5. Congruences

(266) For which positive integers n is the number $3^n + 1$ a multiple of 10?

(267) Find the smallest positive residue modulo 7 of $1! + 2! + \cdots + 50!$.

(268) What is the remainder of the division of $\sum_{i=1}^{111} i!$ by 12?

(269) Show that for each positive integer n, $10 \cdot 32^n + 1$ is a composite number.

(270) Is it true that 36 divides $n^6 + n^2 + 4$ for infinitely many positive integers n? Explain.

(271) In a letter sent to Christian Huygens (1629–1695) in 1659, Fermat wrote that using his method of infinite descent, he was successful in showing that no integer of the form $3k - 1$ can be written as $x^2 + 3y^2$ (with x and y integers). Is it possible to prove this result in a very simple manner? Explain.

(272) Let m and n be positive integers such that $p^m \| n$ for a certain prime number p. Show that

$$\frac{n!}{p^m} \equiv (-1)^m \prod_{k=0}^{\left[\frac{\log n}{\log p}\right]} \left(\left[\frac{n}{p^k}\right] - p\left[\frac{n}{p^{k+1}}\right] \right)! \pmod{p}.$$

(273) Let n be a positive integer. Show that the last digit of n^{13} is the same as the last digit of n.

(274) Find the smallest positive integer n such that $\sqrt[7]{n/7}$ and $\sqrt[11]{n/11}$ are both integers.

(275) Show that there exists an arbitrarily long sequence of consecutive integers, each divisible by a perfect square.

(276) Let a and b be integers and let m and n be positive integers. Show that the system of congruences

$$x \equiv a \pmod{m},$$
$$x \equiv b \pmod{n}$$

has solutions if and only if $(m, n) | (a - b)$.

(277) Let p be a prime number. Show that if k is an integer, $1 \leq k < p$, then $\binom{p}{k} \equiv 0 \pmod{p}$.

(278) (a) Let $x_1, x_2, \ldots, x_n$ be integers. Show that

$$(x_1 + x_2 + \cdots + x_n)^p \equiv x_1^p + x_2^p + \cdots + x_n^p \pmod{p}.$$

(b) Show that if a and b are integers such that $a^p \equiv b^p \pmod{p}$, then $a^p \equiv b^p \pmod{p^2}$.

(279) Let p be an odd prime number and let k be an integer such that $1 \leq k < p$. Show that

$$\binom{p-1}{k} \equiv (-1)^k \pmod{p}.$$

(280) Let p be a prime number and let r be an integer such that $1 \leq r < p$. If $(-1)^r r! \equiv 1 \pmod{p}$, show that

$$(p - r - 1)! \equiv -1 \pmod{p}.$$

Use this result to show that $259! \equiv -1 \pmod{269}$ and $463! \equiv -1 \pmod{479}$.

(281) Let $\alpha \geq 3$ and $\beta \geq 6$ be two integers. Show that the equation $2^\beta - 1 = 3p^\alpha$ has no solutions for p prime.

(282) Let p be a prime number and let $n = 2p + 1$. Show that if n is not a multiple of 3 and if $2^{n-1} \equiv 1 \pmod{n}$, then n is prime.

(283) Let p be a prime number and k a positive integer. Show that

$$(*) \qquad a \equiv b \pmod{p^k} \Longrightarrow a^p \equiv b^p \pmod{p^{k+1}}.$$

Then, prove that if $p > 2$, $p \nmid a$ and $p^k \| a - b$, then $p^{k+1} \| a^p - b^p$.

(284) If p is a prime number, can the equation $p^\delta + 1 = 2^\nu$ have solutions with integers $\delta \geq 2$ and $\nu \geq 2$s?

(285) Show that the equation $1 + n + n^2 = m^2$, where m and n are positive integers, is impossible.

(286) Show that the only solution of the equation $1 + p + p^2 + p^3 + p^4 = q^2$, where p and q are primes, is $\{p, q\} = \{3, 11\}$.

(287) Let x_1, x_2, x_3, x_4 and x_5 be integers such that

$$x_1^3 + x_2^3 + x_3^3 + x_4^3 + x_5^3 = 0.$$

Show that necessarily one of the x_i's is a multiple of 7.

(288) Show that $2^p + 3^p$ is not a power (> 1) of an integer if p is prime.

(289) Show that for each positive integer n,

$$1^n + 2^n + 3^n + 4^n + 5^n + 6^n$$

is divisible by 7 if and only if n is not divisible by 6.

(290) Is it true that if n is a positive odd integer whose last digit in decimal representation is different from 5, then the last two digits of the decimal representation of n^{400} are 0 and 1? Explain.

(291) What are the possible values of the last digit of 4^m for each $m \in \mathbb{N}$?

(292) Show that the difference of two consecutive cubes is never divisible by 3, nor by 5.

(293) Is it true that $27 | (2^{5n+1} + 5^{n+2})$ for each integer $n \geq 0$? Explain.

(294) Show that for each positive integer k, the number $(13^2)^{2k+1} + (98^2)^{2k+1}$ is divisible by 337.

(295) Find the last two digits of the decimal representation of $19^{19^{19}}$.

(296) If a and b are positive integers such that $(ab, 70) = 1$, show that $a^{12} - b^{12} \equiv 0 \pmod{280}$.

(297) Show that for each integer $n \geq 2$, $n^{13} - n$ is divisible by 2730.

(298) Find the smallest positive integer which divided by 12, by 17, by 45 or by 70 gives in each case a remainder of 4.

(299) If n is an arbitrary positive integer, is the number

$$3n^{13} + 4n^{11} + n^7 + 3n^5 + 3n$$

divisible by 7?

(300) Let p be a prime number; show that $\binom{2p}{p} \equiv 2 \pmod{p}$.

(301) Show that a 3-digit positive integer whose decimal representation is of the form "abc" (for three digits a, b and c) is divisible by 7 if and only if $2a + 3b + c$ is divisible by 7.

(302) Show that a 6-digit positive integer whose decimal representation is of the form "*abcabc*" (for three digits a, b and c) is necessarily divisible by 13.

(303) Show that $561|2^{561}-2$ and that $561|3^{561}-3$.

(304) Given a positive integer n, show that

$$\frac{12}{35}n^{13}+\frac{23}{35}n$$

is an integer.

(305) Does there exist a rational number r such that for each positive integer n relatively prime with 481,

$$\frac{50}{481}n^{36}+r$$

is a positive integer?

(306) Let p be an odd prime number, $p \neq 5$. Show that p divides infinitely many integers amongst $1, 11, 111, 1\,111, \ldots$.

(307) According to Fermat's Little Theorem, if n is an odd prime number and if a is a positive integer such that $(a,n)=1$, then $a^{n-1} \equiv 1 \pmod{n}$. Show that the reverse of this result is false.

(308) Let $p>3$ be a prime number. Show that $ab^p - ba^p \equiv 0 \pmod{6p}$ for any integers a and b.

(309) If n is a positive integer, is it true that

$$1+2+3+\cdots+(n-1) \equiv 0 \pmod{n}?$$

Explain.

(310) For which positive integers n do we have

$$1^2+2^2+3^2+\cdots+(n-1)^2 \equiv 0 \pmod{n}?$$

(311) Is it true that if n is a positive integer divisible by 4, then

$$1^3+2^3+3^3+\cdots+(n-1)^3 \equiv 0 \pmod{n}?$$

(312) Prove that for each positive integer n, we have

$$5^n \equiv 1+4n \pmod{16} \quad \text{and} \quad 5^n \equiv 1+4n+8n(n-1) \pmod{64}.$$

(313) Show that for each positive integer $k \geq 3$,

$$5^{2^{k-3}} \not\equiv 1 \pmod{2^k} \quad \text{while} \quad 5^{2^{k-2}} \equiv 1 \pmod{2^k}.$$

More generally, show that for $k>2$ and a given odd integer a, we have

$$a^{2^{k-2}} \equiv 1 \pmod{2^k}.$$

(314) Show that

$$\frac{n^5}{5}+\frac{n^3}{3}+\frac{7n}{15}$$

is an integer for all $n \in \mathbb{N}$. More generally, show that if p and q are prime numbers, then

$$\frac{n^p}{p}+\frac{n^q}{q}+\frac{(pq-p-q)n}{pq}$$

is an integer for all $n \in \mathbb{N}$.

(315) Find the solution of the congruence $x^{24}+7x \equiv 2 \pmod{13}$.

(316) Because of Wilson's Theorem, the numbers $2, 3, 4 \ldots, 15$ can be arranged in seven pairs $\{x,y\}$ such that $xy \equiv 1 \pmod{17}$. Find these seven pairs.

(317) Let $m = m_1 m_2 \cdots m_r$, where the m_i's are integers > 1 and pairwise coprime. Show that

$$m_1^{\phi(m)/\phi(m_1)} + m_2^{\phi(m)/\phi(m_2)} + \cdots + m_r^{\phi(m)/\phi(m_r)} \equiv r - 1 \pmod{m}.$$

(318) Let p be a prime number and k an integer, $0 < k < p$. Show that

$$(k-1)!(p-k)! \equiv (-1)^k \pmod{p}.$$

(319) If p and q are distinct prime numbers, is it true that we always have

$$p^{q-1} + q^{p-1} \equiv 1 \pmod{pq}\,?$$

More generally, if m and n are positive integers such that $(m,n) = 1$, is it true that

$$n^{\phi(m)} + m^{\phi(n)} \equiv 1 \pmod{mn}\,?$$

(320) Show that for each positive integer n,

$$3^{2n+2} \equiv 8n + 9 \pmod{64}.$$

(321) Let $p \geq 5$ be a prime number. Find the value of $(p!, (p-2)! - 1)$.

(322) Show that

$$5^{6614} - 12^{857} \equiv 1 \pmod{7}.$$

(323) *Divisibility tests.* Let N be a positive integer whose decimal representation is $N = a_n 10^n + \cdots + a_2 10^2 + a_1 10 + a_0$, where $0 < a_n \leq 9$ and for $k = 0, \ldots, n-1$, $0 \leq a_k \leq 9$. Show that

(a) N is divisible by 3 $\iff$ $a_n + a_{n-1} + \cdots + a_1 + a_0 \equiv 0 \pmod{3}$.

(b) N is divisible by 4 $\iff$ $10a_1 + a_0 \equiv 0 \pmod{4}$.

(c) N is divisible by 6 $\iff$ $4(a_n + \cdots + a_1 + a_0) \equiv 3a_0 \pmod{6}$.

(d) N is divisible by 7 $\iff$ $(100a_2 + 10a_1 + a_0) - (100a_5 + 10a_4 + a_3) + (100a_8 + 10a_7 + a_6) - \cdots \equiv 0 \pmod{7}$.

(e) N is divisible by 8 $\iff$ $100a_2 + 10a_1 + a_0 \equiv 0 \pmod{8}$.

(f) N is divisible by 9 $\iff$ $a_n + a_{n-1} + \cdots + a_0 \equiv 0 \pmod{9}$.

(g) N is divisible by 11 $\iff$ $a_n - a_{n-1} + \cdots + (-1)^n a_0 \equiv 0 \pmod{11}$.

(324) Assume that 168 divides the integer whose decimal representation is "770ab45c". Find the digits a, b and c.

(325) Let a be an integer ≥ 2 and let $m \in \mathbb{N}$. If $(a,m) = (a-1,m) = 1$, show that

$$1 + a + a^2 + \cdots + a^{\phi(m)-1} \equiv 0 \pmod{m}.$$

(326) Let p be a prime number. Show that for each $a \in \mathbb{N}$, we have

$$a^{(p-1)!+1} \equiv a \pmod{p}.$$

(327) Show that if p is a prime number, then $1^{p-1} + 2^{p-1} + \cdots + (p-1)^{p-1} \equiv -1 \pmod{p}$.

(328) Show that if p is an odd prime number, then $1^p + 2^p + \cdots + (p-1)^p \equiv 0 \pmod{p}$.

(329) Let p be an odd prime number. Show that

$$\sum_{k=1}^{p-1} (k-1)!(p-k)!k^{p-1} \equiv 0 \pmod{p}.$$

(330) Letting p be a prime number of the form $4n+1$, show that $((2n)!)^2 \equiv -1 \pmod{p}$. More generally, if p is a prime number and if $m+n=p-1$, $m \geq 0$, $n \geq 0$, show that

$$m!\,n! \equiv (-1)^{m+1} \pmod{p}.$$

(A similar result was obtained in Problem 318.) Use this last formula to prove that

$$\left\{\left(\frac{p-1}{2}\right)!\right\}^2 \equiv (-1)^{(p+1)/2} \pmod{p}.$$

(331) Show that an integer $n > 2$ is prime if and only if n divides the number $2(n-3)!+1$.

(332) Show that if p is a prime number and a an arbitrary integer, then p divides the expression $a^p + a(p-1)!$.

(333) Show that if $\pi = 3.141592\ldots$ stands for Archimede's constant and $\pi(x)$ stands for the number of prime numbers $p \leq x$, then

$$\pi(x) = \sum_{2 \leq n \leq x} \left[\cos^2\left(\pi \frac{(n-1)!+1}{n}\right)\right],$$

where $[y]$ stands for the largest integer smaller or equal to y.

(334) Let $m_1, m_2 \in \mathbb{N}$ be such that $(m_1, m_2) = 1$. If a, r and s are positive integers such that $a^r \equiv 1 \pmod{m_1}$ and $a^s \equiv 1 \pmod{m_2}$. Show that

$$a^{[r,s]} \equiv 1 \pmod{m_1 m_2}.$$

(335) Let m be a positive integer. Show that for each $a \in \mathbb{N}$,

$$a^m \equiv a^{m-\phi(m)} \pmod{m}.$$

(336) Let m be a positive odd integer. Show that the sum of the elements of a complete residue system modulo m is congruent to $0 \pmod{m}$.

(337) Let $a, b \in \mathbb{Z}$, $m \in \mathbb{N}$. If E is a complete residue system modulo m and if $(a, m) = 1$, show that

$$E' = \{ax + b \mid x \in E\}$$

is also a complete residue system modulo m.

(338) Is it possible to construct a reduced residue system modulo 7 made up entirely of multiples of 6? Explain.

(339) Let $m > 2$ be an integer. Show that the sum of the elements of a reduced residue system modulo m is congruent to $0 \pmod{m}$.

(340) If $\{r_1, r_2, \ldots, r_{p-1}\}$ is a reduced residue system modulo a prime number p, show that

$$\prod_{j=1}^{p-1} r_j \equiv -1 \pmod{p}.$$

(341) Let $a, b \in \mathbb{Z}$, $m \in \mathbb{N}$. Using a counter-example, show that if E is a reduced residue system modulo m and if $(a, m) = 1$, then the set $\{ax + b \mid x \in E\}$ is not necessarily a reduced residue system modulo m.

(342) Find all integers x, y and z with $2 \leq x \leq y \leq z$ such that

$$xy \equiv 1 \pmod{z}, \quad xz \equiv 1 \pmod{y}, \quad yz \equiv 1 \pmod{x}.$$

(343) Let n and k be positive integers. Show that there exists a sequence of n consecutive composite integers such that each is divisible by at least k distinct prime numbers. Using this result, find the smallest sequence of four consecutive integers divisible by 3, 5, 7 and 11 respectively.

(344) Find all positive integers which give the remainder 1, 2 and 3 when divided respectively by 3, 4 and 5.

(345) Find the smallest integer $a > 2$ such that

$$2|a, \quad 3|a+1, \quad 4|a+2, \quad 5|a+3, \quad 6|a+4.$$

(346) Find the cycle and the period of $1/3, 1/3^2, 1/3^3, 1/3^4, 1/7, 1/7^2, 1/7^3$. Let p be an arbitrary prime number for which the period of $1/p$ is m. Using these computations, what should one conjecture regarding the periods of $1/p^2, 1/p^3, \ldots, 1/p^n$?

(347) The decimal expansion of $2/3 = 0.666\ldots$ consists in a repetition of $6 = 2 \cdot 3$. The same phenomenon occurs with the decimal expansion of $1/3 = 0.333\ldots$. Find all positive rational numbers a/b with $(a, b) = 1$, whose decimal expansion is formed by an infinite repetition of the product of its numerator and of its denominator.

(348) Show that the period of a fraction m/n with $m < n$, $(m, n) = 1$, $(n, 10) = 1$ is the smallest positive integer h such that $10^h \equiv 1 \pmod{n}$.

(349) If m/n has the cycle $a_1 a_2 \cdots a_h$, show that $m | a_1 a_2 \cdots a_h$.

(350) If $m/n = 0.\overline{a_1 a_2 \ldots a_r}$, show that

$$\frac{m}{n} = \frac{a_1 a_2 \ldots a_r}{10^r - 1},$$

where the numerator is the number made up of the r digits $a_1, a_2, \ldots, a_r$ (and not of their product).

6. Primality Tests and Factorization Algorithms

(351) Let $d > 1$ be a proper divisor of the positive integer n. Prove that $2^{n-1} + 2^{d-1} - 1$ is a composite number.

(352) Prove that if a Mersenne number, that is a number of the form $2^q - 1$ where q is prime, is not squarefree, then it must be divisible by a Wieferich prime, that is a prime number p such that $2^{p-1} \equiv 1 \pmod{p^2}$.

(353) Find the three smallest prime factors of the number $n = 5^{96} - 7^{112}$.

(354) Let $m \geq 4$ be an even integer and let $a \geq 2$ be an integer. Show that $\frac{m^a}{2} + \frac{m}{2} - 1$ is a composite number.

(355) Show that the sequence $2^{2^n} + 3$, $n = 1, 2, \ldots$, contains infinitely many composite numbers.

(356) Use Problem 354 to prove that $2^{2^6} + 15$ is a composite number.

(357) Is it true that $2^{2^n} + 15$ is a prime number for each integer $n \geq 0$? If it is true, prove it. If it is false, provide a counter-example.

(358) By a close examination of the representation of the number n given in Problem 84, obtain that $973|n$ and therefore that 139 is a prime factor of n.

(359) Knowing that the number $n = 999\,951$ has a prime factor p such that $300 < p < 400$ and observing that $n + 49 = 10^6$, find this number p.

(360) Show that 127 is a prime divisor of $2^{21} - 1$.

(361) Find four prime factors of $2^{2^6} - 1$.

(362) Prove that at least one third of the integers of the form $n10^n + 1$ are composite.

(363) Use Problem 75 to show that 3, 7 and 31 are prime factors of $2^{30} - 1$ and that 31 and 127 are prime factors of $2^{35} - 1$.

(364) Let $n = 2^{30} - 1$. Show that $11|n$ without computing explicitly the value of n.

(365) Use Problem 75 to show that 2, 5, 7 and 13 are prime factors of $3^{12} - 1$ and that 2, 5, 7, 13, 41 and 73 are prime factors of $3^{24} - 1$.

(366) Given two integers a and m larger than 1, show that, if m is odd, then $a + 1$ is a divisor of $a^m + 1$. Use this result to obtain the factorization of 1001.

(367) Generalize the result of Problem 366 to obtain that if a and m are two integers larger than 1 and if $d \geq 1$ is an odd divisor of m, then $a^{m/d} + 1$ is a divisor of $a^m + 1$. Use this result to show that 101 is a factor of 1000001.

(368) Show that 7, 11 and 13 are factors of $10^{15} + 1$.

(369) Show that $n^4 + 4$ is a composite number for each integer $n \geq 2$. More generally show that if a is a positive integer such that $2a$ is a perfect square, then $n^4 + a^2$ is a composite number provided $n \geq \sqrt{2a}$.

(370) Show that there exist infinitely many composite numbers of the form $k10^k + 1$.

(371) Show that if the number $k + 2$ is prime, then it is a prime divisor of the number $2k^k + 1$.

(372) Find three factors of $2^{58} + 1$.

(373) Let $M_p = 2^p - 1$, where p is an odd prime number. Show that all the factors of M_p are of the form $2kp + 1$, where $k \in \mathbb{N}$.

(374) The primality test of Lucas-Lehmer may be read as follows: "Let p be an odd prime number. The Mersenne number $M_p = 2^p - 1$ is prime if and only if $M_p | S_{p-1}$, where $S_1 = 4$ and $S_{n+1} \equiv S_n^2 - 2 \pmod{M_p}$, $n \geq 1$." Use this test (and a computer) to prove that M_{61} is prime.

(375) Factor the number $n = 10^{48} - 1$. A computer may prove handy to obtain certain factors of n smaller than 10^9.

(376) In 1960, Waclaw Sierpinski (1882–1969) proved that there exist infinitely many integers k such that each of the numbers $N = k \cdot 2^n + 1$ ($n = 1, 2, 3, \ldots$) is composite. Three years later, Selfridge proved that the number $k = 78\,557$ is such a number. Prove this last result of Selfridge by establishing that, in this case, N is always divisible by 3, 5, 7, 13, 19, 37 or 73.

(377) Find three prime factors of $10^{27} + 1$.

(378) In order to obtain the factorization of the odd integer $n > 1$, it certainly helps to notice that, if n is composite, it is always possible to write n as

$$(*)\quad n = x^2 - y^2 = (x+y)(x-y) \quad \text{with } x, y \text{ positive integers, } x - y > 1,$$

thus revealing the factors $x + y$ and $x - y$ of n (see Problems 81 and 82). To obtain a representation of type $(*)$, we may proceed as follows. We look for an integer x such that $x^2 - n$ is a perfect square, that is such that

$$x^2 - n = y^2.$$

As a first value for x, we choose the smallest integer k such that $k^2 \geq n$, and then we try with $k + 1$, and so on. By proceeding in this manner, it is clear that we will eventually find an integer x such that $x^2 - n$ is a perfect square, the reason being that n is odd and composite. This factorization method is called FERMAT'S FACTORIZATION METHOD.

To show the method, we take $n = 2001$. Since $\sqrt{n} = 44.7325\ldots$, we shall successively try several values of x starting with $x = 45$; we then obtain the following table:

x	$x^2 - n = ?$	Perfect square?
45	$45^2 - 2001 = 24$	NO
46	$46^2 - 2001 = 115$	NO
47	$47^2 - 2001 = 208$	NO
48	$48^2 - 2001 = 303$	NO
49	$49^2 - 2001 = 400$	YES

Hence, $2001 = 49^2 - 20^2 = (49+20)(49-20) = 69 \cdot 29$, thus providing a factorization of 2001.

Proceed as above in order to factorize 2009, and then use Fermat's factorization method to find two proper divisors of $n = 289\,751$.

(379) Fermat's factorization method works very well when the odd integer n which is to be factored has two divisors of roughly the same size. But if $n = pq$, where $p < q$ are far apart, the number of steps to reach a factorization may be very large. But this difficulty may be overcome. For instance, take the number $n = 1\,254\,713$. Multiply this number by a small prime number p_0, the goal being to obtain a number $m = p_0 n = d_1 d_2$,

where d_1 and d_2 are two positive integers whose quotient d_2/d_1 is close to 1. Use this strategy to obtain the factorization of n.

(380) Assume that $n = pq$, where p and q are two prime numbers satisfying $p < q < 2p$. Let δ be the number defined by

$$\frac{q}{p} = 1 + \delta,$$

so that $0 < \delta < 1$. Show that the number of steps necessary to factorize n by using Fermat's factorization method is approximately $\frac{p\delta^2}{8}$.

(381) Knowing that the number $n = 188\,686\,013$ is the product of two prime numbers p and q such that

$$\left|\frac{p}{q} - 3\right| < \frac{1}{100},$$

find the factorization of n.

(382) Given an integer $r \geq 2$ and an odd integer $k \geq 5$, consider the number

$$n = r^k + r^{k-1} + \cdots + r^2 + r + 1.$$

Prove that the number n has at least three prime factors and moreover that they are distinct if $r \geq 3$ or if $r = 2$ and $k \geq 7$.

(383) Let k be a positive integer. Show that $\{2^k \pm 2^{k-1} \pm 2^{k-2} \pm \cdots \pm 2^1 \pm 1\}$ represents the set of all positive odd numbers $\leq 2^{k+1} - 1$.

(384) The number 11 is prime, while it is easy to check that the numbers 111, 1 111 and 11 111 are composite.

(i) Show that if a number of the form $\underbrace{111\ldots1}_{k} = (10^k - 1)/9$ is prime, then the number k is necessarily a prime.

(ii) Show that, if p is a prime number, then each prime factor of $(10^p - 1)/9$ is of the form $2jp + 1$ for a certain positive integer j.

(iii) Use a computer to find the five smallest prime numbers p such that the number corresponding to $(10^p - 1)/9$ is prime.

(iv) Use a computer to obtain the factorization of the numbers $(10^p - 1)/9$ for each prime number $p < 50$.

(385) Show that each positive integer n for which there exist positive integers k, x and y such that

$$(*) \qquad n = x^{2k+1} + y^{2k+1}$$

is composite.

(386) Let n be a positive odd integer for which there exists a prime number $p_0 < \sqrt{n}$ such that $p_0 \cdot n$ can be written as the sum of two positive cubes. Show that n must be a composite number.

(387) Consider the number $n = 52\,657\,403$. Show that $7n$ can be written as the sum of two cubes (one of which is rather small!) and conclude that n is composite and divisible by 719.

(388) Consider the number $n = 237\,749\,938\,896\,803$. Show that $11n$ can be written as the sum of two fifth powers (one of which is rather small!) and conclude that n is composite and divisible by 1213.

(389) Let $n \geq 3$ be a squarefree odd composite number. Show that if for each prime divisor p of n, we have $p - 1 | n - 1$, then n is a Carmichael number.

(390) Let $p \geq 5$ be a prime number such that $2p-1$ and $3p-2$ are primes. Show that the number $n = p(2p-1)(3p-2)$ is a Carmichael number.

(391) Use Korselt's Criterion (mentioned in the remark on the solution of Problem 389) in order to prove that each Carmichael number must have at least three distinct prime factors.

(392) In the remark attached to the solution of Problem 389, we observed that an integer $n = q_1 q_2 \cdots q_k$, where $k \geq 3$ and $2 < q_1 < q_2 < \ldots < q_k$ are prime numbers, is a Carmichael number if and only if

$$(*) \qquad q_j - 1 \Big| \prod_{i=1}^{k} q_i - 1 \qquad (j = 1, 2, \ldots, k).$$

Show that condition $(*)$ can be replaced by the condition

$$q_j - 1 \Big| \prod_{\substack{i=1 \\ i \neq j}}^{k} q_i - 1 \qquad (j = 1, 2, \ldots, k).$$

(393) Observing that

$$(*) \qquad 327\,763 = 30^3 + 67^3 = 51^3 + 58^3,$$

find the factorization of 327 763.

(394) Searching for a prime factor of $n = 48\,790\,373$, we observe that

$$7 \cdot n = 341\,532\,611 = 699^3 + 8^3.$$

Use this information to obtain the factorization of n.

(395) In 1956, Paul Erdős raised the question of obtaining the value of the smallest integer $n > 3$ such that $2^n - 7$ is prime. Use a computer to find this number n as well as the five next numbers n with the same property. Show that, in this search, one may ignore even integers n, the integers $n \equiv 1 \pmod 4$, the integers $n \equiv 7 \pmod{10}$ as well as the integers $n \equiv 11 \pmod{12}$.

(396) Let $a \geq 2$ be an integer and let p be a prime number such that p does not divide $a(a^2-1)$. Show that the number

$$n = \frac{a^{2p} - 1}{a^2 - 1}$$

is pseudoprime in basis a. Use this method to find pseudoprimes in basis 2 and 3.

(397) Show that there exist infinitely many pseudoprimes in basis 2.

(398) Let a and m be two positive integers such that $(a, m) = 1$. We say that s is the order of a modulo m if s is the smallest positive integer such that $a^s \equiv 1 \pmod m$. Show that if $a^n \equiv 1 \pmod m$, then $s|n$.

(399) (LUCAS' TEST) Let $n \geq 3$ be an integer such that for each prime factor q of $n-1$ there exists an integer $a > 1$ such that $a^{n-1} \equiv 1 \pmod n$ and $a^{(n-1)/q} \not\equiv 1 \pmod n$. Show that n is prime.

(400) Let $n = 10^{12} + 61$. First verify that $2^2 \cdot 5 \cdot 3947 \cdot 12667849$ is indeed the factorization of $n-1$, and then use Lucas' Test, explained in Problem 399 (with an appropriate choice of a), to show that n is prime.

(401) Use the primality test of Lucas, explained in Problem 399, to prove that the numbers $n = r^4 + 1$, where r takes successively the values 1910, 1916 and 1926, are all primes.

(402) Let $n = 10^{12} + 63$. Verify that $n - 1 = 2 \cdot 3^2 \cdot 7 \cdot 47 \cdot 168861871$, and then use Lucas' Test, explained in Problem 399 (with an appropriate choice of a), to show that n is prime.

(403) (POLLARD $p-1$ FACTORIZATION METHOD) Let n be a positive integer. Assume that n has an odd prime factor p such that $p-1$ has all its prime factors $\leq k$, where k is a relatively small positive integer (such as $k = 100$ or 1000 or 10000), so that $(p-1)|k!$. Let m be the residue modulo n of $2^{k!}$ and let $g = (m-1, n)$. Show that $g > 1$, thus identifying a factor of n.

(404) Use the Pollard $p-1$ factorization method to find the smallest prime factor of the Fermat number $F_9 = 2^{2^9} + 1$.

(405) Use the Pollard $p-1$ factorization method and a computer to factor the number 252123019542987435093029.

(406) Use the Pollard $p-1$ factorization method and a computer to obtain the three prime factors of the Mersenne number

$$2^{71} - 1 = 2361183241434822606847.$$

(407) Use the Pollard $p-1$ factorization method and a computer to factor the number 136258390321.

(408) Let $n = 302\,446\,877$. Let m be the quantity $2^{25!}$ modulo n. Show that $g = (m-1, n) = 17\,389$. Use the Pollard $p-1$ factorization method to conclude that 17 389 is a (prime) divisor of 302 446 877.

(409) Show that each prime factor p of the Fermat number $F_n = 2^{2^n} + 1$ with $n \geq 2$ is of the form $p = k \cdot 2^{n+2} + 1$, $k \in \mathbb{N}$.

(410) Use the result of Problem 409 in order to prove that 641 is a prime factor of $F_5 = 2^{2^5} + 1 = 4\,294\,967\,297$.

(411) Use the result of Problem 409 in order to prove that 274 177 is a prime factor of

$$F_6 = 2^{2^6} + 1 = 18\,446\,744\,073\,709\,551\,617.$$

(412) (PEPIN'S TEST) Let $F_n = 2^{2^n} + 1$ be a Fermat number and let $k > 2$ be an integer. Show that, for $n \geq 2$,

$$F_n \text{ is prime and } \left(\frac{k}{F_n}\right) = -1 \quad \Longleftrightarrow \quad k^{\frac{F_n - 1}{2}} \equiv -1 \pmod{F_n}.$$

12. Quadratic Reciprocity

(883) Characterize all prime numbers $p > 11$ for which

$$x^2 \equiv 11 \pmod{p}$$

has a solution.

(884) Which of the following congruences have solutions?
(a) $x^2 \equiv 1 \pmod 3$;
(b) $x^2 \equiv -1 \pmod 3$;
(c) $x^2 + 4x + 8 \equiv 0 \pmod 3$;
(d) $x^2 + 8x + 16 \equiv -1 \pmod{17}$.

(885) Find the solutions of the congruence $2x^2 + 3x + 1 \equiv 0 \pmod 7$.

(886) Show that $(1!)^2 + (2!)^2 + \cdots + (n!)^2$ is never a perfect square, whatever the integer $n > 1$.

(887) Let $n \in \mathbb{N}$. Show that the odd prime divisors of $n^2 + 1$ are of the form $12k + 1$ or of the form $12k + 5$.

(888) Let $p > 3$ be a prime number. Show that p divides the sum

$$\sum_{\substack{j=1 \\ (\frac{j}{p})=1}}^{p-1} j.$$

(889) Assuming that m is a positive integer such that $p = 4m+3$ and $q = 2p+1$ are two prime numbers, show that $q|M_p = 2^p - 1$. Use this result to show that the Mersenne number $M_{1\,122\,659}$ is composite.

(890) Show that 9239 divides $2^{4619} - 1$.

(891) Show that 5 is a nonquadratic residue of all the prime numbers of the form $6^n + 1$.

(892) Does there exist a perfect square of the form $1997k - 1$?

(893) Show that there exist infinitely many prime numbers of the form $3k + 1$.

(894) Does there exist a perfect square of the form $1! + 2! + \cdots + k!$ with $k > 3$?

(895) Show that for each integer $n > 1$, $(2^n - 1) \not| (3^n - 1)$.

(896) Let p and q be two odd prime numbers, and a an integer. If $p = q + 4a$, is it true that $\left(\frac{p}{q}\right) = \left(\frac{a}{q}\right)$?

(897) If p is a prime number of the form $24k + 1$, is it true that $\left(\frac{3}{p}\right) = 1$?

(898) Does the congruence $x^2 \equiv 52 \pmod{159}$ have any solutions?

(899) If p is a prime number of the form $8k+3$ and if $q = \frac{p-1}{2}$ is a prime number, can one conclude that q is a quadratic residue modulo p?

(900) Show that 3 is a nonquadratic residue of all Mersenne primes larger than 3.

(901) If p is a prime number of the form $p = 8k + 7$, show that

$$p|2^{\frac{p-1}{2}} - 1.$$

(902) Does the congruence $x^2 \equiv 2 \pmod{231}$ have any solution? If so, what are they? If not, explain why.

(903) Does there exist a positive integer n and a prime number p of the form $p = 100k + 3$ such that $p|n^2 + 1$? Explain.

(904) Is it true that there exist infinitely many positive integers n such that $23|n^2+14n+47$? Explain.

(905) Does there exist an integer x such that the prime number 541 divides x^2-3x-1? Explain.

(906) If p is a prime number, $p \equiv 1 \pmod{24}$, does the congruence $x^2 \equiv 6 \pmod{p}$ have any solution? Explain.

(907) Let n be a positive integer such that $p = 4^n + 1$ is a prime number. Does the congruence $x^2 \equiv 3 \pmod{p}$ have any solution? Explain.

(908) Let A be the set of integers a, $1 \leq a \leq 43$, for which there exists a prime number $p \equiv a \pmod{44}$ such that the corresponding congruence

$$x^2 \equiv 11 \pmod{p}$$

has solutions. Determine A.

(909) Find all prime numbers p for which $\left(\frac{5}{p}\right) = -1$.

(910) Let p and q be odd prime numbers such that $p = q + 4a$, $a \in \mathbb{N}$. Show that

$$\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right).$$

(911) Of which prime numbers is the number -2 a quadratic residue?

(912) Let p be an odd prime number. Show that $x^2 \equiv 2 \pmod{p}$ has solutions if and only if $p \equiv 1$ or $7 \pmod{8}$. Using this result, prove that $2^{4n+3} \equiv 1 \pmod{8n+7}$ for each integer $n \geq 0$. In particular, find a proper divisor of the Mersenne number $2^{131} - 1$.

(913) Observing that $2717 = 11 \cdot 13 \cdot 19$, determine if the quadratic congruence $x^2 \equiv 1237 \pmod{2717}$ has solutions.

(914) Let a be an integer such that $(a, p) = 1$. Determine all prime numbers p such that $\left(\frac{a}{p}\right) = \left(\frac{p-a}{p}\right)$.

(915) Does the congruence $x^2 \equiv 131313 \pmod{1987}$ have any solutions?

(916) Show that the equation $x^2 - y^3 = 7$ has no integer solution.

(917) Determine all prime numbers p for which 15 is a quadratic residue modulo p.

(918) Show that the statement of the law of quadratic reciprocity can be written (as Gauss did) as

$$\left(\frac{p}{q}\right) = \left(\frac{(-1)^{(q-1)/2}q}{p}\right).$$

(919) Does the congruence $x^2 \equiv 34561 \pmod{1234577}$ have any solution?

(920) Show that if r is a quadratic residue modulo $m > 2$, then

$$r^{\phi(m)/2} \equiv 1 \pmod{m}.$$

(921) Let a be an integer > 1 and let n be a positive integer. Show that $n|\phi(a^n - 1)$.

(922) Show that if p is an odd prime number, then

$$\sum_{j=1}^{p-1} \left(\frac{j}{p}\right) = 0.$$

(923) Let p be an odd prime number. Show that

$$\sum_{k=1}^{p-2}\left(\frac{k(k+1)}{p}\right) = -1.$$

(924) Let $p > 5$ be a prime number. Using the Problem 923, show that one can always find two consecutive integers which are quadratic residues modulo p, as well as two consecutive integers which are quadratic nonresidues modulo p.

(925) Find all prime numbers p such that the corresponding numbers $5p+1$ are perfect squares. Is it possible to find prime numbers p for which $5p+2$ are perfect squares?

(926) Let $f\colon \mathbb{Z} \to \mathbb{Z}$ be a polynomial function and let a, b be integers. Set $\left(\frac{m}{p}\right) = 0$ if $p|m$. If $(a,p) = 1$, show that

$$\sum_{k=0}^{p-1}\left(\frac{f(ak+b)}{p}\right) = \sum_{k=0}^{p-1}\left(\frac{f(k)}{p}\right).$$

Use this to prove that if $(a,p) = 1$, then

$$\sum_{k=0}^{p-1}\left(\frac{ak+b}{p}\right) = 0.$$

(927) Let $a, b \in \{-1, 1\}$, p be an odd prime number and

$$N(a,b) = \#\left\{k \mid 1 \le k \le p-2, \quad \left(\frac{k}{p}\right) = a, \quad \left(\frac{k+1}{p}\right) = b\right\}.$$

Show that

$$N(a,b) = \frac{1}{4}\left(p - 2 - b - ab - a(-1)^{(p-1)/2}\right).$$

Use this to prove that the number of pairs of consecutive quadratic residues modulo p is given by

$$N(1,1) = \frac{p - 4 - (-1)^{(p-1)/2}}{4}.$$

(928) Let p be a prime number satisfying $p \equiv 1 \pmod 4$. Show that

$$\sum_{j=1}^{(p-1)/2}\left(\frac{j}{p}\right) = 0.$$

(929) Let p be a prime number such that $p \equiv 1 \pmod 4$. Show that

$$\sum_{k=1}^{p-1} k\left(\frac{k}{p}\right) = 0.$$

(930) Let p be a prime number such that $p \equiv 1 \pmod 4$. Show that

$$\sum_{\substack{k=1 \\ \left(\frac{k}{p}\right)=1}}^{p-1} k = \frac{p(p-1)}{4}.$$

(931) Let p be a prime number such that $p \equiv 3 \pmod 4$. Show that

$$\sum_{k=1}^{p-1} k^2 \left(\frac{k}{p}\right) = p \sum_{k=1}^{p-1} k \left(\frac{k}{p}\right).$$

(932) Show that the equation $x^2 - 33y^2 = 5$ has no integer solutions.