TOPICS IN NUMBER THEORY

Valentin Goranko

Topics in Number Theory

This essay is an introduction to some basic topics in number theory related to *divisibility, prime numbers* and *congruences*. These topics are sources of numerous elementary (but often far from simple) problems which traditionally appear in all advanced mathematical competitions, in particular the International Mathematical Olympiad.

The articles is divided into 8 chapters each presenting a minimum of necessary background, i.e. basic definitions, facts and theorems which can themselves be regarded as interesting problems. Every chapter ends with a number of problems ranging from elementary to quite advanced ones, many of which have been given at various competitions and Olympiads. Hints and solutions to these problems are given at the end of the article and a number of additional problems are included.

No special knowledge outside school curriculum is required as a prerequisite to this article, but a good deal of mathematical inclination and persistence are necessary for successful work with it. The reward of the work done will be twofold: intellectual — the feeling of a contact with a beautiful piece of mathematics, and practical — the confidence to know how to approach and cope with a large variety of problems in number theory. Of course, due to limitations of space, some interesting related topics traditionally covered by mathematical competitions are left untouched in this essay, perhaps the most important being *Diophantine equations* which will be the topic of another essay.

Here is the content of the article:

Introduction: induction

Number theory is one of the most important and oldest branches of mathematics and is concerned with the properties of the *natural numbers*, or *positive integers* $1, 2, 3, 4, \ldots$. (Sometimes 0 is also regarded as a natural number, but we shall keep it apart.) We shall denote the set of natural numbers by $\mathbb{N}$.

A fundamental property of the set of natural numbers, which we take for granted, is the following:

Every non-empty collection of natural numbers has a least element.

The most common method for proving facts about natural numbers is the *principle of mathematical induction*, a popular form of which is:

If
some assertion P about natural numbers holds for 1
and
whenever P holds for some natural number n, then P holds for $n+1$ too,
then
P holds for every natural number.

Indeed, *assume* that there are natural numbers for which P does not hold. The collection of such numbers has a least element m. It must be greater than 1 since P holds for 1. Therefore $m-1$ is a number less than m, hence P holds for $m-1$. But then P must hold for m, since $m=(m-1)+1$, which is not the case. Thus we have fallen into an absurd situation: the statement "P holds for M" is both false and true. The only way to escape from this absurd is to agree that *our assumption was wrong*. Thus, there are no natural numbers for which P does not hold, that it, P holds for all natural number.

The trick used in the above argument is called *proof by contradiction*. It is a very useful and powerful method for (not only) mathematical reasoning and will be often applied further.

As a typical application of the principle of mathematical induction we shall prove the following fact:

For every natural number n,

$$1+2+\cdots+n=\frac{n(n+1)}{2}. \tag{1}$$

First we verify (1) for $n=1$: $1=\frac{1(1+1)}{2}$.
Then we have to show that whenever P holds for some natural number n, P holds for $n+1$, too. In order to show this we *assume* that (1) holds for some natural number n. This assumption is called the *inductive hypothesis*. Now, using this assumption, we have to show that (1) holds for $n+1$. Here it goes:

$$\begin{aligned} 1+2+\cdots+(n+1) &= (1+2+\cdots+n)+(n+1) \\ &= \frac{n(n+1)}{2}+(n+1) \\ &= \frac{n(n+1)+2(n+1)}{2} \\ &= \frac{(n+1)(n+2)}{2}. \end{aligned}$$

Thus we have shown that the conditions of the principle of induction hold for (1) and therefore, (1) holds for every natural number n.

A seemingly stronger but in fact equivalent form of the principle of mathematical induction reads:

If
for every natural number n, the assumption that an assertion P holds for every natural number $m<n$ leads to the conclusion that P holds for n itself,
then
P holds for every natural number n.

Exercise. Prove this principle, using a similar argument to the previous one.

1 Divisibility: basic properties. Division with a remainder

When we deal with divisibility of numbers it is convenient to consider not only the natural numbers, but all *integers*

$$\ldots,-2,-1,0,1,2,\ldots.$$

Here is the basic definition: *A non-zero integer a divides an integer b if there is an integer x such that*

$$b=ax.$$

If a divides b we write $a \mid b$ and also say that b *is divisible by* a, or a is a *divisor of* b, or b is a *multiple of* a.

Is a does not divide b we write $a \nmid b$.
For instance $3 \mid 15$ and $-3 \mid 15$, but $3 \nmid 16$, $-3 \nmid 16$ and $4 \nmid 15$.
Hereafter, whenever we write $a \mid b$, a is assumed non-zero.

Here are some basic properties of divisibility:

(D1) $1 \mid b$ for any integer b;

(D2) $a \mid 0$ and $a \mid a$ for any non-zero integer a;

(D3) If $a \mid b$, then $-a \mid b$ and $a \mid -b$;

(D4) If $a \mid b$ then $a \mid bc$ for any integer c;

(D5) If $a \mid b$ and $b \mid c$, then $a \mid c$;

(D6) If $a \mid b$ and $a \mid c$, then $a \mid (mb + nc)$ for any integers m and n. In particular, $a \mid b - c$ and $a \mid b + c$;

(D7) If $a \mid b$ and $b \mid a$, then $a = b$ or $a = -b$. In particular, if a and b are natural numbers, then $a = b$;

(D8) If $a \mid b$ and $a, b > 0$, then $a \leq b$;

(D9) If m is a non-zero integer then $a \mid b$ if and only if $ma \mid mb$;

(D10) If $a \mid b$ and $c \mid d$, then $ac \mid bd$.

All of these properties are immediate consequences of the definition. Let us show for instance (D6). Let $a \mid b$ and $a \mid c$. Then $b = xa$ for some integer x and $c = ya$ for some integer y. Then $mb + nc = mxa + nya = (mx + ny)a$, hence $a \mid (mb + nc)$.

A frequently used fact, which follows from (D6) is that if $a \mid b$ and $a \mid b + c$, then $a \mid c$ since $c = (b + c) - b$; and likewise, if $a \mid b$ and $a \mid b - c$, then $a \mid c$ since $c = b - (b - c)$.

Exercise. Verify all other properties listed above.

The following is a fundamental theorem about division of integers.

Theorem 1.1. *Given any integers $a > 0$ and b, there exist unique integers q and r such that*

$$b = qa + r \quad \textit{and} \quad 0 \leq r < a.$$

Furthermore, $r = 0$ if and only if $a \mid b$.

Proof. If $b = 0$, then $b = 0 \cdot a + b$ and $b < a$. Suppose that $b \neq 0$. Consider the arithmetic sequence $\ldots, b - 2a, b - a, b, b + a, b + 2a, \ldots$. Notice that 0 belongs to this sequence if and only if $b = qa$ for some integer q, i.e. if and only if $a \mid b$. Now, suppose that $a \nmid b$, hence no term of the sequence is zero. There are positive terms in the sequence (show this!); let $r = b - qa$ be the least of them. It exists due to the fundamental property of the natural numbers, discussed in the introduction. We claim that $r < a$. Indeed, if $r \geq a$, then $r - a \geq 0$ and $r - a = (b - qa) - a = b - (q + 1)a$, so $r - a$ belongs to the sequence too. Furthermore, $r - a$ is less than r, which contradicts the choice of r. Thus $0 < r < a$, so we have proved the existence of r and q with the desired properties. Now let us show that they are unique. Suppose that there are two pairs (q_1, r_1) and (q_2, r_2) satisfying the conditions of the theorem and assume $r_1 \geq r_2$. Then $r_2 - r_1 = (b - q_1 a) - (b - q_2 a) = (q_2 - q_1)a$. On the other hand $0 \leq r_1 - r_2 < a$, which leaves the only possibility for $q_2 - q_1$ to be 0, i.e. $q_1 = q_2$ from where $r_1 = r_2$.

Finally, if $r = 0$ then $a \mid b$ by definition. Conversely, if $a \mid b$ then $a = kb + 0$ for some integer k. Then, by uniqueness of q and r, q must equal k and r must be 0. □

The numbers q and r from the above theorem are called, respectively, the *quotient* and the *remainder* of the division of b by a. Thus, the theorem says that every integer b can be divided with remainder by any natural number a in a unique way.

Problems

1.1. Show that every non-zero integer a has only finitely many divisors.

1.2. How many integers between 100 and 100 are divisible by 11?

1.3. Prove that for any integer n the remainder of the division of n^2 by 4 is either 0 or 1.

1.4. A right-angled triangle has sides with integer lengths. Show that

(a) the length of one of the two shorter sides of the triangle is divisible by 3;

(b) the length of one of the sides of the triangle is divisible by 5.

1.5. Show that for any natural number n represented in decimal system, n is divisible by

(a) 2 if and only if its last digit is divisible by 2;

(b) 4 if and only if the number formed by its last two digits is divisible by 4;

(c) 5 if and only if its last digit is divisible by 5.

1.6. Prove that for every natural number n

(a) if n is odd then $8 \mid n^2 - 1$;

(b) $8 \mid 3^{2n} - 1$;

(c) $9 \mid 4^n + 15n - 1$.

1.7. Show that for any natural numbers n and m the following sums are not integers.

(a) $N_1 = \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n}$;

(b) $N_2 = \frac{1}{n} + \frac{1}{n+1} + \cdots + \frac{1}{n+m}$;

(c) $N_3 = \frac{1}{3} + \frac{1}{5} + \cdots + \frac{1}{2n+1}$.

1.8. Prove that if $m \mid ab^n + cn + d$ for every integer $n \geq 0$, then $m \mid c^2$.

1.9. If m is a natural number greater than 1, show that every natural number N, can be uniquely represented in the form

$$N = c_0 + c_1 m + c_2 m^2 + \cdots + c_k m^k,$$

(when $k = 0$, $N = c_0$) where the coefficients c_i are integers satisfying the conditions $0 \leq c_i < m$ $(i = 0, 1, \ldots, k-1)$, $0 < c_k < m$.

This statement means that every natural number can be uniquely represented in a number system with base m for every natural number $m > 1$.

2 Greatest common divisor

An integer d is a *common divisor* of the integers a and b if $d \mid a$ and $d \mid b$. The greatest integer amongst the common divisors of a and b (if it exists) is called the *greatest common divisor* of a and b, denoted $\gcd(a, b)$ or simply (a, b).

Note that (a, b) is always positive: if c is a common divisor of a and b and c is negative, then $-c$ is also a common divisor of a and b, and is greater than c.

Now we shall derive the most important facts about the greatest common divisor.

Theorem 2.1. *If a and b are integers, at least one of them non-zero, then*

(i) *(a, b) exists;*

(ii) *$(a, b) = ua + vb$ for some integers u and v. Moreover, (a, b) is the least positive integer which can be represented in this way.*

Proof. (i) It follows from exercise 1.1 that, unless $a = b = 0$, a and b have finitely many common divisors, hence there is a greatest among them.

(ii) Consider the set L of all *linear combinations* $xa + yb$ where x and y range over all integers. There are positive values in L (why?). Let $d = ua + vb$ be the least positive integer in L. (Here we apply again the fundamental property of the natural numbers.) We shall show that $d \mid a$ and $d \mid b$.

Suppose $d \nmid a$. Then, by Theorem 1.1, there are integers q and r such that $a = dq + r$ and $0 < r < d$. Hence we have

$$r = a - qd = a - q(ua + vb) = (1 - qu)a + (qv)b$$

and thus r belongs to L, which is impossible since r is a positive integer less than d. Therefore $d \mid a$. Likewise $d \mid b$. Thus d is a common divisor of a and b. Let $g = (a, b)$. Then $a = ga'$ and $b = gb'$, hence $d = (ga')u + (gb')v = g(a'u + b'v)$. Thus $g \mid d$, hence $g \leq d$ by (D8), and $d \leq g$ by definition of g. Therefore $g = d$.

□

Theorem 2.2. *If the integers a and b have a greatest common divisor (a, b) then every common divisor of a and b divides (a, b).*

Proof. By Theorem 2.1, $(a, b) = ua+vb$ for some integers u and v. Now, if $d \mid a$ and $d \mid b$, then $d \mid ua+vb$, by property (D6). □

Here are some basic properties of the greatest common divisor.

(GCD1) $(a, b) = (b, a)$;

(GCD2) If $a \mid b$ then $(a, b) = |a|$;

(GCD3) If $a = 0$ and $b \neq 0$, then $(a, b) = |b|$;

(GCD4) $(a, b) = (a, -b) = (-a, b) = (-a, -b)$;

(GCD5) For any integer c, $(a, b) = (a, b + ac) = (a + bc, b)$;

(GCD6) For any integer m, $(ma, mb) = |m|\,(a, b)$;

(GCD7) If $d \mid a$ and $d \mid b$ then $\left(\frac{a}{d}, \frac{b}{d}\right) = \frac{(a,b)}{d}$. In particular, if $d = (a, b)$, then $\left(\frac{a}{d}, \frac{b}{d}\right) = 1$;

(GCD8) $((a, b), c) = (a, (b, c))$ for any integers a, b, c.

We shall verify (GCD5), (GCD6) and (GCD7); the rest are left as exercises.

(GCD5) Let $g = (a, b)$, $h = (a, b + ac)$. Then $g \mid b + ac$ by (D6), hence $g \mid h$ by Theorem 2.2. On the other hand, for some integers u and v, $g = au + bv = a((u - cv) + (b + ac)v)$. Thus $h \mid g$ by (D6). Therefore $g = h$ by (D6) since g and h are both positive. Likewise $(a, b) = (a + bc, b)$.

(GCD6) We can assume that $m > 0$, otherwise we take $-m$ and apply (GCD4). Now, (ma, mb) = the least positive value of $max + mby$ where x and y are integers = m times the least positive value of $ax + by$ where x and y are integers = $m(a, b)$.

(GCD7) Again we can assume that $d > 0$. Let $g = \left(\frac{a}{d}, \frac{b}{d}\right)$ and $h = (a, b)$. Then $a = da'$, $b = db'$ and, by (GCD6), $h = d(a', b') = dg$, hence $g = \frac{h}{d}$.

The definition of greatest common divisor is easily generalized to several integers. We denote the greatest common divisor of the integers $a_1, \ldots, a_k$ by $(a_1, \ldots, a_k)$.

Exercise. Show that $(a_1, a_2, a_3) = (a_1, (a_2, a_3))$, $\ldots$, $(a_1, a_2, \ldots, a_k) = (a_1, (a_2, \ldots, a_k))$. Furthermore, show that if $b_1, b_2, \ldots, b_k$ is a rearrangement of $a_1, a_2, \ldots, a_k$, then $(b_1, b_2, \ldots, b_k) = (a_1, a_2, \ldots, a_k)$. Hint: use properties (GCD1) and (GCD8).

It is not difficult to see that Theorem 2.1 and Theorem 2.2 can be generalized for greatest common divisors of several integers:

(1) If $a_1, a_2, \ldots, a_k$ are not all zero then $(a_1, a_2, \ldots, a_k)$ exists and equals the least positive integer which can be represented as a linear combination of $a_1, a_2, \ldots, a_k$: $(a_1, a_2, \ldots, a_k) = u_1a_1 + u_2a_2 + \cdots + u_ka_k$ for some integers $u_1, u_2, \ldots, u_k$.

(2) Every common divisor of $a_1, a_2, \ldots, a_k$ divides $(a_1, a_2, \ldots, a_k)$.

Exercise. Prove these statements for three integers.

Now we know many properties of the greatest common divisor of two integers, but still the main question remains: *how to compute it?* Due to properties (GCD1), (GCD3) and (GCD4) we see that it is sufficient to ba able to compute the greatest common divisor of *natural numbers*; then we can do so for any integers. For instance $(123, -321) = (123, 321)$.

Theorem 2.3. *Let a and b be natural numbers. The following procedure computes the greatest common divisor of a and b.*

1. *Denote by X the greater of a and b, and by Y the smaller one; if $a = b$ then $X = Y = a$.*
2. *Divide X by Y with a remainder: $X = QY + R$, where $0 \leq R \leq Y$.*
3. *If $R = 0$, then $(a, b) = Y$ and the procedure ends. If not, continue with 4.*
4. *If $R > 0$ replace X by Y and then Y by R, and go back to step 2.*

This simple and elegant procedure was invented by Euclid, the celebrated mathematician of ancient Greece who laid the sound foundations not only of the geometry, but of number theory as well. This procedure was perhaps one of the first and most famous instances of what is nowadays called the *algorithm*.

Before we show *why* this algorithm works, let us see *how* it works on a particular example.

Example. Find $(30, 102)$ using the Euclidean algorithm. We follow the procedure:

1. Set X to be 102 and Y to be 30.
2. Divide X by Y with a remainder: $102 = 3 \cdot 30 + 12$.
3. The remainder is not 0, hence continue with 4.
4. X becomes 30 and Y becomes 12; the go back to 2.
2. Divide X by Y with a remainder: $30 = 2 \cdot 12 + 6$.
3. The remainder is not 0, hence continue with 4.
4. X becomes 12 and Y becomes 6; then go back to 2.
2. Divide X by Y with a remainder:
3. The remainder is 0, hence $(30, 102) = Y = 6$.

- End of procedure.

Now let us prove that the Euclidean algorithm works. We must check two things:

1. That, for any two natural numbers, if the procedure ends the result is indeed their greatest common divisor.
2. That for any two natural numbers the procedure ends.

To say it in terms of computer science, we must verify the *correctness* of the algorithm. Here it is:

1. Let us first observe that at any stage of the execution of the algorithm, (X, Y) remains equal to (a, b). (As a computer scientist would say, (X, Y) is an *invariant* of the algorithm.) At the beginning this is trivially so. The only changes of the values of X and Y occur at point 4. There the pair (X, Y) is replaced by Y, R, where $R = X - QY$ is the remainder of the division of X by Y. Hence we only have to check that

$$(X, Y) = (Y, X - QY)$$

which easily follows from (GCD5) and (GCD1).

Thus (X, Y) is always equal to (a, b). It remains to show that whenever the procedure ends, the result is what we need. The procedure ends only if the remainder R becomes 0, that is, the values of X and Y become such that $Y \mid X$. Then the result is Y, which is indeed (X, Y), due to (GCD2).

The first task is completed.

2. Suppose that for some natural numbers a, b the procedure never ends. This can only happen if the point 4 (the only one which sends the execution back) is executed infinitely many times. Let us notice two things:

   - each time when point 4 is executed, the value of X *strictly diminishes*, being replaced by Y (for, $X \geq Y$ and if $X = Y$, then R would be 0).
   - the values of X and Y always remain natural numbers.

   Thus, the consecutive values of X form an infinite strictly decreasing sequence of natural numbers. Due to the fundamental property of the natural numbers, this is impossible because the collection of the terms of such a sequence has no least element.

   Therefore the procedure must terminate.

   In the long run, we have established the correctness of Euclid's algorithm. □

Exercise. Using the Euclidean algorithm, find:

(a)$(70, 112)$ (b)$(258, 801)$ (c)$(7469, 2464)$ (d)$(2689, 4001)$.

Problems

2.1. Given that $(a, 4) = 2$ and $(b, 4) = 2$, show that $(a + b, 4) = 4$.

2.2. Let x and y be integers such that $x + y = 1000$. Is it possible that $(x, y) = 3$?

2.3. Prove that for any integers a and b, $(a, b) = (3a + 5b, 11a + 18b)$.

2.4. Prove that the fraction $\frac{21n+4}{14n+3}$ is irreducible for any natural n.
This was Problem 1 from the First International Mathematical Olympiad (IMO) in Romania, 1959.

2.5. Let a, b, c, A, B, C be integers such that $(a, b) = c$ and $(A, B) = C$. Show that $(aA, aB, Ab, AB) = cC$.

2.6. Let k be any natural number and $a_n = k^{2^n} + 1$. Show that if $m \neq n$, then $(a_m, a_n) = 1$ if k is even, otherwise $(a_m, a_n) = 2$.

2.7. Let $a > 1$ and m be natural numbers. Show that

$$\left(\frac{a^m - 1}{a - 1}, a - 1\right) = (a - 1, m).$$

2.8. If a, m, n are natural numbers, $a > 1$ and $(m, n) = d$, show that

$$(a^m - 1, a^n - 1) = a^d - 1.$$

3 Relatively prime numbers

Natural numbers a and b are called *relatively prime* if

$$(a, b) = 1.$$

Example. 8 and 15 are relatively prime, 8 and 14 are not.

The following theorem will summarize those properties of relatively prime numbers which will be used further on.

Theorem 3.1. *For all integers a, b and c:*

(1) *If $c \mid ab$ and $(c, a) = 1$, then $c \mid b$.*

(2) *If $(a, b) = 1$, then $(a, bc) = (a, c)$.*

(3) *$(a, bc) = 1$ if and only if $(a, b) = 1$ and $(a, c) = 1$.*

(4) *If $(a, b) = 1$, then $ab \mid c$ if and only if $a \mid c$ and $b \mid c$.*

Proof. (1) Assume that $c \mid ab$ and $(c, a) = 1$. Then $ab = kc$ for some integer k and $1 = uc + va$ for some integers u and v. Multiplying the latter equality by b we get $b = ubc + vab = ubc + vkc = (ub + vk)c$, hence $c \mid b$.

(2) Let $(a, b) = 1$, $(a, bc) = d_1$ and $(a, c) = d_2$. Then obviously $d_2 \mid d_1$. Conversely, d_1 must be relatively prime to b because $d_1 \mid a$. Hence by (1), $d_1 \mid c$ since $d_1 \mid bc$. Thus $d_1 \mid d_2$ and therefore $d_1 = d_2$.

(3) If $(a, bc) = 1$ then $(a, b) = 1$ and $(a, c) = 1$ since every divisor of (a, b) or (a, c) is a divisor of (a, bc). Conversely, if $(a, b) = 1$ and $(a, c) = 1$ then by (2), $(a, bc) = (a, c) = 1$.

(4) If $ab \mid c$ then $a \mid c$ and $b \mid c$. Now, let $(a, b) = 1$ and suppose that $a \mid c$ and $b \mid c$. Then $c = ak$ for some integer k and $b \mid ak$. Therefore, by (1), $b \mid k$ hence $ab \mid ak$, i.e. $ab \mid c$.

□

Natural numbers $a_1, \ldots, a_n$ are said to be:

(i) *relatively prime* if $(a_1, \ldots, a_n) = 1$;

(ii) *relatively prime in pairs* if every two of them are relatively prime.

Obviously, if the integers $a_1, \ldots, a_n$ are relatively prime in pairs, then they are relatively prime. The converse is not generally true (see Problem 3.1).

Problems

3.1. (a) Find three integers which are relatively rime but no two of them are relatively prime.
(b) Find four integers which are relatively prime but no three of them are relatively prime.
(c) Find four integers such that every three but no two of them are relatively prime.

3.2. Show that amongst any 5 consecutive integers there is at least one which is relatively prime to each of the others.

3.3. Show that the product of every
(a) 3 consecutive integers is divisible by 6;
(b) 4 consecutive integers is divisible by 24;
(c) 5 consecutive integers is divisible by 120.

3.4. Prove that for every integer n
(a) $6 \mid n^3 - n$;
(b) $30 \mid n^5 - n$;
(c) $120 \mid n^5 - 5n^3 + 4n$.

3.5. Show that the sequence $\{2^n - 3 | n = 2, 3, 4, \ldots\}$ contains infinitely many numbers relatively prime in pairs.

This was Problem 3 from the 13th IMO in Czechoslovakia, 1971.

3.6. A sequence of natural numbers is defined by the equalities $t_1 = 2$ and $t_{n+1} = t_n^2 - t_n + 1$ for $n \geq 0$. Show that if $m \neq n$, then $(t_m, t_n) = 1$.

4 Least common multiple

An integer m is a *common multiple* of the non-zero integers a and b if $a \mid m$ and $b \mid m$. The least positive number amongst the common multiples of a and b, if it exists, is called the *least common multiple* of a and b, denoted $[a, b]$.

Let us observe that if a and b are non-zero, then $[a, b]$ always exists. Indeed, the collection of positive common multiples of a and b is non-empty, since $|ab|$ belongs to it. Therefore, by the fundamental property of the natural numbers, there is a least number in that collection.

Here are some basic properties of least common multiples.

(LCM1) $[a, b] = [b, a]$.

(LCM2) if $a \mid b$ then $[a, b] = |b|$.

(LCM3) $[a, b] = [a, -b] = [-a, b] = [-a, -b]$.

(LCM4) $[na, nb] = n[a, b]$.

(LCM5) $[[a, b], c] = [a, [b, c]]$.

Exercise. Verify these properties.

We can likewise introduce a least common multiple of several integers $a_1, a_2, \ldots, a_k$. It is denoted by $[a_1, a_2, \ldots, a_k]$.

Exercise. Show that $[a_1, a_2, a_3] = [a_1, [a_2, a_3]], \ldots, [a_1, a_2, \ldots, a_k] = [a_1, [a_2, \ldots, a_k]]$.

Theorem 4.1. *The least common multiple of the non-zero integers $a_1, a_2, \ldots, a_k$ is a divisor of every one of their common multiples.*

Proof. Let $m = [a_1, a_2, \ldots, a_k]$ and n be a common multiple of $a_1, a_2, \ldots, a_k$. Let us divide n by m with remainder: $n = mq + r$, $0 \leq r < m$. Then $r = n - mq = 1 \cdot n + (-q) \cdot m$. Hence, by (D5), r must be a common multiple of $a_1, a_2, \ldots, a_k$, less than m. Therefore $r = 0$, hence $m \mid n$. □

Theorem 4.2. *For every natural numbers a and b,*

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

Proof. Let $g = (a, b)$, $m = [a, b]$ and $d = \frac{ab}{m}$. Then $a = \frac{m}{b}d$ and $b = \frac{m}{a}d$ where $\frac{m}{b}$ and $\frac{m}{a}$ are integers. Therefore d is a common divisor of a and b. By Theorem 2.2, $d \mid g$, i.e. $g = dk$ for some positive integer k. Then $\frac{m}{k}$ is a positive common multiple of a and b: $\frac{m}{k} = \frac{a}{g}b = \frac{b}{g}a$, where $\frac{a}{g}$ and $\frac{b}{g}$ are integers. Since m is the least positive common multiple of a and b, it follows that $m \leq \frac{m}{k}$ which is possible only if $k = 1$. Thus $g = d$, as was to be proved. □

Exercise. Find the least common multiple of

(a)6 and 8(b)28 and 42(c)70 and 71(d)482 and 1687.

Problems

4.1. Let n be a natural number. Find $[n, n + 1]$.

4.2. Let m and n be natural numbers such that $(m, n) = [m, n]$. Show that $m = n$.

4.3. Find all pairs of natural numbers m, n for which $(m, n) = 10$ and $[m, n] = 100$.

4.4. Prove that for any natural number n,

$$[1, 2, 3, \ldots, 2n] = [n + 1, n + 2, \ldots, 2n].$$

4.5. Prove that for any natural numbers m and n,

$$[1, 2, \ldots, m, n, n + 1, \ldots, n + m - 1] = [n, n + 1, \ldots, n + m - 1].$$

5 Prime numbers. The fundamental theorem of arithmetic

A natural number $p > 1$ is called *prime* (or a *prime number*) if it has exactly two natural divisors: 1 and p (called *trivial* divisors of p). Otherwise p is called a *composite number*.

Exercise. 2, 3, 5, 27, 101, 1993 are primes; 4, 189, 1001 are composite (show this); 1 is neither prime nor composite (by definition).

Theorem 5.1. *Every natural number greater than 1 has a prime divisor.*

Proof. Assume the contrary: there are natural numbers greater than 1, without any prime divisors. Let m be the least of them. Since $m \mid m$, m cannot be prime, hence it is composite, i.e. has a positive divisor n, different from 1 and from m. Then $1 < n < m$, hence n must have a prime divisor p. Thus $p \mid n$ and $n \mid m$, hence $p \mid m$ which is a contradiction. Therefore there is no such m. □

Remark. In fact, every composite number n has a prime divisor not greater than $\sqrt{n}$. Indeed, let $n = n_1 n_2$. Then at least one of n_1 and n_2, assume n_1, is not greater than $\sqrt{n}$. Now, n_1 has a prime divisor which is of course not greater than n_1 and is a divisor of n also.

Theorem 5.2 (Euclid, about 2350 years ago)**.** *There are infinitely many primes.*

Proof. Assume the contrary: there are finitely many primes and let $p_1, p_2, \ldots, p_k$ be all of them. Now consider the number

$$N = p_1 p_2 \cdots p_k + 1.$$

Since N is greater than each of $p_1, p_2, \ldots, p_k$ it must be composite. By the previous Theorem, N has a prime divisor p which must be some of $p_1, p_2, \ldots, p_k$, for instance $p = p_1$. Then $p_1 \mid N$ and $p_1 \mid p_1 p_2 \cdots p_k$ since p_1 occurs as a factor in $p_1 p_2 \cdots p_k$. Hence, by (D6), $p_1 \mid N - p_1 p_2 \cdots p_k$, i.e. $p_1 \mid 1$ which is impossible since every prime is greater than 1. Therefore we must conclude that there are infinitely many primes. □

Theorem 5.3. *(1) For every natural number a and a prime p, either $p \mid a$ or $(p, a) = 1$.*

(2) For very natural numbers a and b and a prime p, if $p \mid ab$ then p divides at least one of a and b.

Proof. (1) (p, a) can only be either p or 1.

(2) If $p \nmid a$ then $(p, a) = 1$ hence, by Theorem 3.1 (1), p divides b.

□

Theorem 5.3 can easily be generalized by induction to

For all natural numbers $a_1, \ldots, a_k$ and a prime p, if $p \mid a_1 a \cdots a_k$ then p divides at least one of $a_1, \ldots, a_k$.

The notion of prime number is basic in number theory. As we shall see from the next theorem the prime numbers are like "elementary particles" from which all natural numbers are built.

Theorem 5.4 (Fundamental theorem of arithmetic)**.** *Every natural number $n > 1$ can be decomposed into a product of primes:*

$$n = p_1 \cdots p_k \quad (k \geq 1).$$

Moreover, this decomposition is unique up to the order of the factors.

Proof. We can reformulate the theorem as follows: for every natural number n, if $n > 1$ then n can be decomposed.... Now we can apply the principle of mathematical induction. Assume that the theorem is valid for all natural numbers m such that $m < n$. We must conclude that it is valid for n too. If $n = 1$, nothing is claimed so that this case is trivially true. Now, let $n > 1$. Then n has prime divisors, by Theorem 5.1. Let p_1 be the least of them. Then $n = p_1 n_1$ and $n_1 < n$. If $n_1 = 1$ then $n = p_1$ is prime and this is the decomposition of n; it is unique since p_1 cannot be expressed as a product of two or more primes. Now, if $1 < n_1$ then, according to the inductive assumption, n_1 is decomposed into a product of primes: $n_1 = p_2 \cdots p_k$. Then we have a decomposition of n: $n = p_1 \mathfrak{p}_2 \cdots p_k$.

Suppose that besides this decomposition of n there is another one $q_1 \cdots q_m$. Then

$$p_1 \cdots p_k = q_1 \cdots q_m.$$

Thus $p_1 \mid q_1 \cdots q_m$, hence p_1 divides some of the factors $q_1, \ldots, q_m$. We may assume (possibly after reordering) that $p_1 \mid q_1$. This means that $p_1 = q_1$ since q_1 is prime. Then we obtain

$$p_2 \cdots p_k = q_2 \cdots q_m.$$

Again, the inductive assumption holds for $p_2 \cdots p_k$, so $q_2, \cdots q_m$ must be a reordering of $p_2, \ldots, p_k$. Thus, the theorem is valid for n.

Now we can conclude that the theorem is true for any natural number. □

The above theorem can also be reformulated as follows:
Every natural number $n > 1$ can be decomposed into a product of powers of *different* primes:

$$n = p_1^{\alpha_2} \cdots p_k^{\alpha_k}, \quad \alpha_1, \ldots, \alpha_k, k \geq 1.$$

Furthermore, this decomposition is unique up to the order of the factors.

An important topic in number theory is the distribution of prime numbers amongst the natural numbers. Perhaps it was the Greek mathematician Eratosthenes (circa 200 B.C.) who first introduced a general method to single out the primes in the sequence of natural numbers using the so-called "Eratosthenes's sieve": in order to list all the prime numbers between 1 and n we take the sequence of all natural numbers from 2 to n and cross out all multiples of 2 greater than 2, then all multiples of 3 greater than 3, etc. until we have deleted all numbers divisible by any natural number not greater than $\sqrt{n}$. The remaining numbers are precisely the primes between 1 and n (recall the remark after Theorem 5.1).

Looking at the sequence of primes one can see that they are rather irregularly scattered amidst the natural numbers. There are many (a hypothesis says *infinitely many*) so-called *prime twins* of the kind p and $p + 2$. On the other hand there are arbitrarily large "gaps", i.e. sequences of natural numbers without any primes. An example of a sequence of k consecutive composite natural numbers, for *any* natural number k, can be constructed as follows. We denote by $n!$ the product $1 \cdot 2 \cdots (n-1) \cdot n$. Now, consider the numbers $(k+1)! + 2, \ldots, (k+1)! + k, (k+1)! + (k+1)$. They are all composite (why?). For a stronger fact see Problem 5.11.

We shall give without proofs (which are too complicated to be discussed here) two important and very useful facts about the distribution of primes. The first one was conjectures by Bertrand in 1845 and proved by Tchebychef in 1850:

Theorem 5.5 (Bertrand's Postulate)**.** *For every integer $n \geq 4$ there is at least one prime p such that $n < p < 2n - 2$.*

The second one is credited to Dirichlet:

Theorem 5.6 (Dirichlet's Theorem on primes in arithmetic progressions)**.** *Every arithmetic progression $a, a + d, a + 2d, \ldots$ where $d > 0$ and $(a, d) = 1$ contains infinitely many primes.*

Problems

5.1. Without using Dirichlet's Theorem 5.6 show that there are infinitely many primes of the form

(a) $4n + 3$;

(b) $6n + 5$.

5.2. (a) Show that if a prime is divided by 30 the remainder is either 1 or a prime.

(b) Is this true if 30 is replaced by 60?

5.3. If p_n denotes the n-th prime in the sequence of natural numbers, prove the inequality

$$p_n < 2^{2^n}.$$

5.4. Prove that for every $n > 2$ there is a prime p such that $n < p < n!$.

5.5. Show that if the number $2^p - 1$ is prime, then p is a prime. (Prime numbers of the kind $2^p - 1$ are called *Mersenne primes*).

5.6. Show that if the number $2^n + 1$ is a prime, then n is a power of 2. (Prime numbers of the kind $2^{2^k} + 1$ are called *Fermat primes*.)

5.7. A natural number m is called *perfect* if it equals the sum of its proper positive divisors (i.e. all positive divisors of m excluding m itself). For example $6 = 1 + 2 + 3$ and $28 = 1 + 2 + 4 + 7 + 14$ are perfect numbers.

Prove the following theorem (Euclid, *Elementa, Book 9*):
If $2^m - 1$ is a prime then $2^{m-1}(2^m - 1)$ is a perfect number.

5.8. Let $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ and $m = p_1^{\beta_1} \cdots p_k^{\beta_k}$ be decompositions of m and n in products of primes, where $p_1, p_2, \ldots, p_k$ are different primes and some of the α's and β's can be 0.

(a) Show that $n \mid m$ if and only if $\alpha_1 \leq \beta_1$, ..., $\alpha_k \leq \beta_k$.

(b) Denote $\min(\alpha_i, \beta_i)$ (the minimum of α_i and β_i) by γ_i and $\max(\alpha_i, \beta_i)$ (the maximum of α_i and β_i) by δ_i, for $i = 1, \ldots, k$. Then show that

$$(m, n) = p_1^{\gamma_1} \cdots p_k^{\gamma_k} \quad \text{and} \quad [m, n] = p_1^{\delta_1} \cdots p_k^{\delta_k}.$$

For example, if $n = 9800 = 2^3 \cdot 5^2 \cdot 7^2$ and $m = 14742 = 2 \cdot 3^4 \cdot 7 \cdot 13$ then we can represent tham as $n = 2^3 \cdot 3^0 \cdot 5^2 \cdot 7^2 \cdot 13^0$ and $m = 2^1 \cdot 3^4 \cdot 5^0 \cdot 7^1 \cdot 13^1$, hence $(m, n) = 2^1 \cdot 3^0 \cdot 5^0 \cdot 7^1 \cdot 13^0 = 14$ and $[m, n] = 2^3 \cdot 3^4 \cdot 5^2 \cdot 7^2 \cdot 13^1 = 10319400$.

5.9. Using Problem 5.8 prove the following identities for any natural numbers a, b, c:

(a) $(a, [b, c]) = [(a, b), (a, c)]$;

(b) $[a, (b, c)] = ([a, b], [a, c])$;

(c) $[(a, b), (b, c), (c, a)] = ([a, b], [b, c], [c, a])$;

(d) $[a, b, c] = \dfrac{abc}{(ab, bc, ca)}$;

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

5.10. Let $m_1, \ldots, m_k$ be natural numbers, $M = m_1 \cdots m_k$ and $M_i = \frac{M}{m_i}$, for $i = 1, 2, \ldots, n$. Prove that $m_1, \ldots, m_n$ are relatively prime in pairs if and only if $(M_1, M_2, \ldots, M_n) = 1$.

5.11. Let n and $k \geq 2$ be natural numbers. Show that there exist n consecutive natural numbers each of which can be factorized in a product of at least k prime divisors (not necessarily different).

6 Congruences

Now we shall develop a very convenient and powerful "language" for expressing and solving problems in number theory.

Here is the basic definition. Let a and b be integers and m a natural number greater than 1.If $m \mid a-b$ then a and b are called *congruent modulo* m, denoted

$$a \equiv b \pmod{m}.$$

An expression like this is called a *congruence*. In particular, if $0 \leq b < m$ we say that b is the *remainder of* a *modulo* m.

As we see, using congruences is just another way to speak about divisibility. Thus many properties of divisibility can easily be translated into properties of congruences. Here are the basic ones (a, b, c, d, k, n are arbitrary integers and m is a natural number):

(CON1) $a \equiv b \pmod{m}$ if and only if $a - b \equiv 0 \pmod{m}$;

(CON2) $a \equiv a \pmod{m}$;

(CON3) if $a \equiv b \pmod{m}$ then $b \equiv a \pmod{m}$;

(CON4) if $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$ then $a \equiv c \pmod{m}$;

(CON5) if $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$ then $ak + cn \equiv bk + dn \pmod{m}$. In particular

(a) if $a \equiv b \pmod{m}$ then $a + c \equiv b + c \pmod{m}$ and $a - c \equiv b - c \pmod{m}$;

(b) if $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$ then $a+c \equiv b+d \pmod{m}$ and $a-c \equiv b-d \pmod{m}$;

(CON6) if $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$ then $ac \equiv bd \pmod{m}$;

(CON7) if $a \equiv b \pmod{m}$ and $n \geq 0$ then $a^n \equiv b^n \pmod{m}$;

(CON8) if $a \equiv b \pmod{m}$ and $d \mid m$, $d > 0$ then $a \equiv b \pmod{d}$;

(CON9) if $a \equiv b \pmod{m}$ and $c > 0$, then $ac \equiv bc \pmod{mc}$.

All these properties are straightforward consequences of the definition of a congruence and the basic properties of divisibility. Let us verify two of them:

(CON5) Let $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$. Then $m \mid a - b$ and $m \mid c - d$. Therefore $m \mid ak - bk$ and $m \mid cn - dn$, hence $m'div(ak - bk) + (cn - dn)$, i.e. $m \mid (ak + cn) - (bk + dn)$ which means that $ak + cn \equiv bk + dn \pmod{m}$.

(CON6) Again $m \mid a-b$ and $m \mid c-d$, hence $m \mid (a-b)c$ and $m \mid (c-d)b$. Therefore $m \mid (a-b)c-(c-d)b$, i.e. $m \mid ac - bd$, so $ac \equiv bd \pmod{m}$.

Exercise. Verify the other properties listed above.

Here is a typical demonstration of the power of congruences:

Problem: Find the last two digits of $7^{7^{7^7}}$.
Solution: First, notice that the last two digits (in decimal notation) of *any* natural number are given by the remainder of that number modulo 100. Therefore we have to solve for x the congruence

$$7^{7^{7^7}} \equiv x \pmod{100}, \quad 0 \leq x < 100.$$

The idea is to start with some power of 7 which has a small remainder modulo 100, preferably 1 or -1, and then to raise that congruence to a power close to $7^{7^{7^7}}$. In this case we are lucky to have

$$7^4 = 2401 \equiv 1 \pmod{100}.$$

Now we want this congruence to some power x such that $(7^4)^x = 7^{4x}$ is as close as possible to $7^{7^{7^7}}$. Then we would get $7^{4x} \equiv 1^{4x} = 1 \pmod{100}$ and, suppose that $7^{7^7} = 4x + y$, then $7^{7^{7^7}} = 7^{4x} \cdot 7^y$, from where

$$7^{7^{7^7}} \equiv 7^y \pmod{100}.$$

Thus we can reduce our problem to: find the *remainder* y *of* 7^{7^7} *modulo* 4, i.e. solve for y the congruence

$$7^{7^7} \equiv y \pmod{4}, \quad 0 \leq y < 4.$$

We have $7 \equiv -1 \pmod{4}$, hence $7^{7^7} \equiv (-1)^{7^7} = -1 \equiv 3 \pmod{4}$. Therefore

$$7^{7^{7^7}} = 7^3 = 343 \equiv 43 \pmod{100}.$$

Thus, the last two digits of $7^{7^{7^7}}$ are 43.
It's like magic isn't it?

We can see that in a way the congruences behave like equalities with respect to addition, subtraction and multiplication. With division however, the matter is delicate. Instead of the usual cancellation law, the following holds.

Theorem 6.1. *for all integers a, x, y and any natural number m, $ax \equiv ay \pmod{m}$ if and only if $x \equiv y \pmod{\frac{m}{(a,m)}}$.*

Proof. We may assume that $a \neq 0$ and $x \neq y$, otherwise the statement is trivial. Now, if $ax \equiv ay \pmod{m}$ then $ax - ay = km$ for some integer $k/ne0$. Hence

$$\frac{a}{(a,m)}(x-y) = \frac{m}{(a,m)}k.$$

and thus

$$\frac{m}{(a,m)} \,\Big|\, \frac{a}{(a,m)}(x-y).$$

But $\left(\frac{m}{(a,m)}, \frac{a}{(a,m)}\right) = 1$ by (GCD7). Therefore $\frac{m}{(a,m)} \,\Big|\, (x-y)$ by Theorem 3.1 (1), which implies $x \equiv y \pmod{\frac{m}{(a,m)}}$.

Conversely, if $x \equiv y \pmod{\frac{m}{(a,m)}}$ then $ax \equiv ay \pmod{\frac{am}{(a,m)}}$ by (CON9). The number $b = \frac{a}{(a,m)}$ is an integer, hence $m \mid \frac{am}{(a,m)}$ and therefore $ax \equiv ay \pmod{m}$ by (CON8). □

For example, $x \equiv y \pmod{5}$ if and only if $12x \equiv 12y \pmod{30}$.

As a consequence we obtain the following frequently used fact:

Corollary 6.2. *If $ax \equiv ay \pmod{m}$ and $(a, m) = 1$, then $x \equiv y \pmod{m}$.*

For example, if $45x \equiv 45y \pmod{14}$, then $x \equiv y \pmod{14}$.

Theorem 6.3. *$x \equiv y \pmod{m_i}$ for $i = 1, 2, \ldots, k$ if and only if $x \equiv y \pmod{[m_1, m_2, \ldots, m_k]}$.*

Proof. if $x \equiv y \pmod{m_i}$ for $i = 1, 2, \ldots, k$ then $m_i \mid (x - y)$ for $i = 1, 2, \ldots, k$. Thus $x - y$ is a common multiple of $m_1, m_2, \ldots, m_k$ and hence $[m_1, m_2, \ldots, m_k] \mid (x-y)$ by Theorem 4.1, which implies $x \equiv y \pmod{[m_1, m_2, \ldots, m_k]}$. Conversely if $x \equiv y \pmod{[m_1, m_2, \ldots, m_k]}$ then $x \equiv y \pmod{m_1}$ for $i = 1, 2, \ldots, k$ by (CON8). □

Problems

6.1. Show that

(a) every decimal number which is a square has one of the following for its unit digit: 0, 1, 4, 5, 6, 9.

(b) every decimal number which is a fourth power has one of the following for its digit: 0, 1, 5, 6.

6.2. Find

(a) the possible remainders modulo 8 of any square of an integer.

(b) the possible remainders modulo 7 of any cube of an integer.

6.3. Find the last decimal digit of (a) 2^{222}; (b) 3^{333}; (c) 7^{777}.

6.4. Prove that the number $3n^2 - 5$ where n is an integer can never be a perfect square.

6.5. Prove that if $x \equiv y \pmod{m}$ then $(x, m) = (y, m)$.

6.6. Show that any natural number n in decimal representation is divisible by

(a) 3 if and only if the sum of its digits is divisible by 3.

(b) 9 if and only if the sum of its digits is divisible by 9.

6.7. Let A be the sum of its digits of the number 4444^{4444} and B be the sum of the digits of A. Find the sum of the digits of B. (All numbers are decimal.)

This was Problem 4 from the 17th IMO in Bulgaria, 1975.

7 Residue systems. Euler's function. Theorems of Euler and Fermat

Given a natural number m, we consider the set of numbers $\{0, 1, 2, \ldots, m-1\}$. This is the set of all possible remainders modulo m, therefore it has the following property: every integer is congruent modulo m to exactly one number from this set. The sets $\{1, 2, \ldots, m\}$, $\{2, 3, \ldots, m+1\}$, $\{-1, 0, \ldots, m-2\}$ and infinitely many others have the same property. This observation leads us to the following definition.

Given a natural number m, a set of integers $\{x_1, \ldots, x_m\}$ is called a *complete residue system modulo* m if for every integer y there is exactly one x_i such that $y \equiv x_i \pmod{m}$.

Of course the numbers $x_1, \ldots, x_m$ do not need to be consecutive. For instance $\{-25, 13, 134, -1359, 2\}$ is a complete residue system modulo 5.

Let us notice that:

(1) m integers form a complete residue system modulo m if and only if no two of them are congruent modulo m.

(2) If $x_1, \ldots, x_m$ is a complete residue system modulo m then for any integer a, the numbers $x_1 + a, \ldots, x_m + a$ is such a complete residue system modulo m.

Exercise. Verify these facts.

Theorem 7.1. *If $x_1, \ldots, x_m$ is a complete residue system modulo m and k is an integer relatively prime to m, then $kx_1, \ldots, kx_m$ is also a complete residue system modulo m.*

Proof. Suppose $kx_i \equiv kx_j \pmod{m}$ for some $i \neq j$. Then $m \mid k(x_i - x_j)$ and since $(m, k) = 1$, it follows by Theorem 3.1 (1) that $m \mid (x_i - x_j)$ which contradicts the assumption that $x_1, \ldots, x_m$ is a complete residue system modulo m. □

Now we shall introduce a function on the set of natural numbers which plays an important role in number theory. It is called *Euler's function*, denoted by ϕ and defined for all natural numbers as follows:

$\phi(n)$ *equals the number of positive integers less than or equal to n and relatively prime to n.*

For example $\phi(1) = 1$, $\phi(11) = 10$ and $\phi(12) = 4$.

Obviously for large values of n the definition is not convenient for computation of $\phi(n)$ and we need some sort of a formula. In order to find such a formula we have to make several observations about Euler's function.

(1) If n is prime then $\phi(n) = n - 1$ since all $n - 1$ positive integers less than n are relatively prime to n.

(2) If $n = p^k$ where p is prime then $\phi(n) = p^k - p^{k-1}$. Indeed, the numbers between 1 and p^k which *are not* relatively prime to p^k are exactly the p^{k-1} multiples of p: $1 \cdot p, 2 \cdot p, \ldots, p^{k-1} \cdot p$ and the remaining $p^k - p^{k-1}$ numbers *are* relatively prime to p^k.

(3) $\phi(n)$ has the following *multiplicative property*: for every two relatively prime natural numbers m and n,

$$\phi(mn) = \phi(m)\phi(n).$$

In order to verify this property let us arrange the integers from 1 to mn in a rectangular table with m rows and n columns as follows:

$$\begin{array}{cccc} 1 & 2 & \cdots & n \\ n+1 & n+2 & \cdots & 2n \\ 2n+1 & 2n+2 & \cdots & 3n \\ \vdots & \vdots & \ddots & \vdots \\ (m-1)n+1 & (m-1)n+2 & \cdots & mn \end{array}$$

We see that the number in the i-th row and j-th column of this table is $(i-1)n + j$.

First let us notice that this number is relatively prime to n if and only if j is relatively primes to n, by (GCD5). Thus the numbers from the table which are relatively prime to n are precisely the elements of those $\phi(n)$ columns which correspond to the numbers j relatively prime to n.

Next, $0 \cdot n, 1 \cdot n, \ldots, (m-1)n$ is a complete residue system modulo m since $(m, n) = 1$, by Theorem 7.1. Therefore $0 \cdot n + j, 1 \cdot n + j, \ldots, (m-1)n + j$ is a complete residue system modulo m for every integer j. Thus the numbers from the table which are relatively prime to m are precisely the elements of those $\phi(m)$ rows which correspond to the numbers i for which $i - 1$ is relatively prime to n.

Now, the numbers from the table which are relatively prime to mn are those which are relatively prime to n and the $\phi(m)$ rows with numbers relatively prime to m. therefore there are exactly $\phi(m) \cdot \phi(n)$ numbers in the table which are relatively prime to mn, i.e. $\phi(mn) = \phi(m)\phi(n)$.

- Applying Theorem 3.1 (3) several times we can generalize the multiplicative property of $\phi(n)$ as follows:
  If $n_1, \ldots, n_k$ are relatively prime in pairs, then

$$\phi(n_1 \cdots n_k) = \phi(n_1) \cdots \phi(n_k).$$

Now we are ready to compute $\phi(n)$ for any natural number n. Let $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ where $p_1^{\alpha_1}$, ..., $p_k^{\alpha_k}$ are powers of different primes. (Due to the Fundamental theorem of arithmetic every natural numbers can be represented in this way.) Then every two of these powers are relatively prime. Applying the properties (4) and (2) of $\phi(n)$ we find:

$$\phi(n) = \phi\left(p_1^{\alpha_1}\right) \cdots \phi\left(p_k^{\alpha_k}\right) = \left(p_1^{\alpha_1} - p_1^{\alpha_1 - 1}\right) \cdots \left(p_k^{\alpha_k} - p_k^{\alpha_k - 1}\right).$$

In a slightly more concise form:
If $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$, then $\phi(n) = n\left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_k}\right)$..

For instance:

$$\begin{aligned} \phi(2646) &= \phi(2 \cdot 3^3 \cdot 7^2) = (2^1 - 2^0)(3^3 - 3^2)(7^2 - 7^1) = 1512, \\ \text{and} \quad \phi(1000) &= \phi(2^3 5^3) = 1000 \cdot \frac{1}{2} \cdot \frac{4}{5} = 400. \end{aligned}$$

Theorem 7.2 (Euler's Theorem)**.** *For every natural number n and integer a relatively prime to n the following congruence holds:*

$$a^{\phi(n)} \equiv 1 \pmod{n},$$

that is, $n \mid (a^{\phi(n)} - 1)$.

Proof. Let $x_1, \ldots, x_{\phi(n)}$ be the natural numbers less than n and relatively prime to n. Now consider $ax_1, \ldots, ax_{\phi(n)}$. These are $\phi(n)$ numbers which are all relatively prime to n, by Theorem 3.1 (3), and no two of them are congruent. (A system of $\phi(n)$ integers with such properties is called a *reduced residue system modulo* n). Therefore if y_i is the remainder if ax_i modulo n for $i = 1, 2, \ldots, \phi(n)$ then $y_1, \ldots, y_{\phi(n)}$ are $\phi(n)$ different natural numbers less than n and relatively prime to n. But then they are exactly the numbers $x_1, \ldots, x_{\phi(n)}$, perhaps in another order! Therefore $x_1 \cdots x_{\phi(n)} = y_1 \cdots y_{\phi(n)}$. Now $ax_i \equiv y_i \pmod{n}$ for $i = 1, \ldots, \phi(n)$, hence $(ax_1) \cdots (ax_{\phi(n)}) \equiv y_1 \cdots y_{\phi(n)} \pmod{n}$.

But $(ax_1) \cdots (ax_{\phi(n)}) = a^{\phi(n)} x_1 \cdots x_{\phi(n)} = a^{\phi(n)} y_1 \cdots y_{\phi(n)}$. Thus $a^{\phi(n)} y_1 \cdots y_{\phi(n)} \equiv y_1 \cdots y_{\phi(n)} \pmod{n}$.

Furthermore, the product $y_1 \cdots y_{\phi(n)}$ is relatively prime to n by Theorem 3.1 (3). Therefore, by Corollary 6.2, we may cancel the last congruence by $y_1 \cdots y_{\phi(n)}$ and thus we find that

$$a^{\phi(n)} \equiv 1 \pmod{n}.$$

□

For example, since $\phi(1000) = 400$ and $(1993, 1000) = 1$ it follows that

$$1993^{400} \equiv 1 \pmod{1000}$$

which means that the last three digits of the number 1993^{400} are 001. Try to imagine how much time it would take to establish this result by calculation of the number itself. Or, consider the problem: find the last two digits of $77^{77^{77}}$. We can approach this problem similarly to the one about 7^{7^7}, but it could take a lot of time until we get an appropriate "starting point". Here is where Euler's theorem comes to help: $\phi(100) = 40$, hence $77^{40} \equiv 1 \pmod{100}$, etc.

Exercise. Complete the solution of this problem.

The particular case of Euler's theorem when n is prime is known as *Fermat's theorem*: *For every prime number p and integer a not divisible by p the following congruence holds*:

$$a^{p-1} \equiv 1 \pmod{p},$$

that is, $p \mid (a^{p-1} - 1)$.

(Do not confuse this with the famous *Fermat's Last Theorem* which, after more than 300 years of futile attempts, was proved by the mathematician Andrew Wiles.)

Theorem 7.3. *For every natural number n and integer a relatively prime to n there exists a least positive integer k such that*

$$a^k \equiv 1 \pmod{n}.$$

Moreover, every natural number m for which $a^m \equiv 1 \pmod{n}$ is a multiple of k. In particular $k \mid \phi(n)$.

The number k is called the order of a modulo n, *and a is said to* belong to the exponent of k.

Proof. The set S of all natural numbers k for which $a^k \equiv 1 \pmod{n}$ is non-empty since it contains $\phi(n)$. Then, by the fundamental property of natural numbers, there is a least natural number in S, which we call k. Now, let m be any number from S. Dividing m by k with a remainder we get $m = kq + r$, $0 \le r < k$. Then

$$1 \equiv a^{kq+r} \equiv a^{kq} \cdot q^r \equiv (a^k)^q \cdot a^r \equiv 1^q \cdot a^r \equiv a^r \pmod{n}.$$

Thus, r satisfies $a^r \equiv 1 \pmod{n}$ and is less than k, hence $r = 0$. □

Problems

7.1. Find a complete residue system modulo 7 consisting of multiples of 3.

7.2. Prove that $a^p \equiv a \pmod{p}$ for every prime number p and integer a.

7.3. Show that $7 \mid n^{30} - 1$ if $(n, 7) = 1$.

7.4. Prove that $42 \mid n^7 - n$ for every integer n.

7.5. Prove the congruences

(a) $2^{11\cdot 31} \equiv 2 \pmod{11 \cdot 31}$

(b) $2^{19\cdot 73} \equiv 2 \pmod{19 \cdot 73}$

7.6. Evaluate $\phi(n)$ for $n = 1, 2, \ldots, 16$.

7.7. (a) Find all positive integers n for which $7 \mid 2^n - 1$.

(b) Show that for every positive integer n, $7 \nmid 2^n + 1$.

This was Problem 1 at the 6th IMO in Moscow, 1964.

7.8. For every natural number $n > 1$ show that

$$\sum_{m<n,(m,n)=1} = \frac{n\phi(n)}{2}$$

where the sum ranges over all natural numbers m less than n and relatively prime to n.

7.9. (a) If $n > 4$ show that n is composite if and only is $(n-1)! \equiv 0 \pmod{n}$.

(b) (*Wilson's Theorem*) Show that if $n > 1$ is a prime then $(n-1)! + 1 \equiv 0 \pmod{n}$.

7.10. Let m and n be natural numbers such that $n > m \geq 1$. The last three digits in the decimal expansion of the number 1978^m coincide with the last three digits in the decimal expansion of the number 1978^n. Find m and n such that the sum $m + n$ is minimal.

This was Problem 1 from the 20th IMO in Romania, 1978.

8 Linear congruences and Chinese Remainder Theorem

If a, b are integers and m is a natural number we say that the congruence

$$ax \equiv b \pmod{m} \tag{2}$$

is a *linear congruence*. We are interested in the question whether this congruence has solutions for x and how to find them.

First, let us observe that if (2) has *one* solution x_0 then it has *infinitely many* solutions: $x_0 \pm m, x_0 \pm 2m, \ldots$. We can say even more: if x_0 is a solution of (2) then *all solutions x of (2) and only they* satisfy the congruence $ax \equiv ax_0 \pmod{m}$, and hence due to Theorem 6.1, the congruence $x \equiv x_0 \pmod{\frac{m}{(a,m)}}$. Thus all solutions of (2) are given by the formula $x = x_0 + \frac{m}{(a,m)}k$ where k is any integer. For instance $6x \equiv 2 \pmod{8}$ has a solution $x = 3$, hence all solutions are the numbers $3 + 4k$. Therefore our problem is reduced to find *just one* solution of (2) or to show that there aren't any.

Second, in the particular case when $(a, m) = 1$ the congruence (2) *has a solution*. Indeed, let x take values $0, 1, \ldots, m-1$. This is a complete residue system modulo m. Therefore, by Theorem 7.1, the numbers $0 \cdot a, 1 \cdot a, \ldots, (m-1)a$ is also a complete residue system modulo m. Hence at least one (in fact exactly one) of the numbers $0, 1, \ldots, m-1$ is a solution of (2).

Now we are ready to attack the general case for which the following theorem gives a necessary and sifficient condition for existence of solution.

Theorem 8.1. *The linear congruence*

$$ax \equiv b \pmod{m}$$

has a solution if and only if $(a, m) \mid b$.

Proof. If x is a solution of the congruence then $m \mid ax-b$ and $(a,m) \mid m$, hence $(a,m) \mid ax-b$. Moreover, $(a,m) \mid a$, hence $(a,m) \mid ax$. Thus $(a,m) \mid b$. Conversely, if $(a,m) \mid b$, let $a = (a,m)a_1$, $b = (a,m)b_1$ and $m = (a,m)m_1$, for some integers a_1, b_1 and m_1 respectively. Then, by Theorem 6.1, the congruence $ax \equiv b \pmod{m}$ is equivalent to

$$a_1 x \equiv b_1 \pmod{m_1},$$

and furthermore $(a_1, m_1) = 1$. As we noticed above, the latter congruence has a solution. □

The drawback of this theorem is that is gives no idea of *how to find a solution* when it exists. This is a typical example of a so-called *non-constructive theorem of existence*. Sometimes in mathematics the most we can say about an object is that it exists but it is impossible *in principle* to find or construct it. Fortunately this is not so in our case. Of course, if m is small enough we may check all numbers $0, 1, \ldots, m-1$ until we find a solution. If m is large this is impractical and we need a more efficient approach. Without going much into technicalities we shall sketch a procedure how to find a solution of (2) when it exists, i.e. when $(a,m) \mid b$. The idea is to reduce in several steps the congruence until we reach an equivalent one which has an obvious solution. First, if a and m are not relatively prime, we may cancel by (a,m) and consider the particular case when $(a,m) = 1$. Then we perform the following pair of reductions:

(1) replace a and b with their respective remainders modulo m. The resulting congruence is equivalent to the initial one and in addition *a becomes less than m.*

(2) reduce the congruence (2) to

$$my \equiv -b \pmod{a}$$

in the following sense: *if y is a solution of the latter congruence then $x = \frac{my+b}{a}$ is a solution of (2).*
Just substitute this x in (2) and you will see it. The benefit of this reduction is obvious: the modulus of the congruence has strictly decreased.

Now, applying this pair of tricks several times we shall inevitably end with a congruence modulo 1 (why? Hint: the Euclidean algorithm for computing (a,m) is built-in in this procedure) which has an obvious solution of (2). Or, reaching a small enough modulus we solve the congruence by inspection. Here is an example: Solve

$$9965 \equiv 19955 \pmod{4950}.$$

First, $(9965, 4950) = 5$ and we reduce this congruence to

$$1993x \equiv 3991 \pmod{990}.$$

Then, $1993 = 2 \cdot 990 + 13$ and $3991 = 4 \cdot 990 + 31$. Thus we reduce our congruence to

$$13x \equiv 31 \pmod{990}.$$

Further we replace it by

$$990y \equiv -31 \pmod{13},$$

and note that the solution we seek is $x = \frac{990y+31}{13}$.

Now we repeat the first two steps: $990 = 76 \cdot 13 + 2$ and $-31 = -3 \cdot 13 + 8$, thus we consider

$$2y \equiv 8 \pmod{13},$$

which we replace by

$$13z \equiv -8 \pmod{2}$$

which has an obvious solution $z = 0$, whence $y = \frac{13 \cdot 0 + 8}{2} = 4$ and

$$x = \frac{990 \cdot 4 + 31}{13} = 307.$$

Let us check it:

$$1993 \cdot 307 = 611851 = 618 \cdot 990 + 31 = 614 \cdot 990 + 3991.$$

It works!

Exercise. (1) Applying the above described procedure solve the congruence $166x \equiv 18 \pmod{38}$, or show that there are no solutions.

Exercise. (2) Present the above procedure as a formal algorithm, as was done in section 2 with the Euclidean algorithm for computing the greatest common divisor. Then prove the correctness of this algorithm.

Having solved completely the problem for *one* linear congruence we can proceed to *systems* of linear congruences. This might appear to be a piece of quite modern, though elementary mathematics, but to our surprise it turns out that the method of solving such systems was essentially known in China in the *first century A.D.*! Of course not presented in the language of congruences which makes our life much easier than the life of the ancient Chinese mathematicians. Anyway, here is the key theorem, known as the Chinese Remainder Theorem:

Theorem 8.2 (Chinese Remainder Theorem)**.** *Let $m_1, \ldots, m_k$ be natural numbers relatively prime in pairs and $b_1, \ldots, b_k$ be any integers. Then the system of congruences*

$$\left|\begin{array}{ll} x \equiv b_1 & (\mathrm{mod}\ m_1) \\ & \vdots \\ x \equiv b_k & (\mathrm{mod}\ m_k) \end{array}\right.$$

has a solution. Moreover, it has infinitely many solutions which are all congruence modulo the product $m_1 \cdots m_k$.

Proof. Let $M = m_1 \cdots m_k$ and $M_i = \frac{M}{m_i}$ for $i = 1, 2, \ldots, k$. Then $(M_1, \ldots, M_k) = 1$ (see Problem 5.10), hence

$$u_1 M_1 + \cdots + u_k M_k = 1$$

for some integers $u_1, \ldots, u_k$. Therefore $u_i M_i \equiv 1 \pmod{m_i}$ and $u_i M_i \equiv 0 \pmod{m_j}$ for any $i \neq j$ (why?). Then

$$x = u_1 M_1 b_1 + \cdots + u_k M_k b_k$$

is a solution of our system. □

The above proof suggests a method to find a solution of the system of congruences: first we find integers $u_1, \ldots, u_k$ such that $u_i M_i \equiv 1 \pmod{m_i}$ for $i = 1, \ldots, k$. Of course there are infinitely many such integers and we cannot expect that those we have found will satisfy $u_1 M_1 + \cdots u_k M_k = 1$, but they will satisfy $u_1 M_1 + \cdots u_k M_k \equiv 1 \pmod{m_i}$ for $i = 1, \ldots, k$ which is enough to claim that $u_1 M_1 b_1 + \cdots + u_k M_k b_k$ is a solution of the system.

For example consider the following

Problem: Find a natural number x giving remainders 1,2,3,4 when divided by 2,3,5,7 respectively.

Solution: The problem boils down to solving the system

$$\left|\begin{array}{ll} x \equiv 1 & (\mathrm{mod}\ 2) \\ x \equiv 2 & (\mathrm{mod}\ 3) \\ x \equiv 3 & (\mathrm{mod}\ 5) \\ x \equiv 4 & (\mathrm{mod}\ 7) \end{array}\right.$$

We look for integers u_1, u_2, u_3 and u_4 such that $105u_1 \equiv 1 \pmod{2}$, $70u_2 \equiv 1 \pmod{3}$, $42u_3 \equiv 1 \pmod{5}$ and $30u_4 \equiv 1 \pmod{7}$. We find $u_1 \equiv 1 \pmod{2}$, $u_2 \equiv 1 \pmod{3}$, $u_3 \equiv 3 \pmod{5}$ and $u_4 \equiv 4 \pmod{7}$. Possible values are $u_1 = 1$, $u_2 = 1$, $u_3 = 3$ and $u_4 = 4$ from where $x = 1{\cdot}1{\cdot}105 + 2{\cdot}1{\cdot}70 + 3{\cdot}3{\cdot}42 + 4{\cdot}4{\cdot}30 = 1103$. This is one solution. All other solutions are obtained from the formula $x + [2, 3, 5, 7]k = x + 210k$. Thus the smallest positive solution is $x - 210 \cdot 5 = 53$.

Now consider a linear system of congruences

$$\left|\begin{array}{ll} a_1 x \equiv b_1 & (\mathrm{mod}\ m_1) \\ & \vdots \\ a_k x \equiv b_k & (\mathrm{mod}\ m_k) \end{array}\right.$$

where $m_1, \ldots, m_k$ are natural numbers relatively prime in pairs and each of the congruences has a solution. Let $x_1, \ldots, x_k$ be respective solutions to these congruences. Then the above system is equivalent to

$$\left|\begin{array}{ll} x \equiv x_1 & (\mathrm{mod}\ m_1) \\ & \vdots \\ x \equiv x_k & (\mathrm{mod}\ m_k) \end{array}\right.$$

which according to the Chinese Remainder Theorem has a solution.

Note that the Chinese Remainder Theorem gives only *sufficient but not necessary conditions* for the existence of a solution of a system of linear congruences. Indeed the system

$$\left|\begin{array}{ll} x \equiv 2 & (\mathrm{mod}\ 6) \\ & \vdots \\ x \equiv 6 & (\mathrm{mod}\ 8) \end{array}\right.$$

has a solution e.g. $x = 14$, without satisfying the conditions of the theorem. Let us only mention that there exist necessary and sufficient conditions which we are not going to discuss here.

Problems

8.1. Solve the congruences or show that there are no solutions.
(a) $25x \equiv 5 \pmod{16}$; (b) $1001x \equiv 91 \pmod{104}$; (c) $3700x \equiv 11 \pmod{111}$.

8.2. Find the smallest possible solutions of the following systems of congruences

$$\text{(a)}\ \left|\begin{array}{ll} x \equiv 2 & (\mathrm{mod}\ 4) \\ x \equiv 3 & (\mathrm{mod}\ 9) \end{array}\right. \quad \text{(b)}\ \left|\begin{array}{ll} x \equiv 0 & (\mathrm{mod}\ 3) \\ x \equiv 1 & (\mathrm{mod}\ 5) \\ x \equiv 7 & (\mathrm{mod}\ 8) \end{array}\right. \quad \text{(c)}\ \left|\begin{array}{ll} x \equiv 2 & (\mathrm{mod}\ 3) \\ x \equiv 1 & (\mathrm{mod}\ 4) \\ x \equiv 1 & (\mathrm{mod}\ 5) \\ x \equiv -2 & (\mathrm{mod}\ 17) \end{array}\right.$$

8.3. Every two of n arithmetic progressions have a common term. Show that all progressions have a common term.

8.4. Show that for every natural number n, in every arithmetic progression of natural numbers there are n consecutive terms which are composite numbers.

8.5. Prove that for every natural number k there exists a prime p such that each of the numbers $p-1$, $p+1$ and $p+2$ has at least k different prime divisors.

Hints and Solutions

Chapter 1

1.1. Hint: If $a \neq 0$ and $b \mid a$ then $|b| \leq |a|$.

1.2. $100 = 9 \cdot 11 + 1$, $1000 = 90 \cdot 11 + 10$. Therefore the multiples of 11 between 100 and 1000 are $10 \cdot 11, 11 \cdot 11, \ldots, 90 \cdot 11$. They are $90 - 10 + 1 = 81$.

1.3. If n is even, say $n = 2k$, then $n^2 = 4k^2 = k^2 \cdot 4 + 0$. If n is odd, say $n = 2k + 1$, then $n^2 = 4k^2 + 4k + 1 = (k^2 + k) \cdot 4 + 1$.

1.4. Hint: Use Pythagoras's theorem.

(a) Consider the possible remainders of a square divided by 3.

(b) Similarly.

1.5. Hints:

(a) if d is the last digit of n then $n = 10n' + d = (5n') \cdot 2 + d$. Then $2 \mid n$ if and only if $2 \mid d$.

(b) if d_1d_2 are the last two digits of n then $n = 100n' + 10d_1 + d_2$ and $4 \mid 100n'$, hence $4 \mid n$ if and only if $4 \mid 10d_1 + d_2$.

(c) See (a).

1.6. Let $n, n+1, \ldots, n+k-1$ be k consecutive integers and let r be the remainder after dividing n by k, i.e. $n = qk + r$, $0 \leq r < k$. If $r = 0$ then $k \mid n$. Otherwise $r \geq 1$, hence $r + k - 1 \geq k$ and therefore one of the consecutive integers $r, r+1, \ldots, r+k-1$, say $r + j$, equals k. Then $n + j = kq + (r + j) = kq + k$, hence $k \mid n + j$.

Now suppose that two of the integers, say $n + i$ and $n + j$ are divisible by k and let $j \geq i$. Then $k \mid (n + j) - (n + i)$, i.e. $k \mid j - i$. But $0 \leq j - i < k$ hence $j - i$ must be 0.

1.7. (a) Let $n = 2k + 1$. Then $n^2 - 1 = 4k^2 + 4k$ and $2 \mid k(k + 1)$ hence $4 \cdot 2 \mid 4k(k + 1)$.

(b) Induction on n:
If $n = 1$ then $3^{2\cdot 1} - 1 = 8$ and the statement is true.
Assume that $8 \mid 3^{2n} - 1$ for some n. Then $3^{2(n+1)} - 1 = 9 \cdot 3^{2n} - 1 = 8 \cdot 3^{2n} + (3^{2n} - 1)$ which, according to the inductive hypothesis, is divisible by 8.

(c) Again induction on n
If $n = 1$ then $4^1 + 15 \cdot 1 - 1 = 18$ — divisible by 9.
Assume that $9 \mid 4^n + 15n - 1$ for some n. Then $9 \mid 4(4^n + 15n - 1) = 4^{n+1} + 60n - 4$ and in order to check that 9 divides $4^{n+1} + 15(n+1) - 1 = 4^{n+1} + 15n + 14$ it is enough to show that 9 divides $(4 \cdot 4^n + 60n - 4) - (4 \cdot 4^n + 15n + 14) = 45n - 18 = (5n - 2) \cdot 9$ which is obvious.

1.8. (a) Let 2^k be the greatest power of 2 not exceeding n. Then $\frac{1}{2^k}$ will be the only term in the sum N_1 with an odd numerator after reducing the sum to a common denominator. Therefore the numerator of the resulting fraction will be odd, whilst the denominator will be even, hence the fraction cannot be an integer.

(b) Similarly: consider the term with denominator divisible by the greatest possible power of 2.

(c) Consider the therm with denominator which is the greatest possible power of 3, say 3^k. Note that $\frac{1}{2 \cdot 3^k}$ does not occur in the sum N_3. Now continue similarly to (a).

1.9. For $n = 0$ we get $m \mid a + d$, (1)
for $n = 1$: $m \mid ab + c + d$, (2)
for $n = 2$: $m \mid ab^2 + 2c + d$, (3)
Then: (2) − (1) $\Rightarrow m \mid a(b - 1) + c$,
hence $m \mid ab(b - 1) + bc$, (4)
and (3) − (2) $\Rightarrow m \mid ab(b - 1) + c$, (5)
hence $m \mid abc(b - 1) + c^2$, (6)
then (4) − (5) $\Rightarrow m \mid c(b - 1)$,
hence $m \mid abc(b - 1)$. (7)
Finally (6) − (7) $\Rightarrow m \mid c^2$.

1.10. Divide N by m with a remainder: $N = mq_0 + r_0$ and put $c_0 = r_0$. If $q_0 < m$ we are done putting $c_1 = q_0$. Otherwise we divide q_0 by m with remainder: $q_0 = mq_1 + r_1$ and put $c_1 = r_1$. Then proceed in the same way with q_1, etc. Thus we obtain a sequence $q_0 > q_1 > \cdots$ of natural numbers. Due to the fundamental property of the natural numbers this process must stop after one or more steps, namely when some q_k becomes less than m. Then we put $c_k = q_k$ and obtain a representation of N in the desired form.

Now let us show that such a representation is unique. Suppose that there are two different ones:

$$N = c_1 + c_1 m + c_2 m^2 + \cdots + c_k m^k, (1)$$

and

$$N = d_0 + d_1 m + d_2 m^2 + \cdots + d_t m^t. (2)$$

We may assume that $k \geq t$ and extend the second sum to

$$N = d_0 + d_1 m + d_2 m^2 + \cdots + d_k m^k, (2')$$

putting $d_{t+1} = \cdots = d_k = 0$.

Let j be the least index for which $c_j \neq d_j$ and assume that $c_j > d_j$. Then subtracting (2') from (1) and dividing the result by m^j we obtain

$$0 = (c_j - d_j) + (c_{j+1} - d_{j+1})m + \cdots + (c_k - d_k)m^{k-j} = (c_j - d_j) + Cm.$$

Then $m \mid (c_j - d_j$ which is impossible since $0 < c_j - d_j < m$.

Chapter 2

2.1. Hint: if $(n, 4) = 2$ then $n = 4k + 2$ for some integer k.

2.2. No. Otherwise $3 \mid x$ and $3 \mid y$, hence $3 \mid x + y = 1000$.

2.3. Using repeatedly (GCD5) we simulate the Euclidean algorithm: $(3a + 5b, 11a + 18b) = (3a + 5b, 11a + 18b - 3(3a + 5b)) = (3a + 5b, 2a + 3b) = (3a + 5b - (2a + 3b), 2a + 3b) = (a + 2b, 2a + 3b) = (a + 2b, 2a + 3b - 2(a + 2b)) = (a + 2b, -b) = (a + 2b + 2(-b), -b) = (a, -b) = (a, b)$.

2.4. Again we use (GCD5):

$$(21n + 4, 14n + 3) = (7n + 1, 14n + 3) = (7n + 1, 1) = 1.$$

2.5. By (D10) $cC \mid aA$, $cC \mid aB$, $cC \mid Ab$ and $cC \mid AB$, hence $cC \mid (aA, aB, Ab, AB)$. Now, by Theorem 2.1, $c = ua + vb$ for some integers u and v; likewise $C = UA + VB$ for some integers U and V. Then $cC = (ua + vb)(UA + VB) = (uU)aA + (uV)aB + (Uv)Ab + (UV)AB$, hence $(aA, aB, Ab, AB) \mid cC$. Therefore $(aA, aB, Ab, AB) = cC$.

2.6. Suppose $m > n$ and let $(a_m, a_n) = d$. Then $d \mid k^{2^n} + 1$, hence $d \mid (k^{2^n} + 1)(k^{2^n} - 1) = k^{2^{n+1}} - 1$, hence $d \mid (k^{2^{n+1}} - 1)(k^{2^{n+1}} + 1) = k^{2^{n+2}} - 1$, etc. Finally $d \mid k^{2^m} - 1$. Then $d \mid (k^{2^m} + 1) - (k^{2^m} - 1) = 2$. Now, if k is even then every a_i is odd, hence $d = 1$; if k is odd then every a_i is even, hence $d = 2$.

2.7. For every natural number k, $a^k - 1 = (a - 1)(a^{k-1} + a^{k-2} + \cdots + a + 1)$ (check this!). Then $\frac{a^m - 1}{a - 1} = a^{m-1} + a^{m-2} + \cdots + a + 1 = (a^{m-1} - 1) + (a^{m-2} - 1) + \cdots + (a - 1) + m$. Now, let $\left(\frac{a^m - 1}{a - 1}, a - 1\right) = d_1$ and $(a - 1, m) = d_2$. Then $d_1 \mid a^k - 1$ for $k = 1, 2, \ldots, m - 1$ and $d_1 \mid (a^{m-1} - 1) + (a^{m-2} - 1) + \cdots + (a - 1) + m$, hence $d_1 \mid m$. Thus $d_1 \mid d_2$. Conversely, $d_2 \mid a^k - 1$ for $k = 1, 2, \ldots, m - 1$, hence $d_2 \mid (a^{m-1} - 1) + (a^{m-2} - 1) + \cdots + (a - 1)$ and $d_2 \mid m$, hence $d_2 \mid (a^{m-1} - 1) + (a^{m-2} - 1) + \cdots + (a - 1) + m = \frac{a^m - 1}{a - 1}$. Thus $d_2 \mid d_1$, hence $d_1 = d_2$.

2.8. If $m = n$ then $d = m = n$ and the statement is obvious. Let $m \neq n$ and suppose $n > m$. Dividing n by m with a remainder we get $n = mq + r$, $0 \leq r < m$. Then $a^n - 1 = a^{mq+r} - 1 = a^{mq}a^r - 1 = (a^{mq}a^r - a^r) + (a^r - 1) = a^r((a^m)^q - 1) + (a^r - 1) = A(a^m - 1) + (a^r - 1)$. Therefore $(a^n - 1, a^m - 1) = (A(a^m - 1) + (a^r - 1), a^m - 1) = (a^r - 1, a^m - 1)$. by (GCD5).

Now, the solution can be completed either by induction on $\max(m, n)$ or by following the steps in the Euclidean algorithm for computing (m, n).

Chapter 3

3.1. (a) 6, 10, and 15.

(b) 30, 42, 70 and 105.

(c) 30, 154, 273 and 715.

3.2. Amongst any 5 consecutive integers there is one which is odd and not divisible by 3.

3.3. (a) The product of every 3 consecutive integers is divisible by 2 and by 3 (follows from Problem 1.5), hence by Theorem 3.1 (4) it is divisible by 6.

(b) The product of every 4 consecutive integers is divisible by 3 and by 8, since some of them is divisible by 4 (Problem 1.3) and another one is divisible by 2.

(c) Use (b) and Theorem 3.1 (4).

3.4. (a) Due to Theorem 3.1 (4) it is enough to show that $2 \mid n^3 - n$ and $3 \mid n^3 - n$. This follows e.g. from Problem 1.5 because $n^3 - n = (n-1)n(n+1)$.

(b) Since $n^5 - n = (n-1)n(n+1)(n^2+1)$, in addition to (a) it is enough to show that $5 \mid n^5 - n$. Consider the 5 possibilities for the remainder r of n when divided by 5. If $r = 2$ then $n = 5k+2$, hence $n^2 + 1 = 25k^2 + 20k + 5$ which is divisible by 5. Likewise $5 \mid n^2 + 1$ when $r = 3$. When r is 0, 1 or 4 then $5 \mid n$, $5 \mid n-1$ and $5 \mid n+1$ respectively. Thus, in any case $5 \mid n^5 - n$.

(c) $n^5 - 5n^3 + 4n = (n-2)(n-1)n(n+1)(n+2)$. Now use Problem 3.3 (c).

3.5. We shall apply a sort of inductive reasoning. Given k terms of the sequence:

$$a_1 = 2^{n_1} - 3,\ a_2 = 2^{n_2} - 3,\ \ldots,\ a_k = 2^{n_k} - 3,$$

which are relatively prime in pairs, and such that $2 = n_1 < n_2 < \cdots < n_k$, we shall construct a number $a_{k+1} = 2^{n_{k+1}} - 3$ relatively prime to each of these numbers. Let $m = a_1 a_2 \cdots a_k$. Amongst the $m+1$ numbers $2^0, 2^1, \ldots, 2^m$ there are two which yield the same remainder when divided by m (pigeon-hole principle). Let 2^r and 2^s be two such numbers and let $r > s$. Then $pm = 2^r - 2^s = (2^{r-s} - 1)2^s$ for some natural number p. Since m is odd and hence $(m, 2^s) = 1$, it follows that $m \mid 2^{r-s} - 1$, hence $qm = 2^{r-s} - 1$ for some natural number q. Then we put $a_{k+1} = 2^{r-s+2} - 3 = 4 \cdot 2^{r-s} - 3 = 4(qm+1) - 3 = 4qm + 1$. Obviously it is relatively prime to m, and hence to each of $a_1, a_2, \ldots, a_k$ and moreover $a_{k+1} > m > a_k$.

In this way we can construct arbitrarily many (and hence there are infinitely many) terms of the sequence $\{2^n - 3\}$ satisfying the condition of the problem.

3.6. Hint: First note that

$$\begin{aligned} t_n - 1 &= t_{n-1}(t_{n-1} - 1) \\ t_{n-1} - 1 &= t_{n-2}(t_{n-2} - 1) \\ &\cdots \\ t_2 - 1 &= t_1(t_1 - 1). \end{aligned}$$

Then show that the sequence is increasing, hence $t_n > 1$ for every n. Now, multiplying all inequalities above we get $t_n = 1 + t_1 t_2 \cdots t_{n-1}$.

Chapter 4

4.1. $[n, n+1] = \frac{n(n+1)}{(n,n+1)} = n(n+1)$.

4.2. Hint: note that $[m, n]$ is not 0, being equal to (m, n). Then $(m, n) \le m \le [m, n]$ and $(m, n) \le n \le [m, n]$.

4.3. Hint: $m = 10a$, $n = 10b$ and $100ab = mn = (m, n)[m, n] = 1000$, hence $ab = 10$.

4.4. See Problem 4.5 for $m = n + 1$.

4.5. Let $M_1 = [1, 2, \ldots, m, n, n+1, \ldots, n+m-1]$ and $M_2 = [n, n+1, \ldots, n+m-1]$. First, clearly $M_2 \mid M_1$. Now, in order to prove that $M_1 \mid M_2$ it is enough to notice that $[n, n+1, \ldots, n+m-1]$ is a common multiple of $1, 2, \ldots, m, n, n+1, \ldots, n+m-1$, which follows from the fact that for every $k = 1, 2, \ldots, m$, one of the numbers $n, n+1, \ldots, n+k-1$ is divisible by k (Problem 1.5).

Chapter 5

5.1. (a) We shall modufy Euclid's proof of Theorem 5.2. Suppose that there are finitely many primes of the form $4n+3$ and let $p_1, p_2, \ldots, p_k$ be all of them. Then consider the number

$$N = 4p_1p_2\cdots p_k + 3.$$

Since N is greater than each of $p_1, p_2, \ldots, p_k$ it must be composite. Then it has at least one prime divisor of the form $4n+3$ (why?). Now proceed as in the proof of Theorem 5.2.

(b) Similar to (a).

5.2. (a) Let p be a prime and $p = 30q + r$, $0 \le r < 30$. Suppose that r is neither 1 nor prime. Then r has a prime divisor not greater than $\sqrt{r} < 6$, i.e. 3 or 5. But 30 is divisible by both of them, hence so is p. Therefore p is 3 or 5 and $r = p$, hence r is prime, which is a contradiction.

(b) No. 109 is a prime, but $109 = 1 \cdot 60 + 49$.

5.3. Hint: Induction on n. Use the inequalities

$$p_n \le p_1p_2\cdots p_{n-1},$$

which follows from the proof of Theorem 5.2, and

$$2^1 + 2^2 + \cdots + 2^{n-1} < 2^n.$$

5.4. The number $n! - 1$ is not divisible by any of 2, 3, ..., n. Therefore it is either prime of has a prime divisor greater than n.

5.5. Suppose $p = mn$ where $m, n > 1$. Let $k = 2^m$. Then $2^p - 1 = 2^{mn} - 1 = (2^m)^n - 1 = k^n - 1 = (k-1)(k^{n-1} + \cdots + k + 1)$ and both factors are greater than 1. Therefore $2^p - 1$ is composite.

5.6. Suppose that $2^n + 1$ is prime and n is not a power of 2. Then n has some odd divisor $m > 1$: $n = qm$. Let $k = 2^q$. Then $2^n + 1 = 2^{qm} + 1 = k^m + 1 = (k+1)(k^{m-1} - k^{m-2} + \cdots - k + 1)$ and both factors are greater than 1 (why?), hence $2^n + 1$ is composite.

5.7. If $2^m - 1$ is a prime then the sum of proper divisors of $2^{m-1}(2^m - 1)$ is

$$\begin{aligned} S &= 1 + 2 + 2^2 + \cdots + 2^{m-1} + (2^m - 1) + 2(2^m - 1) + \cdots + 2^{m-2}(2^m - 1) \\ &= 2^m - 1 + (1 + 2 + 2^2 + \cdots + 2^{m-2})(2^m - 1) \\ &= (2^m - 1) + (2^{m-1} - 1)(2^m - 1) = 2^{m-1}(2^m - 1), \end{aligned}$$

hence $2^{m-1}(2^m - 1)$ is a perfect number. Conversely, let $n = 2^{m-1}(2^m - 1)$ be a perfect number. Since all terms in the sum S are divisors of n and $S = n$, they must be *all* divisors of n, hence $2^m - 1$ must be prime.

5.8. (a) If all inequalities hold, then clearly $m \mid n$. Conversely, if $m \mid n$, suppose that $\alpha_i > \beta_i$ for some i. Assume for convenience that $i = 1$. Then

$$p_1^{\beta_1} p_1^{\alpha_1 - \beta_1} \cdots p_k^{\alpha_k} \;\Big|\; p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k},$$

hence, by (D9), $p_1^{\alpha_1 - \beta_1} \cdots p_k^{\alpha_k} \;\Big|\; p_2^{\beta_2} \cdots p_k^{\beta_k}$ which implies $p_1 \mid p_2^{\beta_2} \cdots p_k^{\beta_k}$ since $\alpha_1 - \beta_1 > 0$.

But this means that p_1 divides some of $p_2, \ldots, p_k$ which is a contradiction to the fact that $p_1, p_2, \ldots, p_k$ are different primes.

(b) Follows easily from (a).

5.9. (a) Let $a = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$, $b = p_1^{\beta_1} \cdots p_k^{\beta_k}$ and $c = p_1^{\gamma_1} \cdots p_k^{\gamma_k}$, where some of the α's, β's and γ's can be 0. Then the probelm boils down to the identity $\min(a, \max(b, c)) = \max(\min(a, b), \min(a, c))$ which can be verified by inspection of all possible orderings of a, b and c.

The proofs of the other identities are similar.

5.10. Suppose that $m_1, \ldots, m_k$ are relatively prime in pairs and $(M_1, \ldots, M_n) > 1$. Then $M_1, \ldots, M_n$ have a common divisor p. Thus p divides $M_1 = m_2 \cdots m_n$ hence $p \mid m_i$ for some i. Then $p \nmid m_j$ for any $j \neq i$. Therefore $p \nmid M_i$ — a contradiction. Conversely, suppose that $(m_i, m_j) = d > 1$ for some $m_i \neq m_j$, $i \neq j$. Then $d \mid M_k$ for every $k \neq i$ and for every $k \neq j$, hence $d \mid M_k$ for every $k = 1, \ldots, n$.

5.11. Hint: Induction on k. When $k = 2$ the sequence $(n+1)! + 2, \ldots, (n+1)! + n, (n+1)! + (n+1)$ satisfies the condition. Suppose that for some k we have found numbers $N, N+1, \ldots, N+(n-1)$ with the desired property. Then for $k+1$ consider the sequence $(N + (n-1))! + N, (N + (n-1))! + (N+1), \ldots, (N + (n-1))! + (N + (n-1))$.

Chapter 6

6.1. Hints:

(a) if d is the units digit of n then $n \equiv d \pmod{10}$, hence $n^2 \equiv d^2 \pmod{10}$. Now consider $d^2 \pmod{10}$ for $d = 0, 1, \ldots, 9$.

(b) Similar.

6.2. Hint: consider

(a) $0^2, 1^2, \ldots, 7^2 \pmod 8$. Answer: 0, 1, 4;

(b) $0^3, 1^3, \ldots, 6^3 \pmod 7$. Answer 0, 1, 6.

6.3. Answers: (a) 4; (b) 3; (c) 7.

6.4. Hint: consider the possible remainders of $3n^2 - 5$ modulo 4 and use Problem 1.3.

6.5. Let $x - y = km$ for some integer k. Since $(x, m) \mid m$ and $(x, m) \mid x$ we have $(x, m) \mid x - km$, i.e. $(x, m) \mid y$. Then $(x, m) \mid (y, m)$. Likewise $(y, m) \mid (x, m)$. Therefore $(x, m) = (y, m)$.

6.6. Let $d_k d_{k-1} \cdots d_1 d_0$ be the decimal representation of n. Then $n = d_k \cdot 10^k + d_{k-1} \cdot 10^{k-1} + \cdots + d_1 \cdot 10 + d_0$. Now note that $10^m \equiv 1 \pmod 3$ for every natural number m, hence $n \equiv d_k + d_{k-1} + \cdots + d_1 + d_0 \pmod 3$.

Likewise $n \equiv d_k + d_{k-1} + \cdots + d_1 + d_0 \pmod 9$.

6.7. Let C be the sum of the digits of B. Since $4444^{4444} < 10000^{4444}$ the number of digits of 4444^{4444} is less than $4 \cdot 4444 + 1 < 20000$. Therefore $A < 9 \cdot 20000 = 180000$, hence $B < 9 \cdot 5 = 45$ (why?), so $C < 13$ (why?). Now, $4444 \equiv -2 \pmod 9$ and $(-2)^{4444} = 2^{3 \cdot 1481 + 1}$, hence $4444^{4444} \equiv 2 \cdot 8^{1481} \equiv 2 \cdot (-10)^{1841} \equiv -2 \equiv 7 \pmod 9$. Therefore $A \equiv 7 \pmod 9$, hence $B \equiv 7 \pmod 9$, hence $C \equiv 7 \pmod 9$ (by Problem 6.6). Then the only possible value of C is 7.

Chapter 7

7.1. 0, 3, 6, 9, 12, 15, 18. Hint: Use Theorem 7.1.

7.2. Hint: Use Fermat's theorem.

7.3. by Fermat's theorem $n^6 \equiv 1 \pmod 7$, hence $n^{30} = (n^6)^5 \equiv 1^5 \equiv 1 \pmod 7$.

7.4. $n^7 - n = n(n-1)(n+1)(n^2-n+1)(n^2+n+1)$. Now, $7 \mid n^7 - n$ (Problem 7.2) and $6 \mid n(n-1)(n+1)$ (Problem 3.3) hence $6 \mid n^7 - n$. Then, by Theorem 3.1 (4), $42 \mid n^7 - n$.

7.5. (a) By Fermat's theorem, $2^{10} \equiv 1 \pmod{11}$, hence $2^{11} \equiv 2 \pmod{11}$, so $2^{11 \cdot 31} \equiv 2^{31} \equiv (2^{10})^3 \cdot 2 \equiv 2 \pmod{11}$. Likewise $2^{30} \equiv 1 \pmod{31}$, hence $2^{31} \equiv 2 \pmod{31}$, so $2^{11 \cdot 31} \equiv 2^{11} \equiv (2^5)^2 \cdot 2 \equiv 2 \pmod{31}$ since $2^5 = 32 \equiv 1 \pmod{31}$.

(b) Similarly.

7.6. Answers: 1, 1, 2, 2, 4, 2, 6, 4, 6, 4, 10, 4, 12, 6, 8, 8.

7.7. (a) $2^1 \equiv 2 \pmod 7$, $2^2 \equiv 4 \pmod 7$, $2^3 \equiv 1 \pmod 7$, hence $2^{3k+r} \equiv 2^r \pmod 7$. Then $7 \mid 2^n - 1$ if and only if $2^n \equiv 1 \pmod 7$ if and only if $n = 3k$ for some integer k.

(b) Follows from (a).

Let us denote the sum by S. Notice that for every $k < n$ if $(k, n) = 1$ then $(n - k, n) = 1$. Then $2S = \sum_{m<n,(m,n)=1} m + (n - m)$ where m ranges on all $\phi(n)$ natural numbers less than n and relatively prime to n. Thus $2S = n\phi(n)$.

7.8. (a) n is composite if and only if $n = n_1 n_2$ for some integers n_1, n_2 such that $1 < n_1 < n$ and $1 < n_2 < n$. If $n_1 \neq n_2$ then they both occur as factors in $(n - 1)!$, hence $n_1 n_2 \mid (n - 1)!$. Otherwise $n_1 = n_2 = \sqrt{n} > 2$, hence $2n_1 < n$ and again $n_1 \cdot 2n_1 \mid (n - 1)!$

(b) For $n = 2, 3, 4$ the statement is verified by a direct inspection. Now, suppose that $n > 4$. If $(n - 1)! + 1 \equiv 0 \pmod n$ then n must be prime, by (a). Conversely, let n be prime. For every k between 2 and $n - 2$, $(k, n) = 1$, hence $k \cdot 0, k \cdot 1, \ldots, k(n - 1)$ is a complete residue system modulo n. Therefore there is exactly one m between 0 and $n - 1$ such that $k \cdot m \equiv 1 \pmod n$. This m cannot be 0, 1 or $n - 1$, otherwise $k \cdot m$ would be congruent respectively to 0, k and $p - k \neq 1$ modulo n. Moreover, id k_1 and k_2 are two different numbers between 2 and $n - 2$ and $1 \leq m \leq n - 1$ then $mk_1 \not\equiv mk_2 \pmod n$, otherwise $n \mid m(k_1 - k_2)$ which is impossible since $(n, m) = 1$ and $(n, k_1 - k_2) = 1$. Thus, the numbers $2, 3, \ldots, n - 2$ are grouped into pairs $\{k, m\}$ such that $km \equiv 1 \pmod 1$. Then $2 \cdot 3 \cdots (n - 2) \equiv 1 \pmod n$, hence $(n - 1)! = 1 \cdot 2 \cdot 3 \cdots (n - 2)(n - 1) \equiv n - 1 \equiv -1 \pmod n$.

(c) If the last three digits in the decimal record of 1978^m and 1978^n coincide then $1000 \mid (1978^n - 1978^m)$, i.e. $2^3 \cdot 5^3 \mid 1978^m(1978^{n-m} - 1)$. Then $2^3 \mid 1978^m$ because $1978^{n-m} - 1$ is odd. Therefore $m \geq 3$ since $1978 = 989 \cdot 2$. Further, by Euler's theorem $1978^{\phi(125)} = 1978^{100} \equiv 1 \pmod{5^3}$, i.e. $5^3 \mid 1978^{100} - 1$. Denote the minimal possible value of $n - m$ for which $5^3 \mid (1978^{n-m} - 1)$ by k. We are going to show that $k = 100$. First, by Theorem 7.3, $k \mid 100$. Further, by Fermat's theorem, $1978^4 \equiv 1 \pmod 5$ and $1978^2 \equiv 3^2 \equiv 4 \pmod 5$, hence 4 is the minimal positive integer r for which $5 \mid 1978^r - 1$. Therefore $4 \mid k$, hence the possible values of k are 4, 20 and 100l Now, $1978 \equiv (-22) \pmod{125}$, hence
$1978^2 \equiv (-22)^2 = 484 \equiv -16 \pmod{125}$, hence
$1978^4 \equiv (-16)^2 = 256 \equiv 6 \pmod{125}$. Therefore
$1978^{20} \equiv 6^5 = 7776 \equiv 26 \pmod{125}$. Thus, k must be 100. Therefore $n - m \geq 100$ and $m \geq 3$ which imply that the required values of m and n are $m = 3$ and $n = 103$.

Chapter 8

8.1. (a) $x \equiv 13 \pmod{16}$; (b) $x \equiv 3 \pmod{104}$; (c) no solutions.

8.2. (a) 30; (b) 111; (c) 1001.

8.3. Induction on n. If $n = 2$ the statement is true. Suppose that it is true for every $n - 1$ arithmetic progressions satisfying the condition of the problem and let n arithmetic progressions be given with differences $d_1, \ldots, d_n$. Then the first $n - 1$ progressions have a common term t. We may assume that $t = 0$, otherwise we subtract t from every term of each of the n progressions and consider the resulting ones. Obviously if they have a common term then the original ones have a common term, too.Thus we may regard that the first $n - 1$ progressions are of the kind $\{kd_i\}$, $i = 1, 2, \ldots, n - 1$ and k is an integer. Let the n-th progression be of the kind $\{a + kd_n\}$. Then there are natural numbers $k_1, \ldots, k_{n-1}$ and $q_1, \ldots, q_{n-1}$ such that

$$\begin{array}{rcll} a + q_1 d_n & = & k_1 d_1 & (1) \\ a + q_2 d_n & = & k_2 d_2 & (2) \\ & \cdots & & \\ a + q_{n-1} d_n & = & k_{n-1} d_{n-1}. & (\text{n-1}) \end{array}$$

Let $M = [d_1 \ldots, d_{n-1}]$ and $m_i = \frac{M}{d_i}$, $i = 1, \ldots, n - 1$. Then $(m_1, \ldots, m_{n-1}) = 1$ (Problem 5.10), hence $u_1 m_1 + \cdots + u_{n-1} m_{n-1} = 1$ for some integers $u_1, \ldots, u_{n-1}$. Now summing $u_1 m_1$ times (1), $u_2 m_2$ times (2), etc. $u_{n-1} m_{n-1}$ times $(n - 1)$, we get

$$a(u_1 m_1 + \cdots + u_{n-1} m_{n-1}) + qd_n = (k_1 u_1 + \cdots + k_{n-1} u_{n-1})M.$$

Therefore $a + qd_n \equiv 0 \pmod{M}$, hence $a + qd_n$ is a common term of all n progressions.

8.4. Given the arithmetic progression $a, a+d, a+2d, \ldots$ where a and d are natural numbers, take primes $p_1, \ldots, p_k$ such that $d < p_1 < \cdots < p_k$. Then $p_1^2, \ldots, p_k^2$ are relatively prime in pairs, hence by the Chinese Remainder Theorem there exists a positive x such that $dx \equiv -a - dj \pmod{p_j^2}$, i.e. $a+d(x+j) \equiv 0 \pmod{p_j^2}$, for $j = 1, \ldots, k$. Then obviously the numbers $a+d(x+j)$ are composite.

8.5. Let n be a fixed natural number and p_k be the k-th prime. Then $p_1 p_2 \cdots p_n$, $p_{n+1} p_{n+2} \cdots p_{2n}$, and $p_{2n+1} p_{2n+2} \cdots p_{3n}$ are relatively prime in pairs, hence there is an integer x such that $x \equiv -2 \pmod{p_1 p_2 \cdots p_n}$, $x \equiv -1 \pmod{p_{n+1} p_{n+2} \cdots p_{2n}}$ and $x \equiv -2 \pmod{p_{2n+1} p_{2n+2} \cdots p_{3n}}$. Now consider the arithmetic progression $x + p_1 p_2 \cdots p_{3n} m$, $m \in \mathbb{N}$. Since $(p_1 p_2 \cdots p_{3n}, x) = 1$ (why?) by Dirichlet's theorem 5.6, there is a prime $p = x + p_1 p_2 \cdots p_{3n} m$ for some natural m. Then $p-1$, $p-1$ and $p+2$ will have n different prime divisors each, namely $\{p_1, p_2, \ldots, p_n\}$, $\{p_{n+1}, p_{n+2}, \ldots, p_{2n}\}$ and $\{p_{2n+1}, p_{2n+2}, \ldots, p_{3n}\}$ respectively.

Additional Problems

1. Show that for every odd natural number n, $48 \mid n^3 + 3n^2 - n - 3$.
2. Prove that for every natural number n, $25 \mid 2^{n+1} 3^n + 5n - 4$.
3. Prove that $m \mid ab^n + cn + d$ for every integer $n \geq 0$ if and only if $m \mid a + d$, $m \mid (b-1)c$ and $m \mid a(b-1) + c$.
4. Show that the fraction $\frac{a^3+2a}{a^4+3a^2+1}$ is irreducible.
5. If $(a, b) = 1$ show that $(a+b, a^2 - ab + b^2)$ is either 1 or 3. If a, b and c are odd integers, prove that
$$(a, b, c) = (\frac{a+b}{2}, \frac{b+c}{2}, \frac{c+a}{2}).$$
6. Prove that for any integers a, b and c,
$$(a, b) = (a + bc, a + b(c-1)).$$
7. Show that $56786730 \mid mn(m^{60} - n^{60})$ for any integers m and n.
8. Find all three-digit numbers n such that the number formed from the last three digits of any power of n equals n.
9. Let m and n be natural number. Show that $(m, n) = 1$ if and only if $(2^m - 1, 2^n - 1) = 1$.
10. Let a, b, m, n be natural numbers such that $a > 1$ and $(a, b) = 1$. Prove that if $a^m + b^m \mid a^n + b^n$ then $m \mid n$.
11. Prove that amongst any 16 consecutive integers there is one which is relatively prime to each of the others.
12. Show that for wny integers a and b,
$$(a, b) = (a + b, [a, b]).$$
13. Prove that if m and n are relatively prime natural numbers such that mn is a perfect k-th power for some $k \geq 2$, then m and n are perfect k-th powers.
14. Find all pairs of natural numbers $\{x, y\}$ satisfying the equation
$$2^x = 3^y + 5.$$
15. N is a sum of the eight powers of 100 consecutive natural numbers. Find the last digit of N.

16. Prove that

    (a) $7 \mid (2222^{5555} + 5555^{2222})$;

    (b) $343 \mid 2^{147} - 1$.

17. Find the last two digits of $2^{999} + 3^{999}$.

18. Find the remainder modulo 7 of

$$10^{10} + 10^{(}10^{2}) + \cdots + 10^{(10^{10})}.$$

19. Let a, b, n be natural number such that for any natural $k \neq b$, $k - b \mid k^n - a$. Show that $a = b^n$.

20. Show that $1^2, 2^2, \ldots, m^2$ is not a complete residue system modulo m if $m > 2$.

21. For any prime p other than 2 and 5 prove that p divides infinitely many of the integers 1, 11, 111, ...

22. Find all natural number n such that $\phi(n) = 24$.

23. Find all natural numbers n such that $n \mid \phi(n)$.

24. If $d \mid n$ and $0 < d < n$ prove that $n - \phi(n) > d - \phi(d)$.

25. Prove that fo any integer a and natural number m,

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

    (A generalization of Euler's theorem.)

26. If p is a prime and $h, k \geq 0$ are integers such that $h + k = p - 1$, show that $h!k! + (-1)^h \equiv 0 \pmod{p}$.

27. If a and n are natural numbers and p is a prime such that $(a, p) = 1$ and $(n, p-1) = 1$, show that there is exactly one integer x between 1 and p such that $x^n \equiv a \pmod{p}$.

28. Let a and $n > 1$ be integers such that $a^{n-1} \equiv 1 \pmod{n}$ but $a^x \not\equiv 1 \pmod{n}$ for every proper divisor x of $n - 1$. Show that n is a prime.

29. Let k, m and n be natural numbers and $(k, m) = 1$ Show that there is an integer x such that $(k + mx, n) = 1$.

30. Show that for all natural numbers k and m the number $2k$ can be represented as a difference of two natural numbers relatively prime to m.

31. Prove that there exists a natural number k such that $k \cdot 2^n + 1$ is composite for every natural number n.

32. (*Problem 3 from the 24th IMO in France, 1983*) Let a, b and c be positive integers, no two of which have a common divisor greater than 1. Show that $2abc - ab - bc - ca$ is the largest integer which cannot be expressed in the form $xbc + yca + zab$ where x, y and z are non-negative integers.

33. (*Problem 2 from the 25th IMO in Czechoslovakia, 1984*) Find one pair of positive integers a and b such that:

    (i) $ab(a + b)$ is not divisible by 7;

    (ii) $(a + b)^7 - a^7 - b^7$ is divisible by 7^7. Justify your answer.

34. (*Problem 6 from the 25th IMO in Czechoslovakia, 1984*) Let a, b, c and d be odd integers such that $0 < a < b < c < d$ and $ad = bc$. Prove that if $a + d = 2^k$ and $b + c = 2^m$ for some integers k and m, then $a = 1$.

35. (*Problem 6 from the 28th IMO in Cuba, 1987*) Let n be an integer greater than or equal to 2. Prove that if k^2+k+n is prime for all integers k such that $0 \leq k \leq \sqrt{n/3}$ then k^2+k+n is prime for all integers k such that $0 \leq k \leq n-2$.

36. (*Problem 6 from the 29th IMO in Australia, 1988*) Let a and b be positive integers such that $ab+1$ divides a^2+b^2. Show that $\frac{a^2+b^2}{ab+1}$ is the square of an integer.

37. (*Problem 3 from the 31th IMO in China, 1990*) Find all $n > 1$ such that $\frac{2^n+1}{n^2}$ is an integer, where $n \in \mathbb{N}$.

38. (*Problem 5 from the 31th IMO in China, 1990*) A game if played between two people as follows: $n_0 \in \mathbb{N}$ is chosen. Given n_{2k}, A chooses $n_{2k+1} \in \mathbb{N}$ such that $n_{2k} \leq n_{2k+1} \leq (n_{2k})^2$. Given n_{2k+1}, B chooses $n_{2k+2} \in \mathbb{N}$ such that $\frac{n_{2k+1}}{n_{2k+2}}$ is a power of a prime. A wins by choosing 1990, B wins by choosing 1.

    For what values of n_0 does A win, B win and nobody win, respectively?

39. (*Problem 2 from the 32th IMO in Sweden, 1991*) Let $n > 6$ be an integer and $a_1, a_2, \ldots, a_k$ be all the natural numbers lee than n and relatively prime to n. If

$$a_2 - a_1 = a_3 - a_2 = \cdots = a_k - a_{k-1} > 0,$$

    prove that n must be either a prime number or a power of 2.

40. (*Problem 1 from the 33th IMO in Russia, 1992*) Find all integers a, b, c with $1 < a < b < c$ such that $(a-1)(b-1)(c-1)$ is a divisor of $abc-1$.