Chapter 1

Divisibility

The parts of this chapter used in the rest of the book are: the Euclidean algorithm and its applications (problems 1.5.7 and 1.5.9), the language of congruences (section 4, "Division with a remainder and congruences"), and some simple facts (e.g., problem 1.1.3 and 1.3.2).

In this chapter all variables are integers. Many solutions are based on M. A. Prasolov's texts.

1. Divisibility (1)

1.1.1. (a) State and prove the rules of divisibility by 2, 4, 5, 10, 3, 9, 11.

(b) Is the number $11\ldots1$ consisting of 1993 ones divisible by 111111?

(c) Prove that the number $1\ldots1$ consisting of 2001 ones is divisible by 37.

1.1.2. If a is divisible by 2 and not divisible by 4, then the number of even divisors of a is equal to the number of its odd divisors.

1.1.3. Which of the following statements are correct for any a and b? (Recall the notation $a|b$ defined on p. xx.)

(a) $2|(a^2-a)$.
(b) $4|(a^4-a)$.
(c) $6|(a^3-a)$.
(d) $30|(a^5-a)$.
(e) If $c|a$ and $c|b$, then $c|(a+b)$.
(f) If $b|a$, then $bc|ac$.
(g) If $bc|ac$ for some $c\neq 0$, then $b|a$.

To solve problem 1.1.3 (c), we used 1.1.4 (a). Prove it using the definition of divisibility, but not using the Unique Factorization Theorem (problem 1.2.8 (d))! The use of this theorem might lead to a circular argument since a result similar to 1.1.4 (a) is usually used in a proof of uniqueness of factorization.

1.1.4. (a) If a is divisible by 2 and 3, then it is also divisible by 6;
(b) If a is divisible by 2, 3, and 5, then it is also divisible by 30;
(c) If a is divisible by 17 and 19, then it is also divisible by 323.

1.1.5. (a) If k is not divisible by 2, 3, or 5, then $k^4 - 1$ is divisible by 240.
(b) If $a + b + c$ is divisible by 6, then $a^3 + b^3 + c^3$ is also divisible by 6.
(c) If $a + b + c$ is divisible by 30, then $a^5 + b^5 + c^5$ is also divisible by 30.
(d) If $n \geq 0$ then $20^{2n} + 16^{2n} - 3^{2n} - 1$ is divisible by 323.

Suggestions, solutions, and answers

1.1.1. In the proofs of divisibility rules below, we denote the number in the statements by $n = \pm(10^m a_m + 10^{m-1} a_{m-1} + \ldots + 10a_1 + a_0)$ for some $0 \leq a_i \leq 9$.

Rule of divisibility by 2: An integer is divisible by 2 if and only if the last digit of the integer is divisible by 2.

Proof. Clearly, the number $n - a_0$ is even. Suppose a_0 is also even. If a number divides each term of the sum, it divides the sum. Therefore n is even. Conversely, if a number n is even, then a_0 is even. □

Rule of divisibility by 4: An integer n is divisible by 4 if and only if the number formed by its last two digits is divisible by 4.

Proof. Clearly, the number $(n - 10a_1 - a_0)$ is divisible by 4. Suppose that the number $a_0 + 10a_1$ formed by the last two digits of n is divisible by 4. Then n is divisible by 4. Conversely, if $4|n$ then $4|(a_0 + 10a_1)$. □

Rule of divisibility by 5: An integer is divisible by 5 if and only if its last digit is 5 or 0.

Prove this similarly to proving the rule of divisibility by 2.

Rule of divisibility by 10: An integer is divisible by 10 if and only if its last digit is 0.

Prove this similarly to proving the rule of divisibility by 2.

Rule of divisibility by 3: An integer n is divisible by 3 if and only if the sum of its digits is divisible by 3.

Proof. Subtract the sum of digits from the number and group the summands as follows:

$$\begin{aligned} n - a_m - a_{m-1} - \ldots - a_1 - a_0 \\ = (10^m - 1)a_m + (10^{m-1} - 1)a_{m-1} + \cdots + (10 - 1)a_1 + (1 - 1)a_0. \end{aligned}$$

The number $10^k - 1 = (10 - 1)(10^{k-1} + 10^{k-2} + \ldots + 10 + 1)$ is divisible by 3. The rule of divisibility by 3 follows from this observation. □

Rule of divisibility by 9: An integer n is divisible by 9 if and only if the sum of its digits is divisible by 9.

Prove this similarly to proving of the rule of divisibility by 3.

Rule of divisibility by 11: Subtract the sum of all digits of n at odd positions from the sum of all digits at even positions. The number n is divisible by 11 if and only if the resulting number $f(n)$ is divisible by 11.

Proof. First, we will prove that for any $m \geq 0$ the number $10^m - (-1)^m$ is divisible by 11. For odd m, the number $10^m + 1 = (10+1)(10^{m-1} - 10^{m-2} + 10^{m-3} - \ldots - 10 + 1)$ is divisible by 11. For even m, the number $10^m - 1$ is divisible by $10^2 - 1$ and hence divisible by 11. Now we have

$$\begin{aligned} n - f(n) = (10^m - (-1)^m)a_m + (10^{m-1} - (-1)^{m-1})a_{m-1} \\ + \ldots + (10 + 1)a_1 + (1 - 1)a_0. \end{aligned}$$

Since every term of the sum on the right-hand side of the equation is divisible by 11, n is divisible by 11 if and only if $f(n)$ is divisible by 11. □

1.1.3. *Answers*: (a, c, d, e, f) true; (b) false.

(a) We have $a^2 - a = a(a - 1)$. Taken in the natural order, every other integer is even; thus one of the numbers a or $a - 1$ is even, so their product $a^2 - a$ is also even.

(b) 4 does not divide $(2^4 - 2) = 14$.

(c) We have $a^3 - a = a(a - 1)(a + 1)$. The number $a(a - 1)$ is divisible by 2 while $(a-1)a(a+1)$ is divisible by 3. Thus $a^3 - a$ is divisible by 2 and 3, and, as follows from 1.1.4 (a), it is divisible by 6.

(d) We have $a^5 - a = a(a - 1)(a + 1)(a^2 + 1)$. Now, $a(a - 1)$ is divisible by 2 while $(a - 1)a(a + 1)$ is divisible by 3. If none of the numbers $a - 1$, a, and $a + 1$ is divisible by 5, then the remainder from dividing a by 5 is equal to 2 or 3. Thus $a^2 + 1$ is divisible by 5. Then, as follows from 1.1.4 (b), $a^5 - a$ is divisible by 30.

(e) If $a = kc$ and $b = mc$, then $a + b = (k + m)c$.

(f) If $a = kb$ then $ac = k(bc)$.

(g) If $ac = kbc$ then $c(a - kb) = 0$. Since $bc \neq 0$ we have $c \neq 0$; therefore $a = kb$.

1.1.4. (a) *Hint.* We have $3a - 2a = a$.

Solution. Since $2|a$ we have $6|3a$, and since $3|a$ we have $6|2a$; therefore $6|(3a - 2a) = a$.

(b) *Hint.* $6a - 5a = a$.

Solution. From the given conditions and part (a) above we have $6|a$ and $5|a$. Therefore $30|6a$ and $30|5a$, so $30|(6a - 5a) = a$.

(c) *Hint.* $19a - 17a = 2a$, $17a - 8 \cdot 2a = a$.

Solution. From the given conditions we have $17|a$ and $19|a$. Therefore $17 \cdot 19|17a$ and $19 \cdot 17|19a$. So $17 \cdot 19|(19a - 17a) = 2a$. Then $17 \cdot 19|(17a - 8 \cdot 2a) = a$.

1.1.5. (d) The number $(a^n - b^n) = (a - b)(a^{n-1} + a^{n-2}b + \ldots + b^{n-1})$ is divisible by $(a-b)$. Therefore $20^{2n}+16^{2n}-3^{2n}-1 = (20^{2n}-3^{2n})+((16^2)^n-(1^2)^n)$ is divisible by 17. Similarly, $20^{2n} + 16^{2n} - 3^{2n} - 1 = (20^{2n} - 1) + ((16^2)^n-(3^2)^n)$ is divisible by 19. Then, according to 1.1.4 (c), $20^{2n}+16^{2n}-3^{2n} - 1$ is divisible by 323.

2. Prime numbers (1)

An integer $p > 1$ is said to be a *prime* if it does not have positive divisors other than p and 1. An integer q is a *composite* if it has at least one positive divisor different from 1 and $|q|$. (Thus 1 is neither a prime nor a composite number.)

1.2.1. (a) **Lemma.** If $a¿1$ is not divisible by any prime $p \leq \sqrt{a}$, then a is a prime.

(b) **Sieve of Eratosthenes.** Let $p_1, \ldots, p_k$ all be primes between 1 and n. For each $i = 1, \ldots, k$ we will cross out all numbers between 1 and n^2 which are divisible by p_i. Numbers which are left are all primes between n and n^2.

(c) Write down all primes between 1 and 200.

1.2.2. (a) Find all p such that p, $p + 2$, and $p + 4$ are primes.

(b) Prove that if the number $11\ldots1$ consisting of n ones is a prime, then n is a prime.

(c) Prove that the converse of (b) is not true.

Theorem 1.2.3 (Euclid)**.** (a) There are infinitely many primes.

(b) There are infinitely many primes of the form $4k + 3$.

Compare to problem 2.3.3 (f). Using advanced techniques it's possible to prove the following statement.

Theorem 1.2.4 (Dirichlet)**.** If the integers $a, b > 0$ have no common divisors other than ± 1, then there are infinitely many primes of the form $ak + b$.

1.2.5. Let p_n denote the nth prime number (in ascending order).

(a) Prove that $p_{n+1} \leq p_1 \cdot \ldots \cdot p_n + 1$

(b) Prove that $p_{n+1} \leq p_1 \cdot \ldots \cdot p_n - 1$ for $n \geq 2$.

(c)* Prove that there is a perfect square between $p_1 + \ldots + p_n$ and $p_1 + \ldots + p_{n+1}$.

1.2.6. (a) Is it true that for any n, the number $n^2 + n + 41$ is a prime?

(b) Prove that for any non-constant quadratic function f with integer coefficients, there exists an integer n such that the number $|f(n)|$ is composite.

(c) Prove that for any non-constant polynomial f with integer coefficients, there exists an integer n such that the number $|f(n)|$ is composite.

1.2.7. There exist 1000 consecutive numbers, none of which is

(a) a prime;

(b) a power of a prime.

1.2.8. (a) Any positive integer may be decomposed into a product of prime numbers.

(b) An even number is called *primish* if it is not a product of two smaller positive even numbers. Is the decomposition of an even number into a product of primish numbers necessarily unique? (See a more meaningful example in problem 3.7.3 (b).)

(c)* If a number is equal to the product of two primes, this decomposition is unique up to the order of the factors.

(d) **Fundamental Theorem of Arithmetic.** The decomposition of any positive integer into a product of primes is unique up to the order of the factors. (This theorem is often referred to as the Unique Factorization Theorem or the Canonical Decomposition Theorem.)

For the (usual) solution of (b) and (c) you will need the lemmas in problem 1.5.7. See also problem 3.4.5.

Suggestions, solutions, and answers

1.2.2. (a)*Answer*: $p = 3$.

Solution. The numbers p, $p + 2$, and $p + 4$ have different remainders upon division by 3. Therefore one of them is divisible by 3. This number is a prime, so it is equal to 3. Since all primes by definition are positive

integers, then $p+4 \neq 3$. Since 1 is not a prime, $p+2 \neq 3$. Thus $p = 3$. This is indeed our solution, because 3, 5, and 7 are primes.

(b) Assume to the contrary that n is composite, i.e., $n = ab$, where $a, b > 1$. We have $x^b - 1 = (x-1)(x^{b-1} + x^{b-2} + \ldots + x + 1)$. Substituting $x = 10^a$ we see that $11\ldots1 = \frac{10^n-1}{9}$ is divisible by $\frac{10^a-1}{9}$.

(c) The converse statement is false: $111 = 37 \cdot 3$.

1.2.7. (a) For example, 1000!+2, 1000!+3, ..., 1000!+1001. The problem can also be solved similarly to part (b).

(b) Take different primes $p_1, p_2, \ldots, p_{2000}$. The *Chinese Remainder Theorem* 1.5.10 (d) implies that there exists n such that $n + i$ is divisible by $p_{2i-1}p_{2i}$ for any $i = 1, 2, \ldots, 1000$.

1.2.8. (a) Suppose that not every integer is a product of primes. Consider the smallest positive integer n which is not a product of primes. If it is not a prime, then it is a composite number, so $n = ab$ for some $a, b > 1$. Therefore $n > a$ and $n > b$. But n is the smallest integer not equal to a product of primes, so a and b are both products of primes. Hence n is also a product of primes. This contradicts our assumption.

(d) Suppose the assertion is false. Consider the smallest number n having two different canonical decompositions: $n = p_1^{a_1} \cdot p_2^{a_2} \cdot \ldots \cdot p_m^{a_m} = q_1^{b_1} \cdot q_2^{b_2} \cdot \ldots \cdot q_k^{b_k}$. Since n is minimal, none of the numbers p_i is equal to any q_j, for otherwise we could divide both sides of the equality by this number and get a smaller number with two different canonical decompositions. On the other hand, q_1 divides $p_1^{a_1} \cdot p_2^{a_2} \cdot \ldots \cdot p_m^{a_m}$ and therefore, as follows from 1.5.7 (c), q_1 divides one of numbers p_i. Since p_i is a prime, we have $q_1 = p_i$. This contradicts our assumption.

3. Greatest common divisor (GCD) and least common multiple (LCM) (1)

The integers a and b are said to be *relatively prime* if they don't have common divisors other than ± 1.

An integer is said to be the *greatest common divisor* (GCD) of two positive integers a and b if it is the greatest number that divides both a and b. We denote the GCD of a and b by (a, b) or $\mathrm{GCD}(a, b)$ or $\gcd(a, b)$.

1.3.1. Find all possible values:
(a) $(n, 12)$; (b) $(n, n+1)$; (c) $(n, n+6)$; (d) $(2n+3, 7n+6)$; (e) $(n^2, n+1)$.

Lemma 1.3.2. For $a \neq b$ the following equality is valid: $(a, b) = (|a-b|, b)$.

1.3.3. (a) $(a, b) = b$ if and only if a is divisible by b.

(b) The numbers $\frac{a}{(a,b)}$ and $\frac{b}{(a,b)}$ are relatively prime.
(c)* The number (a, b) is divisible by any common divisor of a and b.
(d)* We have $(ca, cb) = c(a, b)$ for any $c > 0$.

To solve problems marked with an asterisk, you will need the lemmas in 1.5.7.

1.3.4. (a) For all positive m and n we have

$$(2m, 2n) = 2(m, n), \quad (2m + 1, 2n) = (2m + 1, n),$$
$$(2m + 1, 2n + 1) = (2m + 1, m - n) \quad \text{for } m > n.$$

(b) *Binary algorithm.* Using the equalities from (a) construct an algorithm for finding the GCD.

1.3.5.* If a fraction $\frac{a}{b}$ is irreducible, then the fraction $\frac{a+b}{ab}$ is also irreducible.

An integer is said to be the *least common multiple* (LCM) of two positive integers a and b if it is the smallest number that is divisible by a and b. We denote the LCM of a and b by $[a, b]$ or $\mathrm{LCM}(a, b)$ or $\mathrm{lcm}(a, b)$.

1.3.6. Find $[192, 270]$.

1.3.7. (a) $[a, b] = a$ if and only if a is divisible by b.
(b) The numbers $\frac{[a,b]}{a}$ and $\frac{[a,b]}{b}$ are relatively prime.
(c)* Any common multiple of a and b is divisible by $[a, b]$.
(d)* $[ca, cb] = c[a, b]$ for any $c > 0$.

Suggestions, solutions, and answers

1.3.1. *Answers*: (a) 1,2,3,4,6,12. (b) 1. (c) 1,2,3,6. (d) 1,3,9. (e) 1.
Solutions.
(a) The number $(12, n)$ is a positive divisor of 12. Let $d|12$. The number d does not have divisors greater than itself, so $(12, d) = d$. Thus, all positive divisors of 12 satisfy the condition of the problem.
(b) Let $d|n, d|(n + 1)$, and $d > 0$. Then $d|(n + 1 - n) = 1$, so $d = 1$.
(c) By Lemma 1.3.2 above, $(n, n + 6) = (6, n)$. Similarly to (a), all positive divisors of 6 satisfy the condition of the problem.
(d) By Lemma 1.3.2, $(2n+3, 7n+6) = (2n+3, 5n+3) = (2n+3, 3n) = (2n + 3, n - 3) = (n + 6, n - 3) = (n + 6, 9)$.
Thus, all positive divisors of 9 satisfy the condition of the problem.
(e) Let $d > 0$ be a common divisor of the numbers $n + 1$ and n^2. Thus $d|(n + 1)(n - 1) = n^2 - 1$ by Lemma 1.3.2. So $d|(n^2 - (n^2 - 1)) = 1$, and hence $d = \pm 1$.

1.3.2. The statement follows from the fact that the set of common divisors of a and b coincides with the set of common divisors of a and $a \pm b$. Indeed, if $d|a$ and $d|b$ then $d|(a \pm b)$. Conversely, if $d|(a \pm b)$ and $d|a$ then $d|(a \pm b - a) = \pm b$.

1.3.3. (a) Let $b|a$. Since any positive divisor of a nonzero integer n does not exceed $|n|$, we have $(a, b) = |b|$. Conversely, let $(a, b) = |b|$. Then $b|a$ by definition.

(b) If $d > 0$ is a common divisor of $\frac{a}{(a,b)}$ and $\frac{b}{(a,b)}$, then $d \cdot (a, b)$ is a common divisor of a and b. If $d > 1$ this is a contradiction.

(c) Let $a > b \geq 0$. In the proof of Lemma 1.3.2 we showed that the set of common divisors of a and b coincides with the set of common divisors of a and $a \pm b$. Apply the Euclidean algorithm to the pair of numbers $a_0 = a$ and $b_0 = b$ (see problem 1.5.9 (b)). The numbers a_k and b_k obtained in the kth step are positive. The common divisors of a_k and b_k coincide with common divisors of $a_k - b_k$ and b_k. Therefore all common divisors (and, in particular, the GCD) of all intermediate pairs are the same. At the final step of the Euclidean algorithm, we see that divisors of the number $d = \gcd(a, b)$ coincide with common divisors of the numbers a and b.

(d) The number $c(a, b)$ is a common divisor of the numbers ca and cb.

To prove this we show that $(ca, cb)|c(a, b)$. Obviously $c|ca$ and $c|cb$. From (c) above we conclude that $c|(ca, cb)$, so $(ca, cb) = ck$ for some integer k. The GCD of two numbers divides each of them, so $(ck)|(ca)$ and $(ck)|(cb)$. Thus $k|a$ and $k|b$. From (c) it follows that $k|(a, b)$. Multiplying both sides by c, we see that $(ca, cb)|c(a, b)$.

4. Division with remainder and congruences (1)

Theorem 1.4.1 (Division with a remainder)**.** (a) For any a and $b \neq 0$ there exists q such that $q|b| \leq a < (q + 1)|b|$.

(b) For any a and $b \neq 0$ there exist unique q and r such that $a = bq + r$ and $0 \leq r < |b|$. The number q is said to be the *quotient* and the number r is said to be the *remainder* of division of a by b.

1.4.2. (a, b, c) Find the quotients and remainders for

(a) 1996 divided by -17;

(b) -17 divided by 4;

(c) $n^2 + n + 1$ divided by $n + 1$, for any n.

(d) Find all possible quotients and all possible remainders when dividing 57 by some number. (More precisely, assume that $57 = bq + r$ is division with remainder. Find the list of all possible q's and the list of all possible r's.)

Hint. There is a quicker way to do this than dividing 57 by $1, 2, 3, \ldots$, listing all resulting pairs (q, r), and removing identical entries.

1.4.3. Find
(a) the remainder upon dividing 3^{16} by 23;
(b) the last digit of the number $1997^{1997^{1997}}$.

To solve the problem above (among others), it's useful to be familiar with the following notion: The integers a and b are said to be *congruent* modulo $m \neq 0$ if $a - b$ is divisible by m (or, equivalently, if a and b have equal remainders upon division by m). This is denoted by $a \equiv b \pmod{m}$, or $a \equiv b \bmod m$, or $a \equiv b\ (m)$, or $a \underset{m}{\equiv} b$.

1.4.4. Properties of congruences: For any $a, b, m \neq 0$ the following statements are true:
(a) Transitivity: If $a \equiv b\ (m)$ and $b \equiv c\ (m)$, then $a \equiv c\ (m)$.
(b) Addition: If $a \equiv b\ (m)$ and $c \equiv d\ (m)$, then $a + c \equiv b + d\ (m)$.
(c) Multiplication: If $a \equiv b\ (m)$ and $c \equiv d\ (m)$, then $ac \equiv bd\ (m)$.
(d) Multiplication by an integer: If $a \equiv b\ (m)$, then $ac \equiv bc\ (mc)$ for any $c \neq 0$.
(e)* Division by an integer: If $ac \equiv bc\ (m)$ and $(m, c) = 1$, then $a \equiv b\ (m)$.

1.4.5. (a) Any number is congruent mod 9 and mod 3 to the sum of its digits.
(b) Formulate and prove similar rules of divisibility for 2, 4, and 11.

1.4.6. The sequence of remainders of a^n $(n = 0, 1, \ldots)$ upon division by $b \neq 0$ becomes periodic starting from some n.

Hints

1.4.1. (a) Use induction on a going "up" and "down." The base case when $0 \leq a \leq |b|$ is obvious. If $a \geq |b|$, then the inductive step reduces the assertion to the statement about $a - b$. If $a < 0$, then the next step reduces the assertion to the statement for $a + |b|$.
(b) This statement is equivalent to (a).

1.4.3. We have

$$3^{16} = (3^2)^8 = 9^8 = (9^2)^4 = 81^4 \equiv 12^4 = (12^2)^2 \equiv 6^2 \equiv 13 \bmod 23.$$

5. Linear Diophantine equations (2)

1.5.1. (a) A grasshopper moves along a line jumping 6 cm or 10 cm in either direction. What points can it get to?

(b) On the island of Utopia, each week consists of 7 days, and each month has 31 days. Sir Thomas Moore lived there for 365 days. Was one of the days necessarily Friday the 13th?

(c) Mike added together the day of his birth multiplied by 12 and the number of the month of his birth multiplied by 31 and got 670. What is his birthday? Find all possible solutions!

(d) Solve the equation $nx + (2n-1)y = 3$, where n is a given number (from here on we mean to find a solution in integers).

1.5.2. (a) One can make change for any amount of money greater than 23 yuan using just 5- and 7-yuan coins.

(b)* Find the smallest number m such that one can make change for any amount of money greater than m yuan using 12-, 21-, and 28-yuan coins.

1.5.3. A cue ball is launched from the corner of a billiard table at angle 45°. Will the ball hit the pin standing at the point $(2, 1)$, if the table is a rectangle with one of its vertices at the origin of the coordinate plane and another one at the point

(a) $(12, 18)$; (b) $(13, 18)$?

1.5.4. The equation $19x + 17y = 1$ has a solution in integers.

1.5.5. Let a and b be integers that are not both equal to 0 and let $c \in \mathbb{Z}$.

(a) **Theorem.** Let both a and b be nonzero. If a pair (x_0, y_0) is a solution of $ax + by = c$, then the set of all solutions of the equation is

$$\left\{ \left(x_0 + \frac{b}{(|a|,|b|)}t,\ y_0 - \frac{a}{(|a|,|b|)}t \right) \middle|\ t \in \mathbb{Z} \right\}.$$

(b) The equation $ax + by = c$ has a solution if and only if the equation $(a-b)u + bv = c$ has a solution.

(c) **Theorem.** The equation $ax + by = c$ has a solution if and only if c is divisible by (a, b).

(d) Construct an algorithm that either finds at least one solution of the equation $ax + by = c$ or reports that there are no solutions.

1.5.6. For any a and b not equal to 0 simultaneously, let $M = \{ax + by \mid x, y \in \mathbb{Z}\}$.

(a) Any element of M is divisible by the smallest positive element of M.

(b) The smallest positive element of M is equal to (a, b).

1.5.7. Let a and b be integers that are not both equal to 0 and let $c \in \mathbb{Z}$.

(a) **GCD representation lemma.** There exist x and y such that $ax + by = (a, b)$.

(b) **Lemma.** If $(b, c) = 1$ and $c|ab$, then $c|a$.

(c) **Euclid's lemma.** If p is a prime and $p|ab$, then $p|a$ or $p|b$.

(d) **Lemma.** If $(b, c) = 1$, $b|a$, and $c|a$, then $bc|a$.

1.5.8. (a) Find $(2^{91} - 1, 2^{63} - 1)$.

(b) Find $(2^{2^k} + 1, 2^{2^l} + 1)$.

(c) For which a, b, and n is $n^a + 1$ divisible by $n^b - 1$?

1.5.9. (a) For any a and $b \neq 0$ we have the equality $\gcd(a, b) = \gcd(b, r)$, where r is the remainder on division of a by b.

(b) For a pair of numbers $(a_0, b_0) \neq (0, 0)$, the *Euclidean algorithm* constructs the sequence of pairs (a_k, b_k) by the following rules:

- If $b_k = 0$, set $d := a_k$ and halt the algorithm.
- If $b_k \neq 0$, set $a_{k+1} := b_k$ and let b_{k+1} be equal to the remainder when a_k is divided by b_k.

Prove that for any pair of numbers $(a_0, b_0) \neq (0, 0)$, the Euclidian algorithm will come to an end and return $d = \gcd(a_0, b_0)$.

1.5.10. Solve the following systems of congruences:

(a) $\begin{cases} x \equiv -1 \ (7), \\ x \equiv 15 \ (5); \end{cases}$ (b) $\begin{cases} x \equiv 6 \ (12), \\ x \equiv 8 \ (20); \end{cases}$ (c) $\begin{cases} x \equiv 7 \ (8), \\ x \equiv 18 \ (25), \\ 6x \equiv 2 \ (7). \end{cases}$

(d) **The Chinese Remainder Theorem.** If nonzero integers $m_1, \ldots, m_s$ are pairwise relatively prime, then for any integers $a_1, \ldots, a_s$, there exists x such that $x \equiv a_i \ (m_i)$ for all $i = 1, \ldots, s$.

(e) Construct an algorithm for finding x.

Suggestions, solutions, and answers

1.5.1. (a) *Answer*: The grasshopper can get to all points whose distances from the starting point are even.

Solution. The grasshopper jumps even distances, so it can move away from the starting point only by an even distance. To show that it can get to the point located at a distance $2n$ to the right of the starting point, make $2n$ jumps by 6 to the right and n jumps by 10 to the left, since $6(2n) - 10n = 2n$. An analogous argument works for points located to the left of the starting point.

(b) Consider 7 consecutive months during which Sir Thomas Moore was on the island, numbered 1 to 7 in the same way as we number days of the

week. The number of days in a month has the remainder 3 upon division by 7. This means that if the 13th day of the ith month is the kth day of the week, then the 13th day of the $(i+1)$th month will be the $(k+3)$th day of the week modulo 7. Therefore, the days of the week of 13th days of the seven months are $k, k+3, k+6, k+2, k+5, k+1, k+4$ modulo 7. This contains all 7 days of the week among them. Thus, one of them will be Friday.

1.5.2. (a) If $24 \le n < 29$, we can make change for n yuan as follows:

$$24 = 2 \cdot 5 + 2 \cdot 7, \quad 25 = 5 \cdot 5, \quad 26 = 5 + 3 \cdot 7, \quad 27 = 4 \cdot 5 + 7, \quad 28 = 4 \cdot 7.$$

We will prove the problem's assertion by induction on n. We just proved it for $24 \le n < 29$. If $n \ge 29$, by the induction hypothesis, we can make change for $n-5$ yuan using 5- and 7-yuan coins.

1.5.5. (c) Assume that $a \ge b > 0$ and use induction on $a+b$.

1.5.7. (a) The statement follows from 1.5.5 (c), or from 1.5.6 (b) (or can be proved similarly).

(b) Use part (a).

(c) Use part (b).

Another hint. For fixed numbers p and $a \ge 0$, find the smallest positive number b satisfying the following conditions: $p|ab$ and b is not divisible by p. It's clear that if $p|ab$, then $p|a(b-p)$. Therefore the minimality of b implies that $b \le p$. Since $p|ab$, we have $ab \ge p$. Consider integers $b, 2b, \ldots, (a-1)b, ab$. Among them there is an integer i satisfying $(i-1)b < p \le ib$. If $p = ib$, then $b = 1$, so $p|ab$. Now let $p \le ib$. Note that $0 \le ib - p \le b$ and $p|a(ib-p)$. This contradicts the minimality of b.

1.5.8. (a) Prove that $(n^a - 1, n^b - 1) = n^{(a,b)} - 1$.

1.5.9. (b) If $b_k \ne 0$, then for any two consecutive steps, the largest numbers in a pair will decrease. So at some step the largest number in the pair will reach its minimal value and the algorithm will halt. Therefore at some step we will obtain the pair $(a_k, 0)$. Consequently, $a_k = \gcd(a_k, 0) = \gcd(a_0, b_0)$.

1.5.10. *Answers*: (a) $x \equiv 20\ (35)$; (b) $\emptyset$ (empty set); (c) $x \equiv 943\ (1400)$.

6. Canonical decomposition (2*)

The existence of prime factorization (problem 1.2.8 (a)) implies that for any number $n \ge 2$, there are distinct primes $p_1, \ldots, p_m$ and positive integers $\alpha_1, \ldots, \alpha_m$ such that $n = p_1^{\alpha_1} \cdot \ldots \cdot p_m^{\alpha_m}$. This representation is said to be the *canonical decomposition* of the number n. It is uniquely determined up to the order of the factors (problem 1.2.8 (d)).

1.6.1. Find the canonical decomposition of the following numbers:
(a) 1995; (b) 17!; (c) $\binom{22}{11}$.

1.6.2. (a) **Lemma.** The exponent of a prime p in the canonical decomposition of $n!$ is equal to $\sum\limits_{i=1}^{\infty}\left[\frac{n}{p^i}\right]$.
(b) $n!$ is not divisible by 2^n for any $n \geq 1$.
(c) How many zeros are there at the end of 1000!?

1.6.3. Let $n = p_1^{\alpha_1} \cdot \ldots \cdot p_n^{\alpha_n}$ be the canonical decomposition. Find
(a) the number $\alpha(n)$ of all positive divisors of the number n;
(b) the sum $s(n)$ of all positive divisors of the number n;
(c) $\sum\limits_{d|n} \alpha(d)$, where the sum is taken over all positive divisors of the number n.

1.6.4. (a) Suppose that $(a, b) = 15$ and $[a, b] = 840$. Find a and b.
(b) Prove that $(a, b) \cdot [a, b] = ab$.
(c) Express $[a, b, c]$ in terms of a, b, c, (a, b), (b, c), (c, a), and (a, b, c).
(d) Express (a, b, c) in terms of a, b, c, $[a, b]$, $[b, c]$, $[c, a]$, and $[a, b, c]$.
(e)* Find expressions similar to the ones above for n integers.

1.6.5. A positive number is said to be *perfect* if it is equal to the sum of all of its positive divisors other than itself. Prove that n is an even perfect number if and only if $n = 2^{p-1}(2^p - 1)$, where p and $2^p - 1$ are primes.

1.6.6. (a) If $(a, b) = 1$ and $ab = m^2$, then there exist k and l such that $a = k^2$ and $b = l^2$.
(b) Find $n > m > 100$ such that $1 + 2 + \ldots + n = m^2$.
(c) Find all $m > n > 1$ such that $1^2 + 2^2 + \ldots + n^2 = m^2$.
(d) If $n > 2$, $ab = c^n$, and $(a, b) = 1$, then $a = x^n$ and $b = y^n$ for some x and y.
(e) The integer $m(m + 1)$ is not a power of a prime number for any $m > 1$.

1.6.7. (a) If $ab = cd$, then there exist k, l, m, and n such that $a = kl$, $b = mn$, $c = km$, and $d = ln$.
(b) Find all integers a, b, c, d, k, and m such that $ab = cd$, $a + d = 2^k$, and $b + c = 2^m$.

1.6.8. Find the smallest integer n such that for any set of n numbers between 1 and 200, there are a and b in the set with $a|b$.

1.6.9. (a) Let p be a prime and let $n < p < 2n$. Then $\binom{2n}{n}$ is divisible by p.

(b) The following inequality holds: $2^{2p_{n+1}} > p_1 \cdot \ldots \cdot p_n$, where p_n is the nth prime.

(c) **Bertrand's postulate.** For any $n > 1$ there exists a prime between n and $2n$.

Suggestions, solutions, and answers

1.6.1. (a) We have $1995 = 5 \cdot 399 = 5 \cdot 3 \cdot 133 = 5 \cdot 3 \cdot 7 \cdot 19$ $(= 5 \cdot 7 \cdot 57)$.

(b) Calculate the exponent of 2 in the canonical decomposition of $17! = 1 \cdot 2 \cdot 3 \cdot \ldots \cdot 17$. Every second number in this product is divisible by 2, so we can factor out 2^8. Then, each fourth number is divisible by 4, providing an additional factor of 2^4. Similarly we find two more 2's in factors of 8 and one more 2 in factors of 16. Applying this to the other primes yields

$$17! = 2^{15} \cdot 3^{\left[\frac{17}{3}\right]+\left[\frac{17}{9}\right]} \cdot 5^{\left[\frac{17}{5}\right]} \cdot 7^{\left[\frac{17}{7}\right]} \cdot 11 \cdot 13 \cdot 17 = 2^{15} \cdot 3^6 \cdot 5^3 \cdot 7^2 \cdot 11 \cdot 13 \cdot 17.$$

(c) Similarly to part (b) we have

$$11! = 2^{\left[\frac{11}{2}\right]+\left[\frac{11}{4}\right]+\left[\frac{11}{8}\right]} \cdot 3^{\left[\frac{11}{3}\right]+\left[\frac{11}{9}\right]} \cdot 5^{\left[\frac{11}{5}\right]} \cdot 7 \cdot 11 \quad \text{and}$$

$$22! = 2^{\left[\frac{22}{2}\right]+\left[\frac{22}{4}\right]+\left[\frac{22}{8}\right]+\left[\frac{22}{16}\right]} \cdot 3^{\left[\frac{22}{3}\right]+\left[\frac{22}{9}\right]} \cdot 5^{\left[\frac{22}{5}\right]} \cdot 7^{\left[\frac{22}{7}\right]} \cdot 11^{\left[\frac{22}{11}\right]} \cdot 13 \cdot 17 \cdot 19.$$

Therefore

$$\binom{22}{11} = \frac{22!}{11! \cdot 11!} = 2^{19-16} \cdot 3^{9-8} \cdot 5^{4-4} \cdot 7^{3-2} \cdot 13 \cdot 17 \cdot 19 = 2^3 \cdot 3 \cdot 7 \cdot 13 \cdot 17 \cdot 19.$$

1.6.3. Solve this problem for a prime n, then for $n = p^\alpha$, then for $n = p_1 p_2$, and finally for the general case.

1.6.4. *Hint.* Use the inclusion-exclusion principle and canonical decomposition.

(c) *Answer*:

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

1.6.9. A proof can be found in [**Tik94**]. Most of the technical details there are not needed if we just want to prove Bertrand's postulate, rather than Chebyshev's theorem. See also [**AZ04**].

7. Integer points under a line (2*)

The problems in this section investigate the sum

$$f_\alpha(n) = \sum_{k=1}^{n} [\alpha k],$$

which gives the number of integer points with positive y-coordinate and x-coordinate between 1 and n that lie under the line $y = \alpha x$, where α is a positive real number. An algorithm for rational α is developed in problems 1.7.3 (a, b, c), while problems 1.7.1 and 1.7.2 are useful as warm-ups.

1.7.1. (a) Find $f_{\sqrt{2}}(4)$.

(b) Do there exist numbers $\alpha \neq \beta$ such that $f_\alpha(n) = f_\beta(n)$ for any n?

1.7.2. Find $f_\alpha(n)$

(a) if α is an integer; (b) if 2α is an integer; (c) if 3α is an integer;

(d) if $\alpha = u/n$ for given integers u and n.

(e) Prove that $\lim\limits_{n\to\infty} \frac{f_\alpha(n)}{n^2}$ exists, and find it. (See the definition of limits in problem 6.4.2; skip this problem if you are unfamiliar with this concept.)

1.7.3. (a) Prove the equality $f_\alpha(n) = f_{\{\alpha\}}(n) + \frac{1}{2}[\alpha]n(n+1)$ for arbitrary α and n.

(b) Prove the equality $f_\alpha(n) + f_{1/\alpha}([n\alpha]) - [n/q] = n[n\alpha]$, where q is the denominator of the irreducible fraction representing α if α is rational, and $q = \infty$ (i.e., $[n/q] = 0$) if α is irrational.

(c) Construct an algorithm for calculating $f_\alpha(n)$ for rational α, using (a) and (b).

(d) Find the complexity of that algorithm, that is, the number of operations of addition and multiplication in the algorithm, and compare it with the complexity of the straightforward calculation of $f_\alpha(n)$.

(e) Find an algorithm for calculating the sum $\sum\limits_{k=1}^{n} \{\alpha k\}$ for a rational α.

Remark 1.7.4. The special case of the equality in 1.7.3 (b) for odd positive relatively prime numbers $p < q$, $\alpha = p/q$, and $n = (q-1)/2$ (then $[n\alpha] = (p-1)/2$) appears in the proof of the quadratic reciprocity law (see the solution of problem 2.4.5 (d)). The proof in the general case is similar.

The sum from 1.7.3 (e) was calculated (in a more cumbersome way than proposed here) in [**Dob04**].

Suggestions, solutions, and answers

1.7.2. (a) We have $\sum\limits_{k=1}^{n} [\alpha k] = \alpha \sum\limits_{k=1}^{n} k = \alpha \cdot \frac{n(n+1)}{2}$.

(b) For integer α see (a). For half-integers ($\alpha = q/2$ where q is odd) we have

$$[\alpha] + [2\alpha] + [3\alpha] + \ldots + [n\alpha]$$
$$= \left(\alpha - \frac{1}{2}\right) + 2\alpha + \left(3\alpha - \frac{1}{2}\right) + \ldots = \alpha \cdot \frac{n(n+1)}{2} - \left[\frac{n+1}{2}\right].$$

There are other ways to write this sum, for example

$$[\alpha]\frac{n(n+1)}{2}+\{\alpha\}\frac{n^2+(-1)^n}{2}.$$

(c) For integer α see (a). If α is not an integer we have

$$f_\alpha(n)=\begin{cases}\alpha\cdot\frac{n(n+1)}{2}-\left[\frac{n+1}{3}\right], & n\neq 3k+1;\\ \alpha\cdot\frac{n(n+1)}{2}-\left[\frac{n}{3}\right]-\{\alpha\}, & n=3k+1.\end{cases}$$

Hint. If α is not an integer, we have

$$[\alpha]+[2\alpha]+[3\alpha]=\alpha+2\alpha+3\alpha-\frac{1}{3}-\frac{2}{3}=(1+2+3)\alpha-1.$$

Solutions to (a), (b), (c), and (d) can be obtained using Pick's formula. See [**Sop**].

(e) *Answer*: $\alpha/2$.

1.7.3. (a) We have

$$\begin{aligned}f_\alpha(n)&=\sum_{k=1}^{n}[\alpha k]=\sum_{k=1}^{n}[([\alpha]+\{\alpha\})\cdot k]=\sum_{k=1}^{n}[[\alpha]k+\{\alpha\}k]\\&=\sum_{k=1}^{n}([\alpha]k+[\{\alpha\}k])=\sum_{k=1}^{n}[\alpha]k+\sum_{k=1}^{n}[\{\alpha\}k]\\&=[\alpha]\sum_{k=1}^{n}k+f_{\{\alpha\}}(n)=[\alpha]\frac{n(n+1)}{2}+f_{\{\alpha\}}(n).\end{aligned}$$

(b) Calculate the number of integer points in the rectangular region $1\le x\le n$, $1\le y\le[n\alpha]$. The details are similar to the solution of problem 2.4.5 (d).

(c) For example,

$$\begin{aligned}&f_{2/3}(n)=n\Big[\frac{2n}{3}\Big]+\Big[\frac{n}{3}\Big]-f_{3/2}\Big(\Big[\frac{2n}{3}\Big]\Big);\\&f_{3/2}\Big(\Big[\frac{2n}{3}\Big]\Big)=\frac{1}{2}\Big[\frac{2n}{3}\Big]\Big(\Big[\frac{2n}{3}\Big]+1\Big)+f_{1/2}\Big(\Big[\frac{2n}{3}\Big]\Big);\\&f_{1/2}\Big(\Big[\frac{2n}{3}\Big]\Big)=\Big[\frac{2n}{3}\Big]\Big[\frac{n}{3}\Big]+\Big[\frac{n}{3}\Big]-f_2\Big(\Big[\frac{n}{3}\Big]\Big),\end{aligned}$$

since $[[x]/n]=[x/n]$ for an integer $n>0$ and so $\left[\frac{\left[\frac{2n}{3}\right]}{2}\right]=\left[\frac{n}{3}\right]$;

$$f_2\Big(\Big[\frac{n}{3}\Big]\Big)=\Big[\frac{n}{3}\Big]\Big(\Big[\frac{n}{3}\Big]+1\Big).$$