N}$.

(158) Show that if p and $8p - 1$ are primes, then $8p + 1$ is composite.

(159) Show that all positive integers of the form $3k + 2$ have a prime factor of the same form, that all positive integers of the form $4k + 3$ have a prime factor of the same form, and finally that all positive integers of the form $6k + 5$ have a prime factor of the same form.

(160) A positive integer n has a *Cantor expansion* if it can be written as

$$n = a_m m! + a_{m-1}(m-1)! + \cdots + a_2 2! + a_1 1!,$$

where the a_j's are integers satisfying $0 \leq a_j \leq j$.

(a) Find the Cantor expansion of 23 and of 57.

(b) Show that all positive integers n have a Cantor expansion and moreover that this expansion is unique.

(161) If $p > 1$ and $d > 0$ are integers, show that p and $p + d$ are both primes if and only if

$$(p-1)!\left(\frac{1}{p} + \frac{(-1)^d d!}{p+d}\right) + \frac{1}{p} + \frac{1}{p+d}$$

is an integer.

(162) Find all prime numbers p such that $p + 2$ and $p^2 + 2p - 8$ are primes.

(163) Is it true that if p and $p^2 + 8$ are primes, then $p^3 + 4$ is prime? Explain.

(164) Let $n \geq 2$. Show that the integers n and $n + 2$ form a pair of twin primes if and only if

$$4\left((n-1)! + 1\right) + n \equiv 0 \pmod{n(n+2)}.$$

(165) Identify each prime number p such that $2^p + p^2$ is also prime.

(166) For which prime number(s) p is $17p + 1$ a perfect square?

(167) Given two integers a and b such that $(a, b) = p$, where p is prime, find all possible values of:

(a) (a^2, b); (b) (a^2, b^2); (c) (a^3, b); (d) (a^3, b^2).

(168) Given two integers a and b such that $(a, p^2) = p$ and $(b, p^4) = p^2$, where p is prime, find all possible values of:

(a) (ab, p^5); (b) $(a + b, p^4)$; (c) $(a - b, p^5)$; (d) $(pa - b, p^5)$.

(169) Given two integers a and b such that $(a, p^2) = p$ and $(b, p^3) = p^2$, where p is a prime number, evaluate the expressions (a^2b^2, p^4) and $(a^2 + b^2, p^4)$.

(170) Let p be a prime number and a, b, c be positive integers. For each of the following statements, say if is true or false. If it is true, give a proof; if it is false, provide a counter-example.

(a) If $p|a$ and $p|(a^2 + b^2)$, then $p|b$.
(b) If $p|a^n$, $n \geq 1$, then $p|a$.
(c) If $p|(a^2 + b^2)$ and $p|(b^2 + c^2)$, then $p|(a^2 - c^2)$.
(d) If $p|(a^2 + b^2)$ and $p|(b^2 + c^2)$, then $p|(a^2 + c^2)$.

(171) Let a, b and c be positive integers. Show that $abc = (a, b, c)[ab, bc, ac] = (ab, bc, ac)[a, b, c]$.

(172) Let a, b and c be positive integers and assume that $abc = (a, b, c)[a, b, c]$. Show that this necessarily implies that $(a, b) = (b, c) = (a, c) = 1$.

(173) Let a, b and c be positive integers. Show that $(a, b, c) = \dfrac{(a, b)(b, c)(a, c)}{(ab, bc, ac)}$ and that $[a, b, c] = \dfrac{abc\,(a, b, c)}{(a, b)(b, c)(a, c)}$.

(174) Let a, b and c be positive integers. Show that

$$\frac{[a, b, c]^2}{[a, b][b, c][c, a]} = \frac{(a, b, c)^2}{(a, b)(b, c)(c, a)}.$$

(175) Find three positive integers a, b, c such that

$$[a, b, c] \cdot (a, b, c) = \sqrt{abc}.$$

(176) Let $\#n = [1, 2, 3, \ldots, n]$ be the lowest common multiple of the numbers $1, 2, \ldots, n$. Show that

$$\prod_{p \le n} p \le \#n = \prod_{p \le n} p^{[\log n / \log p]}.$$

(177) Let p be a prime number and r a positive integer. What are the possible values of $(p, p + r)$ and of $[p, p + r]$?

(178) Let $p > 2$ be a prime number such that $p|8a - b$ and $p|8c - d$, where $a, b, c, d \in \mathbb{Z}$. Show that $p|(ad - bc)$.

(179) Show that, if $\{p, p+2\}$ is a pair of twin primes with $p > 3$, then 12 divides the sum of these two numbers.

(180) Let n be a positive integer. Show that if n is a composite integer, then $n|(n - 1)!$ except when $n = 4$.

(181) For which positive integers n is it true that

$$\sum_{j=1}^{n} j \;\Big|\; \prod_{j=1}^{n} j?$$

(182) Let $\pi = 3.141592\ldots$ be Archimede's constant, and for each positive real number x, let $\pi_2(x)$ be the function that counts the number of pairs of twin primes $\{p, p + 2\}$ such that $p \le x$. Show that

$$\pi_2(x) = 2 + \sum_{7 \le n \le x} \sin\left(\frac{\pi}{2}(n+2)\left[\frac{n!}{n+2}\right]\right) \cdot \sin\left(\frac{\pi}{2} n \left[\frac{(n-2)!}{n}\right]\right),$$

where $[y]$ stands for the largest integer $\le y$.

(183) Given an integer $n \ge 2$, show, without using Bertrand's Postulate, that there exists a prime number p such that $n < p < n!$.

(184) In 1556, Niccòlo Tartaglia (1500–1557) claimed that the sums

$$1 + 2 + 4,\ 1 + 2 + 4 + 8,\ 1 + 2 + 4 + 8 + 16,\ \ldots$$

stood successively for a prime number and a composite number. Was he right?

(185) Show that if $a^n - 1$ is prime for certain integers $a > 1$ and $n > 1$, then $a = 2$ and n is prime.

REMARK: *The integers of the form $2^p - 1$, where p is prime, are called Mersenne numbers. We denote them by M_p in memory of Marin Mersenne* (1588–1648), *who had stated that M_p is prime for*

$$p = 2, 3, 5, 7, 13, 17, 19, 31, 67, 127, 257$$

and composite for all the other primes $p < 257$. This assertion of Mersenne can be found in the preface of his book Cogita Physico-mathematica*, published in Paris in 1644. Since then, we have found a few errors in the computations of Mersenne: indeed M_p is not prime for $p = 67$ and $p = 257$, while M_p is prime for $p = 61$, $p = 89$ and $p = 109$. One can find in the appendix C of the book of J.M. De Koninck and A. Mercier* [**8**] *the list of Mersenne primes M_p corresponding to the prime numbers p satisfying $2 \le p \le 44\,497$. Note on the other hand that it has recently been discovered that $2^{32\,582\,657} - 1$ is prime (in September 2006), which brings to 44 the total number of known Mersenne primes. It is also known that the primes*

M_p are closely related to the PERFECT NUMBERS*, in the sense that, as was shown by Leonhard Euler (1707–1783), n is an even perfect number if and only if $n = 2^{p-1}(2^p - 1)$, where $2^p - 1$ is a Mersenne prime.*

(186) Show that if there exists a positive integer n and an integer $a \geq 2$ such that $a^n + 1$ is prime, then a is even and $n = 2^r$ for a certain positive integer r.

REMARK: *The prime numbers of the form $2^{2^k} + 1$, $k = 0, 1, 2, \ldots$, are called "Fermat primes". The reason is that Pierre de Fermat claimed in* 1640 *(although saying he could not prove it) that all the numbers of the form $2^{2^k} + 1$ are prime. One hundred years later, Euler proved that*

$$2^{2^5} + 1 = 4294967297 = 641 \cdot 6700417.$$

As of today, we still do not know if, besides the cases $k = 0, 1, 2, 3, 4$, primes of the form $2^{2^k} + 1$ exist. Nevertheless, it is known that $2^{2^k} + 1$ is composite for $5 \leq k \leq 32$; see H.C. Williams [**41**] *and the site* www.prothsearch.net/fermat.html.

(187) Show that the equation $(2^x - 1)(2^y - 1) = 2^{2^z} + 1$ is impossible for positive integers x, y and z. (This implies in particular that a Fermat number, that is a number of the form $2^{2^k} + 1$, cannot be the product of two Mersenne numbers.)

(188) Prove by induction that, for each integer $n \geq 1$,

$$F_0 F_1 F_2 \cdots F_{n-1} = F_n - 2,$$

where $F_i = 2^{2^i} + 1$, $i = 0, 1, 2, \ldots$.

(189) Use the result of problem 188 in order to prove that if m and n are distinct positive integers, then $(F_m, F_n) = 1$.

(190) A positive integer n is said to be *pseudoprime in basis $a \geq 2$* if it is composite and if $a^{n-1} \equiv 1 \pmod{n}$. Find the smallest number which is pseudoprime in each of the bases 2, 3, 5 and 7.

(191) Use Problem 189 to prove that there exist infinitely many primes.

(192) Consider the numbers $f_n = 2^{3^n} + 1$, $n = 1, 2, \ldots$, and show they are all composite and in particular that, for each positive integer n,
(a) $3^{n+1} | f_n$; (b) $p | f_n \Rightarrow p | f_{n+1}$.

(193) Show that there exist infinitely many prime numbers p such that the numbers $p - 2$ and $p + 2$ are both composite.

(194) Show that 641 divides $F_5 = 2^{2^5} + 1$ without doing the explicit division.

(195) Use an induction argument in order to prove that each Fermat number $F_n = 2^{2^n} + 1$, where $n \geq 2$, ends with the digit 7.

(196) Let n be a positive integer and consider the set $E = \{1, 2, \ldots, n\}$. Let 2^k be the largest power of 2 which belongs to E. Show that for all $m \in E \setminus \{2^k\}$, we have $2^k \not| m$. Using this result, show that $\sum_{j=1}^{n} 1/j$ is not an integer if $n > 1$.

(197) Show that, for each positive integer n, one can find a prime number $p < 50$ such that $p | (2^{5n} - 1)$.

(198) Show that the integers defined by the sequence of numbers

$$M_k = p_1 p_2 \cdots p_k + 1 \qquad (k = 1, 2, \ldots),$$

where p_j stands for the j–th prime number, are prime numbers for $1 \leq k \leq 5$ and composite numbers for $k = 6, 7$. What about M_8, M_9 and M_{10}?

(199) Use the proof of Euclid's Theorem on the infinitude of primes to show that, if we denote by p_r the r-th prime number, then $p_r \leq 2^{2^{r-1}}$ for each $r \in \mathbb{N}$.

(200) In Problem 199, we obtained an upper bound for p_r, the r-th prime number, namely $p_r \leq 2^{2^{r-1}}$. Use this inequality to obtain a lower bound for $\pi(x)$, the number of prime numbers $\leq x$. More precisely, show that, for $x \geq 3$, $\pi(x) \geq \log\log x$.

(201) Show that there exist infinitely many prime numbers of the form $4n + 3$.

(202) Show that there exist infinitely many prime numbers of the form $6n + 5$.

(203) Let $f\colon \mathbb{N} \to \mathbb{R}$ be the function defined by

$$f(x) = a_r x^r + a_{r-1}x^{r-1} + \cdots + a_1 x + a_0,$$

where $a_r \neq 0$ and where each a_i, $0 \leq i \leq r$, is an integer. Show that, by an appropriate choice of a_i, $0 \leq i \leq r$, the set $\{f(n) : n \in \mathbb{N}\}$ contains at least r prime numbers.

(204) Consider the positive integers which can be written as an alternating sequence of 0's and 1's. The number 101 010 101 is such a number and observe that $101\,010\,101 = 41 \cdot 271 \cdot 9091$. Besides 101, do there exist other prime numbers of this form?

(205) Find all prime numbers of the form $2^{2^n} + 5$, where $n \in \mathbb{N}$. Would the question be more difficult if one replaces the number 5 by another number of the form $3k + 2$? Explain.

(206) The largest gaps between two consecutive prime numbers $p_r < p_{r+1} < 100$ occur successively when

$$\begin{aligned} p_{r+1} - p_r &= 5 - 3 = 2, \\ p_{r+1} - p_r &= 11 - 7 = 4, \\ p_{r+1} - p_r &= 29 - 23 = 6, \\ p_{r+1} - p_r &= 97 - 89 = 8. \end{aligned}$$

Is it true that these constantly increasing gaps always occur by jumps of length 2? In other words, does the first gap of length $2k$ always occur before the first gap of length $2k + 2$?

(207) Show that $\displaystyle\sum_{\alpha=2}^{\infty} \sum_{p} \frac{1}{p^\alpha} < 1$, where the inner sum runs over all the prime numbers p.

(208) Let

$$f(x) = \pi(x) + \frac{1}{2}\pi(x^{1/2}) + \frac{1}{3}\pi(x^{1/3}) + \frac{1}{4}\pi(x^{1/4}) + \cdots,$$

be a series which is in fact a finite sum for each real number $x \geq 1$ since $\pi(x^{1/n}) = 0$ as soon as $n > \log x / \log 2$. Show that

$$\pi(x) = \sum_{n=1}^{\infty} \frac{\mu(n)}{n} f(x^{1/n}).$$

REMARK: It is possible to show that $f(x)$ is a better approximation of $\pi(x)$ than $Li(x) := \displaystyle\int_2^x \frac{dt}{\log t}$ (see H. Riesel [**31**]).

(209) Let $n \geq 2$ be an integer. Show that the interval $[n, 2n]$ contains at least one perfect square.

(210) If n is a positive integer such that $3n^2 - 3n + 1$ is composite, show that n^3 cannot be written as $n^3 = p + m^3$, with p prime and m a positive integer.

(211) It is conjectured that there exist infinitely many prime numbers p of the form $p = n^2 + 1$. Identify the primes $p < 10\,000$ of this particular form. Why is the last digit of such a prime number p always 1 or 7? Is there any reasonable explanation for the fact that the digit 7 appears essentially twice as often?

(212) Show that, for each integer $n \geq 2$,

$$(n!)^{1/n} \leq \prod_{p \leq n} p^{\frac{1}{p-1}}.$$

(213) For each integer $N \geq 1$, let $S_N = \{n^2 + 2 : 6 \leq n \leq 6N\}$. Show that no more than $\frac{1}{6}$ of the elements of S_N are primes.

(214) Let p be a prime number and consider the integer $N = 2 \cdot 3 \cdot 5 \cdots p$. Show that the $(p-1)$ consecutive integers

$$N + 2, N + 3, N + 4, \ldots, N + p$$

are composite.

(215) Let $n > 1$ be an integer with at least 3 digits. Show that
- (a) $2|n$ if and only if the last digit of n is divisible by 2;
- (b) $2^2|n$ if and only if the number formed with the last two digits of n is divisible by 4;
- (c) $2^3|n$ if and only if the number formed with the last three digits of n is divisible by 8.

Can one generalize?

(216) For each integer $n \geq 2$, let

$$P(n) = \prod_{\substack{p|n \\ p > \log n}} \left(1 - \frac{1}{p}\right).$$

Show that $\lim_{n \to \infty} P(n) = 1$.

(217) Prove that there exists an interval of the form $[n^2, (n+1)^2]$ containing at least 1000 prime numbers.

(218) Use the Prime Number Theorem (see Theorem 17) in order to prove that the set of numbers of the form p/q (where p and q are primes) is dense in the set of positive real numbers.

(219) Show that the sum of the reciprocals of a finite number of distinct prime numbers cannot be an integer.

(220) Use the fact that there exists a positive constant c such that if $x \geq 100$,

$$\sum_{p \leq x} \frac{1}{p} = \log\log x + c + R(x) \quad \text{with } |R(x)| < \frac{1}{\log x} \tag{1}$$

and moreover that, for $x \geq 2$,

$$\pi(x) := \sum_{p \leq x} 1 < \frac{3}{2} \frac{x}{\log x} \tag{2}$$

in order to prove that if $P(n)$ stands for the largest prime factor of n, then

$$\frac{1}{x} \#\{n \leq x : P(n) > \sqrt{x}\} = \log 2 + T(x) \quad \text{with } |T(x)| < \frac{9}{2} \frac{1}{\log x}. \tag{3}$$

Use this result to show that more than $\frac{2}{3}$ of the integers have their largest prime factor larger than their square root, or in other words that the density of the set of integers n such that $P(n) > \sqrt{n}$ is larger than $\frac{2}{3}$.

(221) Prove the following formula (due to Adrien-Marie Legendre (1752–1833)):

$$\pi(x) = \pi(\sqrt{x}) + \sum_{n | p_1 \cdots p_r} \mu(n) \left[\frac{x}{n} \right] - 1,$$

where $r = \pi(\sqrt{x})$.

(222) Consider the following two conjectures:

A. *(Goldbach Conjecture) Each even integer ≥ 4 can be written as the sum of two primes.*

B. *Each integer > 5 can be written as the sum of three prime numbers.*

Show that these two conjectures are equivalent.

(223) Show that $\pi(m)$, the number of prime numbers not exceeding the positive integer m, satisfies the relation

$$\pi(m) = \sum_{j=2}^{m} \left[\frac{(j-1)! + 1}{j} - \left[\frac{(j-1)!}{j} \right] \right],$$

where $[y]$ stands for the largest integer $\leq y$.

(224) Given a sequence of natural numbers $\mathcal{A}$, let $A(n) = \#\{m \leq n : m \in \mathcal{A}\}$, and let us denote respectively by

$$\underline{\mathbf{d}}\, \mathcal{A} = \liminf_{n \to \infty} \frac{A(n)}{n} \quad \text{and} \quad \overline{\mathbf{d}}\, \mathcal{A} = \limsup_{n \to \infty} \frac{A(n)}{n}$$

the *asymptotic lower density* and *asymptotic upper density* of the sequence $\mathcal{A}$. On the other hand, if both these densities are equal, we say that the sequence $\mathcal{A}$ has density $\mathbf{d}\, \mathcal{A} = \underline{\mathbf{d}} \mathcal{A} = \overline{\mathbf{d}} \mathcal{A}$. Prove that:

(a) the density of the sequence made up of all the multiples of a natural number a is equal to $1/a$;

(b) the density of the sequence made up of all the multiples of a natural number a which are not divisible by the natural number a_0 is equal to $\dfrac{1}{a} - \dfrac{1}{[a, a_0]}$;

(c) the density of the sequence made up of all natural numbers which are not divisible by any of the prime numbers $q_1, q_2, \ldots, q_r$ is equal to $\displaystyle\prod_{i=1}^{r} \left(1 - \frac{1}{q_i} \right)$.

(225) Let $\mathcal{A}$ be the set of natural numbers n such that $2^{2k} \leq n < 2^{2k+1}$ for a certain integer $k \geq 0$, so that

$$\mathcal{A} = \{1, 4, 5, 6, 7, 16, 17, \ldots, 31, 64, 65, \ldots, 127, 256, 257, \ldots\}.$$

Show that

$$\underline{\mathbf{d}}\,\mathcal{A} \neq \overline{\mathbf{d}}\,\mathcal{A}.$$

(226) We say that a sequence of natural numbers $\mathcal{A}$ is *primitive* if no element of $\mathcal{A}$ divides another one. Examples of such sequences are: the sequence of prime numbers, the sequence of natural numbers having exactly k prime factors (k fixed), and finally the sequence of integers n belonging to the interval $]k, 2k]$ (k fixed). Show that if $\mathcal{A}$ is a primitive sequence, then $\overline{\mathbf{d}}\,\mathcal{A} \leq \frac{1}{2}$.

(227) Let $\mathcal{A}$ be a primitive sequence (see Problem 226). Show that

$$\sum_{a\in\mathcal{A}} \frac{1}{a\log a} < +\infty.$$

(228) Let $E = \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\}$.
  (a) Show that the sum and the product of elements of E are in E.
  (b) Define the norm of an element $z \in E$ by $\|z\| = \|a+b\sqrt{-5}\| = a^2+5b^2$. We say that an element $p \in E$ is *prime* if it is impossible to write $p = n_1n_2$, with $n_1, n_2 \in E$, $\|n_1\| > 1$, $\|n_2\| > 1$; we say that it is *composite* if it is not prime. Show that, in E, 3 is a prime number and 29 is a composite number.
  (c) Show that the factorization of 9 in E is not unique.

(229) Let A be a set of natural numbers and let $A(x) = \#\{n \leq x : n \in A\}$. Show that, for all $x \geq 1$,

$$\sum_{\substack{n\leq x\\ n\in A}} \frac{1}{n} = \sum_{n\leq x} \frac{A(n)}{n(n+1)} + \frac{A(x)}{[x]+1}.$$

(132) (*Contribution of Imre Kátai, Budapest*). Let

$$S := \sum_{j=1}^{n} (a_j^{(1)} + a_j^{(2)})(a_j^{(1)} + a_j^{(3)}).$$

Then,

$$S = \sum_{j=1}^{n} (a_j^{(1)})^2 + \sum_{j=1}^{n} a_j^{(1)} a_j^{(3)} + \sum_{j=1}^{n} a_j^{(2)} a_j^{(1)} + \sum_{j=1}^{n} a_j^{(2)} a_j^{(3)} = n.$$

But since it is clear that the expression $(a_j^{(1)}+a_j^{(2)})(a_j^{(1)}+a_j^{(3)})$ is a multiple of 4, the result follows.

(133) In order to show that a series made up of nonnegative real numbers converges, we only need to bound it by a series which converges. So let $\ell(n)$ be the number of digits of the positive integer n, in its decimal representation. We first observe that, for each positive integer r, we have

$$\sum_{\substack{n \in A \\ \ell(n)=r}} 1 = 8 \cdot 9^{r-1}.$$

Hence, it follows from this that

$$\sum_{n \in A} \frac{1}{n} = \sum_{r=1}^{\infty} \sum_{\substack{n \in A \\ \ell(n)=r}} \frac{1}{n} < \sum_{r=1}^{\infty} \frac{1}{10^{r-1}} \sum_{\substack{n \in A \\ \ell(n)=r}} 1$$

$$= \sum_{r=1}^{\infty} \frac{8 \cdot 9^{r-1}}{10^{r-1}} = 8 \sum_{r=1}^{\infty} \left(\frac{9}{10}\right)^{r-1} = 80,$$

from which the result follows.

(134) If $a > b$, it is clear that $a - b \geq (a, b)$, and we know that $(a, b)[a, b] = ab$. Hence, since

$$(u_{n+1} - u_n)[u_{n+1}, u_n] \geq (u_{n+1}, u_n)[u_{n+1}, u_n] = u_{n+1} \cdot u_n,$$

we obtain

$$\frac{1}{[u_{n+1}, u_n]} \leq \frac{u_{n+1} - u_n}{u_{n+1} \cdot u_n} = \frac{1}{u_n} - \frac{1}{u_{n+1}}.$$

Therefore the series is bounded above by a convergent series and this is why it converges.

(135) (a) With MAPLE, we have
```
> for i from 3 by 2 to 525 do
> if isprime(2^i-1)
> then print(2^i-1, ' is a prime number ')
> else fi; od;
```
(b) With MAPLE, we may use
```
> nextprime(10^(100)+1);
```
We thus obtain the integer $10^{100} + 267$.

(136) With MAPLE, the program below enumerates the first N (here $N = 120$) prime numbers.
```
> for i to 120 do
> p.i :=ithprime(i) od;
```
For example, $p.(1..120)$ gives the first 120 prime numbers.

(137) In order to find four consecutive integers with the same number of prime factors, we must use the function Ω. First we type in

```
> readlib(ifactors):  with(numtheory):
```

and thereafter, we type in the following instructions:

```
> Omega:=n->sum(ifactors(n)[2][i][2],
> i=1..nops(factorset(n))):
> for n to 1000 do if Omega(n)=Omega(n+1) and
> Omega(n+1)=Omega(n+2) and Omega(n+2)=Omega(n+3)
> then print(n) else fi; od;
```

To find four consecutive integers having the same number of divisors, it is enough to type in the instructions

```
> with(numtheory):
> for n to 1000 do
> if tau(n)=tau(n+1) and tau(n+1)=tau(n+2)
> and tau(n+2)=tau(n+3)
> then print(n) else fi; od;
```

(138) (a) With the procedure "return", the search is easily done:

```
> return:=proc(n::integer)
> local m,s;
> m:=n; s:=0;
> while m<>0 do
> s:=10*s+irem(m,10);
> m:=iquo(m,10) od; s end:
```

And for our problem, we have the following procedure:

```
> invp:=proc(N::integer) local n;
> for n from 1 to N do if isprime(n)
> and isprime(return(n)) then
> print (n) fi; od; end:
```

Without the procedure "return", we may proceed as follows:

```
> invp:=proc(N)
> for j from 169 to N do
> L:=convert(ithprime(j),base,10);# N <= 1229
> if type(1000*L[1]+100*L[2]+10*L[3]+L[4],prime)=true
> then print(ithprime(j)) else fi; od; end:
```

(b)

```
> invp:=proc(N::integer)
> local n;
> for n from 1 to N do
> if isprime(n)=false then elif
> type(sqrt(return(n)),integer)=true
> then print(n) else fi; od; end:
```

If we do not use the procedure "return", we may proceed as follows:

```
> invp:=proc(N) local j, L;
> for j from 26 to N
> do L:=convert(ithprime(j),base,10);# N <= 168
> if type(sqrt(100*L[1]+10*L[2]+L[3]),integer)=true then
> print(ithprime(j)) else fi; od; end:
```

or the following procedure:

```
> invp:=proc(N) local j, L;
> for j from 169 to N
> do L:=convert(ithprime(j),base,10);# N <= 1229
> if type(sqrt(1000*L[1]+100*L[2]+10*L[3]+L[4]),
> integer)=true
> then print(ithprime(j)) else fi; od; end:
```

(139) With MAPLE:

```
> for n from 3 by 2 to 10000 do
> if isprime(n) and isprime(n+2) and isprime(n+6)
> then print(n) else fi; od;
```

(140) We prove this result using induction on k. The result is immediate for $k = 2$. Assume that the result is true for a certain integer $k > 2$, that is for which we have $p_k < 2^k$. It is enough to show that $p_{k+1} < 2^{k+1}$. From Bertrand's Postulate, there exists a prime number between p_k and $2p_k$, in which case $p_{k+1} < 2p_k$, and the result is proved.

(141) It is enough to show that $d \not\equiv 2, 4 \pmod 6$. First of all, assume that $d = 2$: if $p_k \equiv 1 \pmod 3$, then $p_{k+1} = p_k + 2 \equiv 0 \pmod 3$, contradicting the fact that p_{k+1} is prime; similarly if $p_k \equiv 2 \pmod 3$, then $p_{k-1} = p_k - 2 \equiv 0 \pmod 3$, contradicting the fact that p_{k-1} is prime. The same type of contradiction emerges when we assume that $d = 4$. If $d = 6k+2$ or $6k+4$ with $k \geq 1$, the same argument works. For $d = 6$, it is $p_{16} = 53$; for $d = 12$, it is $p_{47} = 211$; for $d = 18$, it is $p_{2285} = 20\,201$.
REMARK: It is interesting to observe that the gap $d = 24$ is reached earlier than might be expected in the sequence of prime numbers, namely with $p_{1939} = 16\,787$.

(142) This statement follows from the fact that each of the listed numbers is a perfect square, since

$$12321 = 111^2, \quad 1234321 = 1111^2, \ldots,$$
$$12345678987654321 = 111111111^2.$$

(143) Let $k \geq 2$. Since each number $\leq n_k$ is either 1, a prime number or else a composite number, it is clear that

$$n_k = 1 + \pi(n_k) + k. \tag{1}$$

By using MATHEMATICA and the program

```
n=1;Do[n=n+1;While[PrimePi[n]!=n-10^a-1,n++]; Print[10^a,
" ",n],{a,1,3}]
```

we obtain the table

10	18
100	133
1000	1197

This reveals that $n_{10} = 18$, $n_{100} = 133$ and $n_{1000} = 1197$. For values of k larger than 1000, and to accelerate the computations, one can use the approximation (guaranteed by the Prime Number Theorem) $\pi(x) \approx \frac{x}{\log x} + \frac{x}{\log^2 x}$, so that (1) gives

$$n_k \approx \frac{n_k}{\log n_k} + \frac{n_k}{\log^2 n_k} + k$$

and therefore that

$$n_k \left(1 - \frac{1}{\log n_k} - \frac{1}{\log^2 n_k}\right) \approx k, \tag{2}$$

which in particular means that

$$\log n_k \approx \log k. \tag{3}$$

Combining (2) and (3), we obtain the approximation

$$n_k \approx k \cdot \left(1 - \frac{1}{\log k} - \frac{1}{\log^2 k}\right)^{-1}. \tag{4}$$

Setting $s_k(n) := 1 + \pi(n) + k - n$, it follows that if a number n satisfies $s_k(n) = 0$, then $n = n_k$.

First consider the case $k = 10^4$. From (4), we have as a first approximation $n_{10^4} \approx 11\,369$. By using MATHEMATICA and the program

```
n=11369;While[(a=s[n])!=0,n=n+a];Print[n]
```

where $s(n) = s_{1000}(n)$, we obtain that $n_{10000} = 11\,374$. Similarly, with the approximation $n_{10^5} \approx 110\,425$, we obtain that $n_{10^5} = 110\,487$. The following is the table giving the values of n_{10^α} for $1 \le \alpha \le 10$.

α	n_{10^α}
1	18
2	133
3	1 197
4	11 374
5	110 487

α	n_{10^α}
6	1 084 605
7	10 708 555
8	106 091 745
9	1 053 422 339
10	10 475 688 327

(144) Let $k \ge 2$. Setting $r = [\log n_k / \log 2]$, it is clear that the number n_k satisfies

$$\sum_{i=1}^{r} \pi(n_k^{1/i}) = k.$$

From this relation and the approximation $\pi(x) \approx \dfrac{x}{\log x}$ (guaranteed by the Prime Number Theorem), it follows that

$$\frac{n_k}{\log n_k} \approx k,$$

so that $\log n_k \approx \log k + \log\log n_k \approx \log k$ and therefore that

$$n_k \approx k \log n_k \approx k \log k,$$

which gives a starting point for the computation of the exact value of n_k.

Using MATHEMATICA and the program

```
Do[k = 10^j; n = Floor[N[k*Log[k]]];
While[r = Floor[N[Log[n]/Log[2]]];
s=Sum[PrimePi[n^(1/i)],{i,1,r}];(a=k-s)!=0,n=n+a];
Print[j,"->", n,"=",FactorInteger[n]],{j,3,10}]
```

we finally obtain the following table:

α	n_{10^α}
1	16
2	419
3	7 517
4	103 511
5	1 295 953

α	n_{10^α}
6	15 474 787
7	179 390 821
8	2 037 968 761
9	22 801 415 981
10	252 096 677 813

(145) If n is even, then 2^n+n^2 is also even and therefore not a prime. It follows that $n \equiv 1, 3$ or 5 modulo 6. If $n = 6k+1$ for a certain nonnegative integer k, then $2^n = 2^{6k+1} \equiv 2 \pmod 3$ and $n^2 \equiv 1 \pmod 3$; in this case, we have that $2^n + n^2 \equiv 2 + 1 \equiv 0 \pmod 3$. Similarly, if $n = 6k+5$ for a certain nonnegative integer k, we easily show that $3|2^n + n^2$. Therefore, the only way that $2^n + n^2$ can be a prime number is that $n \equiv 3 \pmod 6$.

Thus, by considering all the positive integers $n < 100$ of the form $n = 6k+3$ and using a computer, we easily find that the only prime numbers of the form $2^n + n^2$, with $n < 100$, are those corresponding to $n = 1, 9, 15, 21, 33$.

(146) We will show that if n is of the form $n = 3k+1$ or $n = 3k+2$ with $k \geq 1$, then $7|a_n$. Moreover, we will show that if n is of the form $n = 3(3k+1)$ or $n = 3(3k+2)$ with $k \geq 1$, then $73|a_n$. Finally, since $3|a_n$ if n is even, it will follow that, for a_n to be prime, n must be an odd multiple of 9.

So let $n = 3k+a$, with $a = 1$ or 2. Since $8^k \equiv 1 \pmod 7$ for each integer $k \geq 1$, we have

$$\begin{aligned} a_n = 2^n(2^n+1)+1 &= 2^{3k+a}(2^{3k+a}+1)+1 \\ &= 8^k 2^a(8^k 2^a+1)+1 \equiv 2^a(2^a+1)+1 \pmod 7. \end{aligned}$$

But

$$2^a(2^a+1)+1 = \begin{cases} 7 \equiv 0 \pmod 7 & \text{if } a = 1, \\ 21 \equiv 0 \pmod 7 & \text{if } a = 2, \end{cases}$$

which establishes our first statement.

Let us now assume that $n = 3(3k+a)$ with $a = 1$ or 2. Since $2^9 \equiv 1 \pmod{73}$, we have

$$\begin{aligned} a_n = 2^n(2^n+1)+1 &= 2^{9k+3a}(2^{9k+3a}+1)+1 \\ &= (2^9)^k 2^{3a}((2^9)^k 2^{3a}+1)+1 \equiv 2^{3a}(2^{3a}+1)+1 \pmod{73}. \end{aligned}$$

But

$$2^{3a}(2^{3a}+1)+1 = \begin{cases} 2^3(2^3+1)+1 = 73 \equiv 0 \pmod{73} & \text{if } a = 1, \\ 2^6(2^{12}+1)+1 = 4161 \equiv 0 \pmod{73} & \text{if } a = 2, \end{cases}$$

which establishes our second statement.

Having observed that a_n is prime for $n = 1, 3$ and 9, and then considering all the numbers of the form $n = 9(2k+1)$, we obtain using a computer that a_n is composite for each integer n, $10 \leq n < 1000$.

(147) That number is $n = 9$; we then have $a_9 = 326981 = 79 \cdot 4139$.

(148) First observe that it follows from Wilson's Theorem that

$$\left[\frac{(j-1)!+1}{j} - \left[\frac{(j-1)!}{j}\right]\right] = \begin{cases} 1 & \text{if } j \text{ is prime,} \\ \\ 0 & \text{if } j \text{ is composite.} \end{cases}$$

Hence, to obtain the formula of Minác and Willans, we only need to prove that

$$p_n = 2 + \sum_{m=2}^{2^n} \left[\left[\frac{n}{1+\pi(m)} \right]^{1/n} \right].$$

But we easily prove that

$$\left[\left[\frac{n}{1+\pi(m)} \right]^{1/n} \right] = \begin{cases} 1 & \text{if } \pi(m) \leq n-1, \\ \\ 0 & \text{otherwise.} \end{cases}$$

Now, as m varies from 2 to 2^n, we have that $\pi(m) \leq n-1$ for $m = 2, 3, \ldots, p_n - 1$, that is a total of $p_n - 2$ numbers. Therefore,

$$2 + \sum_{m=2}^{2^n} \left[\left[\frac{n}{1+\pi(m)} \right]^{1/n} \right] = 2 + p_n - 2 = p_n,$$

as was to be shown.

(149) We use an induction argument. The result is true for $n = 1$ and for $n = 2$. So let $n \geq 3$. Assume that the result is true for all natural numbers $\leq n-1$ and let us show that it implies that it must be true for n. Let $P_n = \prod_{p \leq n} p$. First of all, if n is even, then $P_n = P_{n-1}$, so that the result is true for n. Let us examine the case where n is odd, that is $n = 2k+1$ for a certain positive integer k. It follows that each prime number p such that $k+2 \leq p \leq 2k+1$ is a divisor of the number

$$(*) \qquad \binom{2k+1}{k} = \frac{(2k+1)(2k)(2k-1)(2k-2)\cdots(k+2)}{1 \cdot 2 \cdot 3 \cdots k}.$$

Since

$$2^{2k+1} = (1+1)^{2k+1} > \binom{2k+1}{k} + \binom{2k+1}{k+1} = 2\binom{2k+1}{k},$$

we obtain

$$\binom{2k+1}{k} < 4^k.$$

It follows that the product of all the prime numbers p such that $k+2 \leq p \leq 2k+1$ is a divisor of $\binom{2k+1}{k}$ and therefore smaller than 4^k. On the other hand, using the induction hypothesis, we have that $P_{k+1} \leq 4^{k+1}$. This is why

$$P_n = P_{2k+1} = \prod_{p \leq k+1} p \cdot \prod_{k+2 \leq p \leq 2k+1} p < 4^{k+1} \cdot 4^k = 4^{2k+1} = 4^n,$$

as was to be shown.

(150) Let $m = (a, c)$. Then, there exist two integers u and v such that $(u, v) = 1$ and such that $a = mu$ and $c = mv$. Hence, since $ab = cd$, we have $mub = mvd$ and therefore $ub = vd$. Since $(u, v) = 1$, we have $u|d$ and this is why there exists an integer n such that $d = nu$. Since $ub = vnu$, we therefore have $b = nv$. It follows from these relations that

$$a^2 + b^2 + c^2 + d^2 = m^2u^2 + n^2v^2 + m^2v^2 + n^2u^2 = m^2(u^2+v^2) + n^2(u^2+v^2) = (u^2+v^2)(m^2+n^2),$$

a product of two integers larger than 1.

(151) Since

$$4n^3+6n^2+4n+1 = n^4+4n^3+6n^2+4n+1-n^4 = (n+1)^4-n^4$$
$$= ((n+1)^2-n^2)((n+1)^2+n^2) = (2n+1)(2n^2+2n+1),$$

the product of two integers larger than 1, the result follows.

(152) First of all, since $p+q$ is even, we can write

$$(*) \qquad p+q = 2\cdot\frac{p+q}{2}.$$

Since $\frac{p+q}{2}$ is an integer located between the two consecutive prime numbers p and q, it must be composite, that is the product of at least two prime numbers, and this is why the right-hand side of $(*)$ has at least three prime factors.

(153) The answer is YES. We look for positive integers n, a, b and c such that

$$\frac{n}{2} = a^2, \quad \frac{n}{3} = b^3, \quad \frac{n}{5} = c^5.$$

It is sufficient to find integers a, b and c such that

$$2a^2 = 3b^3 = 5c^5.$$

The task is therefore to find integers α_i, β_i and γ_i $(i = 1, 2, 3)$ such that

$$2\left(2^{\alpha_1}3^{\beta_1}5^{\gamma_1}\right)^2 = 3\left(2^{\alpha_2}3^{\beta_2}5^{\gamma_2}\right)^3 = 5\left(2^{\alpha_3}3^{\beta_3}5^{\gamma_3}\right)^5.$$

To do so, we must find integers α_i, β_i and γ_i $(i = 1, 2, 3)$ such that

$$2\alpha_1+1 = 3\alpha_2 = 5\alpha_3, \quad 2\beta_1 = 3\beta_2+1 = 5\beta_3, \quad 2\gamma_1 = 3\gamma_2 = 5\gamma_3+1.$$

We easily find

$$\alpha_1 = 7, \alpha_2 = 5, \alpha_3 = 3, \quad \beta_1 = 5, \beta_2 = 3, \beta_3 = 2, \quad \gamma_1 = 3, \gamma_2 = 2, \gamma_3 = 1.$$

We then obtain that $n = 2(2^7\cdot 3^5\cdot 5^3)^2 = 30\,233\,088\,000\,000$ serves our purpose.

(154) This follows from the identity

$$n^{42}-27 = (n^{14})^3-3^3 = (n^{14}-3)(n^{28}+3n^{14}+3^2).$$

(155) We proceed by contradiction by assuming that there does not exist any prime number in the interval $]x, 2x]$, in which case we have $\theta(2x) = \theta(x)$. By using the inequalities $0.73x < \theta(x) < 1.12x$, we would then have

$$1.46x = 2(0.73)x < \theta(2x) = \theta(x) < 1.12x,$$

a contradiction.

(156) We proceed by induction. First of all, for $n = 4$, the result is true, since $121 = 11^2 = p_5^2 < p_1p_2p_3p_4 = 210$. Assume that the inequality $p_k^2 < p_1p_2\cdots p_{k-1}$ is true for a certain integer $k \geq 5$. By using Bertrand's Postulate in the form $p_{k+1} < 2p_k$, we then have

$$p_{k+1}^2 < 4p_k^2 < 4p_1p_2\cdots p_{k-1} < p_1p_2\cdots p_k,$$

and the result then follows by induction.

(157) If there exist $q, r, a \in \mathbb{N}$ such that $q^r = (q^{r/2})^2 = a^2$, where r is even and $q^r = p + m^2$ with p prime and $m \in \mathbb{N}$, then $a^2 - m^2 = p$, so that $(a-m)(a+m) = p$. Since p is prime, we must have $a-m = 1$ and $a+m = p$, and therefore $m = a - 1$ and $p = 2a - 1$. Hence, if $2a - 1 = 2q^{r/2} - 1$ is composite, q^r cannot be written as $p + m^2$, as was to be shown.

(158) For $p = 3$, the result is immediate. Assume that $p \geq 5$. If $p = 3k + 1$ for a certain positive integer k, then $8k + 1 = 24k + 9$, a multiple of 3. Otherwise, that is if $p = 3k - 1$ for a certain positive integer k, then $8p - 1 = 24k - 9$, a multiple of 3, which contradicts the fact that $8p - 1$ is prime. In both cases, the result is proved.

(159) If a positive integer of the form $3k + 2$ has no prime factor of the form $3k+2$, then all its prime factors are of the form $3k+1$. Since the product of two integers of the form $3k+1$ is of the form $3k+1$, the result follows.

Since each product of prime numbers of the form $4k+1$ is of the same form and since each product of prime numbers of the form $6k+1$ is of the same form, the result follows.

(160) (a) We have $23 = 3 \cdot 3! + 2 \cdot 2! + 1 \cdot 1!$ and $57 = 2 \cdot 4! + 1 \cdot 3! + 1 \cdot 2! + 1 \cdot 1!$.

(b) To find the Cantor expansion of a positive integer n, we proceed as follows. Let m be the largest positive integer such that $m! \leq n$ and let a_m be the largest positive integer such that $a_m \cdot m! \leq n$. It is clear that $0 < a_m \leq m$; otherwise, this would contradict the maximal choice of m. If $a_m \cdot m! = n$, then the Cantor expansion is given by $n = a_m \cdot m!$. Otherwise, that is if $a_m \cdot m! < n$, let $d_1 = n - a_m \cdot m! > 0$, let m_1 be the largest positive integer such that $m_1! \leq d_1$ and let a_{m_1} be the largest positive integer such that $a_{m_1} \cdot m_1! \leq d_i$. As above, we have $a < a_{m_1} \leq m_1$. If $a_{m_1} \cdot m_1! = d_1$; then the Cantor expansion is given by $n = a_m \cdot m! + a_{m_1} \cdot m_1!$, where $0 < a_{m_1} \leq m_1 < m$. If $a_{m_1} \cdot m_1! < d_1$, then we set $d_2 = d_1 - a_{m_1} \cdot m_1!$ and we let m_2 be the largest positive integer such that $m_2! \leq d_2$. And so on. We thus build a sequence of positive integers $m > m_1 > m_2 > \ldots$ with the corresponding integers $0 < a_{m_i} \leq m_i$. Since the sequence of m_i's is decreasing, it must have an end. Let us show the uniqueness of this representation. Assume that for $0 \leq a_j, b_j \leq j$, we have

$$n = a_m m! + \cdots + a_1 1! = b_m m! + \cdots + b_1 1!,$$

that is $(a_m - b_m)m! + \cdots + (a_1 - b_1)1! = 0$. If both expansions are different, then there exists a smaller integer j such that $1 \leq j < m$ and $a_j \neq b_j$. Hence,

$$j! \left((a_m - b_m)\frac{m!}{j!} + \cdots + (a_{j+1} - b_{j+1})(j+1) + (a_j - b_j) \right) = 0$$

and therefore

$$\begin{aligned} b_j - a_j &= (a_m - b_m)\frac{m!}{j!} + \cdots + (a_{j+1} - b_{j+1})(j+1) \\ &= (j+1)\left((a_m - b_m)\frac{m!}{(j+1)!} + \cdots + (a_{j+1} - b_{j+1}) \right), \end{aligned}$$

which implies that $(j+1)|(b_j - a_j)$. Since $0 \leq a_j, b_j \leq j$, it follows that $a_j = b_j$, a contradiction.

(161) (*TYCM, Vol. 19, 1988, p. 191*). The expression in the statement can be written as

$$\frac{(p-1)!+1}{p}+\frac{(-1)^d d!(p-1)!+1}{p+d}.$$

Since $(p+d-1)! = (p+d-1)(p+d-2)\cdots(p+d-d)(p-1)!$, we have $(p+d-1)! \equiv (-1)^d d!(p-1)! \pmod{p+d}$, and it follows that the expression in the statement is an integer if and only if

$$\frac{(p-1)!+1}{p}+\frac{(p+d-1)!+1}{p+d} \tag{1}$$

is an integer. From Wilson's Theorem, if p and $p+d$ are two prime numbers, then each of the terms of (1) is an integer, which proves the necessary condition.

Conversely, assume that expression (1) is an integer. If p or $p+d$ is not a prime, then by Wilson's Theorem, at least one of the terms of (1) is not an integer. This implies that none of the terms of (1) is an integer or equivalently neither of p and $p+d$ is prime. It follows that both fractions of (1) are in reduced form.

It is easy to see that if a/b and a'/b' are reduced fractions such that $a/b + a'/b' = (ab'+a'b)/(bb')$ is an integer, then $b|b'$ and $b'|b$.

Applying this result to (1), we obtain that $(p+d)|p$, which is impossible. We may therefore conclude that if (1) is an integer, then both p and $p+d$ must be primes.

(162) If $p=3$, then $p+2=5$ is prime and $p^2+2p-8=7$ is prime. It is the only number with this property. Indeed, $p=2$ does not have this property, while if $p>3$, then

$$p^2+2p-8 \equiv 1+2p-2 \equiv 2(p+1) \equiv 0 \pmod 3 \iff 3|(p+1).$$

But for $p>3$, $p=3k\pm 1$, and in each of the cases it is easily seen that at least one of the two numbers $p+2$ and p^2+2p-8 is not a prime.

(163) The answer is YES. If $p=3$, then $p^2+8=17$ is prime and $p^3+4=31$ is prime. It is the only prime number with this property. Indeed, $p=2$ does not have this property, while if $p>3$, then $p \equiv \pm 1 \pmod 3$, in which case $p^2 \equiv 1 \pmod 3$, that is $p^2+8 \equiv 9 \equiv 0 \pmod 3$, so that p^2+8 is not a prime. Thus the result.

(164) (Ribenboim [**28**], p. 145). First assume that the congruence is satisfied. Then $n \neq 2, 4$ and $(n-1)!+1 \equiv 0 \pmod n$. Thus, using Wilson's Theorem, n is prime. Moreover, $4(n-1)!+2 \equiv 0 \pmod{n+2}$; thus, multiplying by $n(n+1)$ we obtain

$$4[(n+1)!+1]+2n^2+2n-4 \equiv 0 \pmod{n+2}$$

and therefore

$$4[(n+1)!+1]+(n+2)(2n-2) \equiv 0 \pmod{n+2};$$

hence, $4[(n+1)!+1] \equiv 0 \pmod{n+2}$. This is why, using Wilson's Theorem, $n+2$ is also prime.

Conversely, if n and $n+2$ are prime, then $n \neq 2$ and

$$\begin{aligned}(n-1)!+1 &\equiv 0 \pmod n,\\ (n+1)!+1 &\equiv 0 \pmod{n+2}.\end{aligned}$$

But $n(n+1) = (n+2)(n-1)+2$, and this is why $2(n-1)!+1 = k(n+2)$, where k is an integer. From the relation $(n-1)! \equiv -1 \pmod{n}$, we obtain $2k+1 \equiv 0 \pmod{n}$. Now, $2(n-1)!+1 = k(n+2)$ is equivalent to $4(n-1)!+2 \equiv 0 \equiv -(n+2) \pmod{n+2}$. Moreover, $4(n-1)!+2 \equiv 4k \equiv -2 \equiv -(n+2) \pmod{n}$. Hence, $4(n-1)!+2 \equiv -(n+2) \pmod{(n(n+2))}$; that is $4\Big((n-1)!+1\Big)+n \equiv 0 \pmod{n(n+2)}$.

(165) The prime number $p = 3$ is the only one with this property, because if $p > 3$, then $p = 2k+1$ for a certain integer $k \geq 2$, in which case

$$2^p = 2^{2k+1} = 4^k \cdot 2 \equiv 2 \pmod{3}$$

while

$$p^2 \equiv 1 \pmod{3},$$

so that

$$2^p + p^2 \equiv 0 \pmod{3}.$$

(166) The answer is $p = 19$. Indeed, $17p+1 = a^2 \Rightarrow 17p = (a-1)(a+1)$. We then have $17 = a-1$ and $p = a+1$ or $17 = a+1$ and $p = a-1$. The first case yields $a = 18$ and $p = 19$, while the second case yields $a = 16$ and $p = 15$, which is to be rejected. Thus the result.

(167) (a) The possible values of (a^2, b) are p and p^2.
(b) The only possible value of (a^2, b^2) is p^2.
(c) The possible values of (a^3, b) are p, p^2 and p^3.
(d) The possible values of (a^3, b^2) are p^2 and p^3.

(168) (a) The only possible value is p^3.
(b) The only possible value is p.
(c) The only possible value is p.
(d) The possible values are p^2, p^3, p^4 and p^5.

(169) We have $(a^2b^2, p^4) = p^4$ and $(a^2+b^2, p^4) = p^2$.

(170) (a) True. (b) True. (c) True.
(d) False. Indeed, we have $13 | 2^2+3^2$ and $13 | 3^2+2^2$, while $13 \nmid 2^2+2^2 = 8$.

(171) It is an immediate consequence of Theorem 12.

(172) Let

$$\begin{cases} a = p_1^{\alpha_1} \cdots p_r^{\alpha_r}, \\ b = p_1^{\beta_1} \cdots p_r^{\beta_r}, \\ c = p_1^{\gamma_1} \cdots p_r^{\gamma_r}. \end{cases}$$

From Theorem 12,

$$(a,b,c) = p_1^{\min(\alpha_1,\beta_1,\gamma_1)} \cdots p_r^{\min(\alpha_r,\beta_r,\gamma_r)}$$

and

$$[a,b,c] = p_1^{\max(\alpha_1,\beta_1,\gamma_1)} \cdots p_r^{\max(\alpha_r,\beta_r,\gamma_r)}.$$

To prove the result, we proceed by contradiction. Assume for example that $(a,b) > 1$. Using the fact that $(a,b,c)[a,b,c] = abc$, it follows, using the above notation, that

$$\min(\alpha_i,\beta_i,\gamma_i) + \max(\alpha_i,\beta_i,\gamma_i) = \alpha_i + \beta_i + \gamma_i \qquad (i = 1, 2, \ldots, r).$$

But it is easy to prove that for the sum of three nonnegative integers to be equal to the sum of the smallest and of the largest of these same three

numbers, at least two of these numbers must be 0. But this contradicts the fact that $(a,b)>1$, an inequality which means that there exists an i_0 $(1\le i_0\le r)$ for which $\min(\alpha_{i_0},\beta_{i_0})\ge 1$. Hence, the result.

(173) We use Theorem 12 and the fact that

$$\min\{\alpha_i,\beta_i,\gamma_i\}=\min\{\alpha_i,\beta_i\}+\min\{\beta_i,\gamma_i\}+\min\{\alpha,\gamma_i\} \\ -\min\{\alpha_i+\beta_i,\beta_i+\gamma_i,\alpha_i+\gamma_i\}.$$

The second part follows from the first part and Problem 171.

(174) Let

$$\begin{cases} a=p_1^{\alpha_1}\cdots p_r^{\alpha_r},\\ b=p_1^{\beta_1}\cdots p_r^{\beta_r},\\ c=p_1^{\gamma_1}\cdots p_r^{\gamma_r}. \end{cases}$$

Since $[a,b]=\prod_{i=1}^r p_i^{\max\{\alpha_i,\beta_i\}}$ and $(a,b)=\prod_{i=1}^r p_i^{\min\{\alpha_i,\beta_i\}}$, it is enough to show that, for each i,

$$2\max\{\alpha_i,\beta_i,\gamma_i\}-\max\{\alpha_i,\beta_i\}-\max\{\beta_i,\gamma_i\}-\max\{\gamma_i,\alpha_i\} \\ =2\min\{\alpha_i,\beta_i,\gamma_i\}-\min\{\alpha_i,\beta_i\}-\min\{\beta_i,\gamma_i\}-\min\{\gamma_i,\alpha_i\}.$$

Without loosing in generality, we may assume that, for a given i, $\alpha_i\ge\beta_i\ge\gamma_i$, from which the result easily follows.

(175) Let $a=\prod_{i=1}^r p_i^{a_i}$, $b=\prod_{i=1}^r p_i^{b_i}$, $c=\prod_{i=1}^r p_i^{c_i}$. Without loosing in generality, we may assume that $a_i\le b_i\le c_i$. The equation of the statement allows one to conclude that $c_i+a_i=\frac{1}{2}(a_i+b_i+c_i)$ and therefore that $a_i+c_i=b_i$, which implies, since $c_i\ge b_i$, that $b_i=c_i$ and $a_i=0$. This means that in order for the relation to be true, for the same prime number, two of the exponents must be equal while the third one should be 0. Hence, we can choose $a=2^1\cdot 3^1\cdot 5^0=6$, $b=2^1\cdot 3^0\cdot 5^1=10$ and $c=2^0\cdot 3^1\cdot 5^1=15$. Note that the numbers 42, 70, 15 will also do.

(176) The left inequality is obvious. To prove the right equality, first observe that

$$\#n=[1,2,\dots,n]=\prod_{p\le n}p^{\delta_p},$$

where p^{δ_p} is the largest power of p not exceeding n. In other words, δ_p is defined implicitly by the inequalities $p^{\delta_p}\le n<p^{\delta_p+1}$. It follows successively that

$$\delta_p\log p\le\log n<(\delta_p+1)\log p,$$

$$\delta_p\le\frac{\log n}{\log p}<\delta_p+1,$$

$$\delta_p=\left[\frac{\log n}{\log p}\right].$$

We have thus established that

$$\#n=\prod_{p\le n}p^{[\log n/\log p]},$$

which was to be shown.

Subject Index

Index of Authors