



Numbers involved in this book are integers, and letters used in this book stand for integers without further specification.

Given numbers a and b , with $b \neq 0$, if there is an integer c , such that $a = bc$, then we say b divides a , and write $b | a$. In this case we also say b is a *factor* of a , or a is a *multiple* of b . We use the notation $b \nmid a$ when b does not divide a (i. e., no such c exists).

Several simple properties of divisibility could be obtained by the definition of divisibility (proofs of the properties are left to readers).

(1) If $b | c$, and $c | a$, then $b | a$, that is, divisibility is transitive.

(2) If $b | a$, and $b | c$, then $b | (a \pm c)$, that is, the set of multiples of an integer is closed under addition and subtraction operations.

By using this property repeatedly, we have, if $b | a$ and $b | c$, then $b | (au + cv)$, for any integers u and v . In general, if a_1, a_2, \dots, a_n are multiples of b , then $b | (a_1 + a_2 + \dots + a_n)$.

(3) If $b | a$, then $a = 0$ or $|a| \geq |b|$. Thus, if $b | a$ and $a | b$, then $|a| = |b|$.

Clearly, for any two integers a and b , a is not always divisible by b . But we have the following result, which is called the division algorithm. It is the most important result in elementary number theory.

(4) (The division algorithm) Let a and b be integers, and $b > 0$. Then there is a unique pair of integers q and r , such that

$$a = bq + r \text{ and } 0 \leq r < b.$$

The integer q is called the (incomplete) *quotient* when a is divided by b , r called the *remainder*. Note that the values of r has b kinds

of possibilities: $0, 1, \dots, b - 1$. If $r = 0$, then a is divisible by b .

It is easy to see that the quotient q in the division algorithm is in fact $\left[\frac{a}{b} \right]$ (the greatest integer not exceeding $\frac{a}{b}$), and the heart of the division algorithm is the inequality about the remainder r : $0 \leq r < b$. We will go back to this point later on.

The basic method of proving $b \mid a$ is to factorize a into the product of b and another integer. Usually, in some basic problems this kind of factorization can be obtained by taking some special value in algebraic factorization equations. The following two factorization formulae are very useful in proving this kind of problems.

(5) if n is a positive integer, then

$$x^n - y^n = (x - y)(x^{n-1} + x^{n-2}y + \dots + xy^{n-2} + y^{n-1}).$$

(6) If n is a positive odd number, then

$$x^n + y^n = (x + y)(x^{n-1} - x^{n-2}y + \dots - xy^{n-2} + y^{n-1}).$$

Example 1 Prove that $\underbrace{10 \dots 01}_{200}$ is divisible by 1001.

Proof By factorization formula (6), we have

$$\begin{aligned} \underbrace{10 \dots 01}_{200} &= 10^{201} + 1 = (10^3)^{67} + 1 \\ &= (10^3 + 1)[(10^3)^{66} - (10^3)^{65} + \dots - 10^3 + 1]. \end{aligned}$$

Therefore, $10^3 + 1 (= 1001)$ divides $\underbrace{10 \dots 01}_{200}$.

Example 2 Let $m > n \geq 0$, show that $(2^{2^n} + 1) \mid (2^{2^m} - 1)$.

Proof Take $x = 2^{2^{n+1}}$, $y = 1$ in factorization (5), and substitute n by 2^{m-n-1} , we get

$$2^{2^m} - 1 = (2^{2^{n+1}} - 1)[(2^{2^{n+1}})^{2^{m-n-1}-1} + \dots + 2^{2^{n+1}} + 1].$$

Thus,

$$(2^{2^{n+1}} - 1) \mid (2^{2^m} - 1).$$

But

$$2^{2^{n+1}} - 1 = (2^{2^n} - 1)(2^{2^n} + 1).$$

Hence,

$$(2^{2^n} + 1) \mid (2^{2^{n+1}} - 1).$$

Further, by property (1) we have $(2^{2^n} + 1) \mid (2^{2^m} - 1)$.

Remark Sometimes it is difficult to prove $b \mid a$ directly when dealing with divisibility problems. Therefore, we can attempt to choose an “intermediate number” c and prove $b \mid c$ and $c \mid a$ first, then use the property (1) of divisibility to deduce the conclusion.

Example 3 For a positive integer n , write $S(n)$ to denote the sum of digits appearing in the expression of n in base 10. Show that $9 \mid n$ if and only if $9 \mid S(n)$.

Proof Write $n = a_k \times 10^k + \cdots + a_1 \times 10 + a_0$ (where $0 \leq a_i \leq 9$, and $a_k \neq 0$), then $S(n) = a_0 + a_1 + \cdots + a_k$. We have

$$n - S(n) = a_k(10^k - 1) + \cdots + a_1(10 - 1). \quad (1.1)$$

For $1 \leq i \leq k$, from factorization (5) we get $9 \mid (10^i - 1)$. So every term of the k terms in the right-hand side of equation (1.1) is a multiple of 9, thus property (2) implies that their sum is also a multiple of 9, that is, $9 \mid (n - S(n))$. Hence, the result can be obtained easily.

Remark 1 The divisibility property (2) provides an elementary method to prove $b \mid (a_1 + a_2 + \cdots + a_n)$. We can try to prove a stronger statement (which is usually easier to prove): b divides every a_i ($i = 1, 2, \dots, n$).

Of course this stronger statement does not always hold true. But even if it does not hold true, the above method is also useful. We can rewrite the sum $a_1 + a_2 + \cdots + a_n$ into $c_1 + c_2 + \cdots + c_k$ by regrouping the numbers, then we need to prove $b \mid c_i$ ($i = 1, 2, \dots, k$). Readers will find out that in order to solve some special problems, sometimes we can express a as a sum of certain numbers, and then apply the above method to prove it.

Remark 2 From the proof of Example 3 we actually obtain a stronger conclusion, that is, the difference between n and $S(n)$ is

always a multiple of 9. So n and $S(n)$ have the same remainder when divided by 9 (so we say n is congruent to $S(n) \pmod{9}$). Please refer to Chapter 6 for details).

Remark 3 In some cases from the properties of digits base 10 of a positive integer we can judge whether or not this integer is divisible by another integer. This kind of results sometimes are called “the digit character of divisibility”. The digit characters of an integer divisible by 2, 5 and 10 are well-known. In Example 3 we present the digit character of an integer divisible by 9. For this result there are many applications. In addition, in Exercise 1.3 the digit character of an integer divisible by 11 is given. This result is useful too.

Example 4 Let $k \geq 1$ be odd. Prove that for any positive integer n , $1^k + 2^k + \dots + n^k$ is not divisible by $n + 2$.

Proof When $n = 1$ the statement is obviously true. For $n \geq 2$, denote the sum by A , then

$$2A = 2 + (2^k + n^k) + (3^k + (n-1)^k) + \dots + (n^k + 2^k).$$

Since k is a positive odd number, from formula (6) we know that for every $i \geq 2$, $i^k + (n+2-i)^k$ is divisible by

$$i + (n+2-i) = n+2.$$

Thus $2A$ has remainder 2 when divided by $n+2$, which implies that A is not divisible by $n+2$ (note that $n+2 > 2$).

Remark In the proof we use the “pairing method” which is a common method to transform the expression of a sum.

Example 5 Let m and n be positive integers with $m > 2$. Prove that $(2^m - 1) \nmid (2^n + 1)$.

Proof At first, when $n \leq m$ it is easy to prove that the result is true. In fact, when $m = n$ the result is trivial. When $n < m$ from inequalities

$$2^n + 1 \leq 2^{m-1} + 1 < 2^m - 1,$$

we can get the result (note that $m > 2$ and refer to the divisibility property (3)).

Secondly, we can reduce the case $n > m$ to the special situation above: by the division algorithm, $n = mq + r$, $0 \leq r < m$, and $q > 0$. Since

$$2^n + 1 = (2^{mq} - 1)2^r + 2^r + 1,$$

we know $(2^m - 1) \mid (2^{mq} - 1)$ by factorization (5). But $0 \leq r < m$, from the discussion above we get $(2^m - 1) \nmid (2^n + 1)$ (note that when $r = 0$ the result is trivial). Hence, when $n > m$ we also have $(2^m - 1) \nmid (2^n + 1)$. The proof is complete.

Exercises

1.1 Let n and k be positive integers, then among numbers $1, 2, \dots, n$ there are exactly $\left[\frac{n}{k} \right]$ numbers which are divisible by k .

1.2 11 girls and n boys go to pick mushrooms. All the children pick $n^2 + 9n - 2$ mushrooms in total, and every child picks the equal number of mushrooms. Are there more girls or more boys among these children?

1.3 Let n be a positive number, and n can be expressed as $\overline{a_k \dots a_1 a_0}$ (where $0 \leq a_i \leq 9$, $a_k \neq 0$). Set

$$T(n) = a_0 - a_1 + \dots + (-1)^k a_k$$

(the alternating sum of the digits of n beginning with the units digit of n). Show that 11 divides $n - T(n)$, which implies that the digit character of an integer divisible by 11 is: 11 divides n if and only if 11 divides $T(n)$.

1.4 Suppose that there are n integers which have the following property: the difference between the product of any $n - 1$ integers and the remaining one is divisible by n . Prove that the sum of the square of these n numbers is also divisible by n .

1.5 Let a, b, c, d be integers with $ad - bc > 1$. Prove that there is at least one among a, b, c, d which is not divisible by $ad - bc$.