New Zealand Mathematical Olympiad Committee

Divisibility and Primes

Arkadii Slinko

1 Introduction

The theory of numbers is devoted to studying the set $\mathbb{N} = \{1, 2, 3, 4, 5, 6, \ldots\}$ of positive integers, also called the *natural numbers.* These notes, the first in a series of tutorials on number theory, explore $\mathbb{N}$'s most fundamental properties.

The set of all integers

$$\ldots, -3, -2, -1, 0,\ 1,\ 2,\ 3, \ldots$$

is denoted by $\mathbb{Z}$. In this section letters of the Roman alphabet

$$a, b, c, \ldots, k, l, m, n, \ldots, x, y, z$$

designate integers unless otherwise specified.

The most important property of $\mathbb{N}$ is the following axiom (which means that it cannot be proved):

Axiom (Least-Integer Principle)**.** *A non-empty set $S \subseteq \mathbb{N}$ of positive integers contains a smallest element.*

Theorem 1 (Division algorithm)**.** *Given any integers a, b, with $a > 0$, there exist unique integers q, r such that*

$$b = qa + r, \qquad 0 \leq r < a.$$

The number q is called the *quotient* and the number r is called the *remainder.* The notation $r \equiv b \pmod{a}$ is often used.

Example 1. $35 \equiv 3 \cdot 11 + 2$, $-51 \equiv (-8) \cdot 7 + 5$; so that $2 \equiv 35 \pmod{11}$ and $5 \equiv -51 \pmod{7}$.

An integer b is *divisible* by an integer $a \neq 0$, if there exists an integer c such that $b = ac$. Equivalently, b is divisible by a if $0 = b \pmod{a}$. We also say that a is a *divisor* of b and write $a|b$.

Let n be a positive integer. Let us denote by $d(n)$ the number of divisors of n. It is clear that 1 and n are always divisors of a number n which is greater than 1. Thus we have $d(1) = 1$ and $d(n) \geq 2$ for $n > 1$.

An integer n is called a *prime* if $d(n) = 2$. An integer $n > 1$, which is not prime is called a *composite* number.

Example 2. $2, 3, 5, 7, 11, 13$ are primes; $1, 4, 6, 8, 9, 10$ are not primes; $4, 6, 8, 9, 10$ are composite numbers.

Example 3. Prove that the set of all primes $P = \{p \mid p > 2\}$ is split into two disjoint classes: primes of the form $4k + 1$ and primes of the form $4k + 3$. Similarly, show that P can be split another pair of disjoint classes: primes of the form $6k + 1$ and primes of the form $6k + 5$.

Solution: We will prove the second statement. Let $p > 2$ be a prime. Let us divide it by 6 with remainder: $p = 6k + r$, where $r = 0, 1, 2, 3, 4, 5$. When r takes values $0, 2, 3, 4$ the right-hand-side is divisible by 2 or 3, hence in this case p cannot be a prime. □

Exercise 1. Prove that any prime of the form $3k + 1$ is of the form $6k + 1$ (but for another k, of course).

2 Prime factorization

Theorem 2 (Fundamental Theorem of Arithmetic)**.** *Every positive integer $n > 1$ can be expressed as a product of primes (with perhaps only one factor), that is*

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r},$$

where $p_1, p_2, \dots, p_n$ are distinct primes and $\alpha_1, \alpha_2, \dots, \alpha_n$ are positive integers. This factoring is unique apart from the order of the prime factors.

Proof. Let us prove first that any number $n > 1$ can be decomposed into a product of primes. If $n = 2$, the decomposition is trivial and we have only one factor, i.e., 2 itself. Let us assume that for all positive integers, which are less than n, a decomposition exists. If n is a prime, then $n = n$ is the decomposition required. If n is composite, then $n = n_1 n_2$, where $n > n_1 > 1$ and $n > n_2 > 1$ and by the induction hypothesis there are prime decompositions $n_1 = p_1 \dots p_r$ and $n_2 = q_1 \dots q_s$ for n_1 and n_2. Then we may combine them

$$n = n_1 n_2 = p_1 \dots p_r q_1 \dots q_s$$

and get the decomposition for n and prove the first statement.

To prove that the decomposition is unique, we shall assume the existence of an integer capable of two essentially different prime decompositions, and from this assumption derive a contradiction. This will show that the hypothesis that there exists an integer with two essentially different prime decompositions is untenable, and hence the prime decomposition of every integer is unique. We will use the Least-Integer Principle.

Suppose that there exists an integer with two essentially different prime decompositions. Then there will be a smallest such integer

$$n = p_1 p_2 \dots p_r = q_1 q_2 \dots q_s, \tag{1}$$

where p_i and q_j are primes. By rearranging the order of the p's and the q's, if necessary, we may assume that

$$p_1 \le p_2 \le \dots \le p_r, \qquad q_1 \le q_2 \le \dots \le q_s.$$

It is impossible that $p_1 = q_1$, for if it were we could cancel the first factor from each side of equation (1) to obtain two essentially different prime decompositions for a number smaller than n, contradicting the choice of n. Hence either $p_1 < q_1$ or $q_1 < p_1$. Without loss of generality we suppose that $p_1 < q_1$.

We now form the integer

$$n' = n - p_1 q_2 q_3 \dots q_s. \tag{2}$$

Then two decompositions of n give the following two decompositions of n':

$$n' = (p_1 p_2 \dots p_r) - (p_1 q_2 \dots q_s) = p_1(p_2 \dots p_r - q_2 \dots q_s), \tag{3}$$

$$n' = (q_1 q_2 \dots q_s) - (p_1 q_2 \dots q_s) = (q_1 - p_1)(q_2 \dots q_s). \tag{4}$$

Since $p_1 < q_1$, it follows from (4) that n' is a positive integer, which is smaller than n. Hence the prime decomposition for n' must be unique and, apart from the order of the factors, (3) and (4) coincide. From (3) we learn that p_1 is a factor of n' and must appear as a factor in decomposition (4). Since $p_1 < q_1 \le q_i$, we see that $p_1 \ne q_i$, $i = 2, 3, \dots, s$. Hence, it is a factor of $q_1 - p_1$, i.e., $q_1 - p_1 = p_1 m$ or $q_1 = p_1(m + 1)$, which is impossible as q_1 is prime and $q_1 \ne p_1$. This contradiction completes the proof of the Fundamental Theorem of Arithmetic. □

Exercise 2. Prove that any positive integer of the form $3k + 2$ has a prime factor of the same form; similarly for each positive integer of the form $4k + 3$ and of the form $6k + 5$.

Exercise 3. Show that every divisor d of

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r},$$

is of the form

$$d = p_1^{\beta_1} p_2^{\beta_2} \dots p_r^{\beta_r},$$

where $\beta_i \le \alpha_i$ for all i. In particular

$$d(n) = (\alpha_1 + 1)(\alpha_2 + 1) \dots (\alpha_r + 1).$$

Exercise 4. Find the smallest positive integer n with $d(n) = 8$.

Any two numbers which do not have common primes in their prime factorisations are called *coprime* or *relatively prime*.

Let x be a real number. Then it can be written in a unique way as $z + e$, where $z \in \mathbb{Z}$ and $0 \le e < 1$. The following notation is used: $z = \lfloor x \rfloor$, $z + 1 = \lceil x \rceil$, $e = \{x\}$. We will use here only the first function $\lfloor x \rfloor$, which is called *the integral part* of x.

Example 4. $\lfloor -2.5 \rfloor = -3$, $\lfloor \pi \rfloor = 3$, $\lfloor 5 \rfloor = 5$.

Theorem 3. *The smallest prime divisor of a composite number n is less than or equal to $\lfloor \sqrt{n} \rfloor$.*

Proof. We prove first that n has a divisor which is greater than 1 but less than $\sqrt{n}$. As n is composite, then $n = d_1 d_2$, $d_1 > 1$ and $d_2 > 1$. If $d_1 > \sqrt{n}$ and $d_2 > \sqrt{n}$, then

$$n = d_1 d_2 > (\sqrt{n})^2 = n,$$

a contradiction. Suppose, $d_1 \le \sqrt{n}$. Then any of the prime divisors of d_1 will be less than or equal to $\sqrt{n}$. But every divisor of d_1 is also a divisor of n, thus the smallest prime divisor p of n will satisfy the inequality $p \le \sqrt{n}$. Since p is an integer, $p \le \lfloor \sqrt{n} \rfloor$. The theorem is proved. □

Exercise 5. A composite number n does not have prime divisors which are less than or equal to $[\sqrt[3]{n}]$. Prove that it is either a product of two distinct primes or the square of a prime.

Example 5. Given n pairwise relatively prime positive integers, greater than 1 but smaller than $(2n-1)^2$, prove that at least one of them is prime.

Solution: Let $a_1, a_2, \dots, a_n$ be the numbers and suppose that they are all composite. Let p_i be the smallest prime divisor of a_i. Since a_i is composite, we must have $p_i \le \sqrt{a_i} < 2n - 1$. There are $n - 2$ odd numbers which are greater than 1 and smaller than $2n - 1$. Since p_i is either odd or 2, we have $n - 1$ boxes, i.e. possibilities, for it. But we have n such primes to go into these boxes. Thus by the Pigeonhole Principle we obtain a contradiction. □

3 Infinitude and distribution of primes

Theorem 4 (Euclid). *The number of primes is infinite.*

Proof. Suppose there were only a finite number of primes $p_1, p_2, \dots, p_r$. Then form the integer

$$n = 1 + p_1 p_2 \dots p_r.$$

Since $n > p_i$ for all i, it must be composite. Let q be the smallest prime factor of n. As $p_1, p_2, \dots, p_r$ represent all existing primes, then q is one of them, say $q = p_1$ and $n = p_1 m$. Now we can write

$$1 = n - p_1 p_2 \dots p_r = p_1 m - p_1 p_2 \dots p_r = p_1 (m - p_2 \dots p_r).$$

We have got that $p_1 > 1$ is a factor of 1, which is a contradiction. □

Proof. Here is an alternative proof, using a very important idea in number theory: to compare how fast two things grow as $n \to \infty$. We assume on the contrary that there are only finitely many primes $p_1, p_2, \dots p_5$. Then we know that any number can be represented in the form

$$p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}, \tag{5}$$

Let us estimate how many such prime factorizations we might have available to represent numbers smaller than or equal to n. Without loss of generality we assume that $p_1 < p_2 < \dots < p_r$. Then $p_1 = 2$ and $\alpha_i \le \log_2 n$, since if $\alpha_i > \log_2 n$, then $p_i^{\alpha_i} > p_1^{\alpha_i} > 2^{\log_2 n} = n$. Therefore, each α_i can take no more than $\log_2 n + 1$ different values, hence we get no more than $(\log_2 n)^r$ possible prime factorizations (5) for numbers smaller than n. Since $(\log_2 n)^r$ grows much slower than n (proving that needs a wee bit of calculus), we get a contradiction. □

The distribution of primes is quite irregular. In particular, there are arbitrarily large gaps in the series of primes.

Example 6. Given a positive integer k, prove that there exist k consequtive composite integers.

Solution: Consider the integers

$$(k+1)! + 2,\ (k+1)! + 3,\ \dots,\ (k+1)! + k,\ (k+1)! + (k+1)$$

Each of them is composite, since $(k+1)! + m$ is divisible by m. □

Nevertheless there are still quite a few primes, as the following theorem shows. Its proof is difficult but still elementary, and is covered in Tutorial 5.

Theorem 5 (Bertrand's Postulate, proved by Chebyschef)**.** *For every positive integer $n > 1$ there is a prime p such that $n < p < 2n$.*

This is a marvelous tool for solving math olympiad problems. Just look at the following example.

Example 7. Prove that $n! = m^k$ has no solutions in integers $k > 1$, $m > 1$, $n > 1$.

Solution: Let p be the largest prime such that $p \le n$. Since by Bertrand's Postulate there is a prime q such that $p < q \le 2p$, we must have $2p \ge q > n$. Therefore n is not divisible by p^2, and $n!$ is not divisible by p^2 either. Thus $k = 1$ which is a contradiction. □

The following three theorems are far from being elementary. Of course, no Jury assumes that students are familiar with these theorems. Nevertheless, some students use them and sometimes a difficult math olympiad problem can be trivialised by doing so. The attitude of the Jury of the International Mathematical Olympiad is to believe that students know what they use. Therefore it pays to understand the statements of these results, even without proof.

Theorem 6. *Let p_i be the ith prime. Then*

$$\frac{1}{p_1} + \frac{1}{p_2} + \dots + \frac{1}{p_n} \longrightarrow \infty$$

as $n \to \infty$.

Theorem 7 (Dirichlet's Theorem)**.** *If a and b are relatively prime positive integers (which means that they don't have common prime factors in their prime factorisations), then there are infinitely many primes of the form $an + b$, where $n = 1, 2, \dots$.*

Let $\pi(x)$ denote the number of primes which do not exceed x. Because of the irregular distribution of the primes, we cannot expect a simple formula for $\pi(x)$. However one of the most impressive results in advanced number theory gives an asymptotic approximation for $\pi(x)$.

Theorem 8 (Prime Number Theorem)**.**

$$\lim_{x \to \infty} \pi(x) \frac{\ln x}{x} = 1,$$

where $\ln x$ is the natural logarithm, to base e.

4 Problems

1. Prove that the remainder of the square of a prime $p > 3$ on dividing by 24 is 1.

2. Twin primes are pairs of primes differing by 2. Show that 5 is the only prime belonging to two such pairs. Show also that there is a one-to-one correspondence between twin primes and positive integers n such that $d(n^2 - 1) = 4$, where as above $d(k)$ stands for the number of divisors of k.

3. Prove that, for all $n \geq 2$, the last decimal digit (the digit in the units place) of the number $2^{2^n} + 1$ is 7.

4. Find the smallest positive integer n such that $n/2$ is a square, $n/3$ is a cube and $n/5$ is a fifth power.

5. Prove that the equation
$$x^2 + x + 1 = py$$
has integer solutions for infinitely many primes p. (**Hint:** Follow the Euclid proof of infinitude of primes as closely as possible.)

6. Prove that there are infinitely many primes
   (a) of the form $4n + 3$;
   (b) of the form $6n + 5$.

January 27, 2009
http://www.mathsolympiad.org.nz