NUMBER THEORY

UNIT 1 DIVISIBILITY

1. Divisibility

Definition 1.1.

Let a and b be integers, $a \neq 0$. We say that ***a* divides *b***, denoted by $a \mid b$, if there exists an integer c such that $b = ca$. We also say 'b is divisible by a', 'b is a multiple of a' or 'a is a divisor of b'.

Illustrations. $2 \mid 6, -3 \mid 9, -5 \mid -10, \ 4 \mid 0, \ 3 \nmid 7, \ 0 \nmid 2$.

The following theorem gives some basic properties about divisibility which are trivial but useful.

Theorem 1.1.

Let a, b, c, x, y be integers.

(1) If $a \mid b$, then $a \mid xb$.

(2) If $a \mid b$ and $b \mid c$, then $a \mid c$.

(3) If $a \mid b$ and $a \mid c$, then $a \mid bx + cy$.

(4) If $a \mid b$, then $xa \mid xb$.

(5) If $a \mid b$, then $|a| \leq |b|$. In particular, if $a \mid b$ and $b \mid a$, then $a = \pm b$.

For practical as well as theoretical purposes, we often want to establish tests to see whether an integer is divisible by a certain number. For instance, to see whether a number is divisible by 4, we need only check whether the last two digits are divisible by 4. Take 123456 as an example. Since 56 is divisible by 4, we know that 123456 is also divisible by 4. Why is it so? This is because

$$123456 = 1234 \times 100 + 56.$$

Since $4 \mid 100$, 1234×100 is divisible by 4. Hence $4 \mid 123456$ if and only if $4 \mid 56$.

Noting that $2|10,\ 8|1000,\ 5|10,\ 25|100$, etc., we can easily establish similar divisibility tests for divisibility by 2, 8, 5, 25, etc.

How about divisibility by 3? We know that a number is divisible by 3 if and only if its sum of digits is divisible by 3. For instance, since

$$1+2+3+4+5+6=21$$

is divisible by 3, the number 123456 is divisible by 3. Why is it so? This is because

$$\begin{aligned}123456 &= 1\times100000+2\times10000+3\times1000+4\times100+5\times10+6\\ &= 1\times(99999+1)+2\times(9999+1)+3\times(999+1)+4\times(99+1)+5\times(99+1)+6\\ &= (1\times99999+2\times9999+3\times999+4\times99+5\times9)+(1+2+3+4+5+6)\end{aligned}$$

Since 9, 99, 999, etc. are all divisible by 3, the whole sum is the first pair of parentheses in the last row is divisible by 3, so $3|123456$ if and only if $3|1+2+3+4+5+6$.

In the same way we can establish divisibility tests for 9 and 11 (the latter needs a little modification, and we leave it to the exercises).

We also know that a number is divisible by 6 if and only if it is divisible by both 2 and 3, and that a number is divisible by 12 if and only if it is divisible by both 3 and 4. In general, if $p|n$, $q|n$, can we say that $pq|n$? If not, what can we say? You should be able to answer this question after studying this and the next section.

More divisibility tests will be discussed in the exercises.

Example 1.1.

(IMO 1990 HK Prelim) The six-digit number $\overline{a1989b}$ is divisible by 72. Determine *a* and *b*.

Solution.

Note that a number is divisible 72 if and only if it is divisible by both 8 and 9.

For the number to be divisible by 8, the last three digits $\overline{89b}$ are divisible by 8. It follows that *b* must be 6.

For the number to be divisible by 9, the sum of digits must be divisible by 9, i.e.

$$9|a+1+9+8+9+b=a+33.$$

Since *a* is between 1 and 9, we must have *a* = 3.

2. G.C.D. and L.C.M.

In this section we shall go over the familiar concepts of G.C.D. (or H.C.F.) and L.C.M., as well as some of their important properties.

Definition 2.1.

Let a and b be integers, not both zeros. The **greatest common divisor** (also called **highest common factor**, abbreviated as G.C.D. or H.C.F.) of a and b, denoted as gcd (a, b) or simply (a, b), is defined to be the largest integer which divides both a and b.

Illustrations. $(24, 36) = 12$, $(-8, 6) = 2$, $(2, -9) = 1$.

Definition 2.2.

Let a and b be non-zero integers. The **lowest common multiple** (abbreviated as L.C.M.) of a and b, denoted as lcm (a, b) or simply $[a, b]$, is defined to be the smallest positive integer which is divisible by both a and b.

Illustrations. $[24, 36] = 72$, $[-8, 6] = 24$, $[2, -9] = 18$.

The G.C.D. and L.C.M. of more than two integers can be similarly defined. The next theorem gives some basic properties of G.C.D. and L.C.M., which are easy to verify.

Theorem 2.1.

Let a, b, c and m be non-zero integers. Then

(1) $(ma, mb) = |m|(a, b)$

(2) $(a, m) = (b, m) = 1$ if and only if $(ab, m) = 1$.

(3) $c \mid ab$ and $(b, c) = 1$ imply $c \mid a$.

(4) $(a, b) = (b, a) = (a, b + ma)$

(5) $(a, b)[a, b] = |ab|$

In school we have learned various methods of computing the G.C.D. and L.C.M. of a given group of integers. Property (4) suggests a useful, simple and yet less commonly used way of computing the G.C.D. by the **Euclidean algorithm**. Before describing the algorithm, we need the following lemma, which is intrinsic in our mind.

Lemma 2.2.

Let a and b be integers, $a \neq 0$. There exist unique integers q and r such that

$$b = aq + r$$

with $0 \leq r < |a|$.

Illustration. Let $a = 13$, $b = 100$. Then $100 = 13 \times 7 + 9$ (i.e. $q = 7$, $r = 9$).

We are now ready to describe the Euclidean algorithm. For simplicity we assume that we are going to find the G.C.D. of two positive integers.

Theorem 2.3. (Euclidean algorithm)

Let a and b be positive integers, $a > b$. Then we apply a series of divisions as follows.

$$\begin{aligned}
a &= bq_0 + r_1 && 0 < r_1 < b \\
b &= r_1q_1 + r_2 && 0 < r_2 < r_1 \\
r_1 &= r_2q_2 + r_3 && 0 < r_3 < r_2 \\
&\vdots && \vdots \\
r_{n-2} &= r_{n-1}q_{n-1} + r_n && 0 < r_n < r_{n-1} \\
r_{n-1} &= r_nq_n
\end{aligned}$$

The process of division comes to an end when $r_{n+1} = 0$. The integer r_n is the G.C.D. of a and b.

Illustration. We try to find the G.C.D. of 2445 and 652. We have

$$\begin{aligned}
2445 &= 652 \times 3 + 489 \\
652 &= 489 \times 1 + 163 \\
489 &= 163 \times 3
\end{aligned}$$

Thus the G.C.D. of 2445 and 652 is equal to 163.

Corollary 2.4.

Let a and b be integers with $(a, b) = d$. There exist integers u and v such that

$$au + bv = d\ .$$

Such u, v can be obtained by backward tracing of the Euclidean divisions in finding the G.C.D.

Illustration. Let $a = 2445$, $b = 652$, as above. Tracing the Euclidean divisions, we have

$$163 = 652 - 489 = 652 - (2445 - 652 \times 3) = 2445(-1) + 652(4)\ .$$

Thus $u = -1$ and $v = 4$.

This 'tracing back' method is a bit inefficient, in the sense that we have been doing the same thing twice. A better method is described below.

Take the example of finding the G.C.D. of 2445 and 652 again. The process of taking Euclidean divisions can be summarized in a table below.

n	r_n	q_n
–1	2445	
0	652	3
1	489	1
2	163	3
3	0	

We start by writing $2445 = r_{-1}$ and $652 = r_0$ in the column 'r_n' which stores the 'remainders', and then we perform divisions, writing down the 'quotients' in the 'q_n' column and the 'remainders' in the 'r_n' column. As in Theorem 2.3, the r_n and q_n are related by

$$r_{n-1} = r_n q_n + r_{n+1},$$

as can be seen from the table.

To find u, v such that $au + bv = d$, the idea is to find u_n, v_n in each row such that

$$au_n + bv_n = r_n\ .$$

Since

$$\begin{cases} a(1)+b(0)=a \\ a(0)+b(1)=b \end{cases}$$

we set $u_{-1}=1,\ v_{-1}=0,\ u_0=0,\ v_0=1$. Moreover u_n and v_n satisfy the same recurrence relations,

$$\begin{cases} u_{n+1}=u_{n-1}-q_n u_n \\ v_{n+1}=v_{n-1}-q_n v_n \end{cases}.$$

because

$$\begin{aligned} r_{n+1} &= r_{n-1}-r_n q_n \\ &= \left(au_{n-1}+bv_{n-1}\right)-\left(au_n+bv_n\right)q_n \\ &= a\left(u_{n-1}-q_n u_n\right)+b\left(v_{n-1}-q_n v_n\right) \end{aligned}$$

When the Euclidean division ends with $r_{k+1}=0$, the values of u_k and v_k are the *u* and *v* we want.

Using our same old example, the process is illustrated in the table below.

n	r_n	q_n	u_n	v_n
–1	2445		1	0
0	652	3	0	1
1	489	1	1	–3
2	163	3	–1	4
3	0			

This is process is known as the **extended Euclidean algorithm**. In the row $n=2$ we see that

$$163 = 2445(-1)+652(4)$$

as desired.

Example 2.1.

In a country there are only $5 and $7 coins. If change is allowed, how can an amount of $12 be paid? How about $23? What integer amounts can be paid exactly?

Solution

To pay an amount of $\$N$ (where N is a positive integer), we need only find integers u, v such that

$$5u + 7v = N\ .$$

(Negative u or v means a change to be given.)

For the case of paying \$12, it is quite obvious that $u = v = 1$ works. So \$12 can be paid by one \$5 coin and one \$7 coin.

The case of paying \$23 is less obvious. Instead of mere observation, we can proceed systematically as follows. Using the (extended) Euclidean algorithm, we find that

$$5(-4) + 7(3) = 1.$$

Multiplying by 23,

$$5(-92) + 7(69) = 23\,.$$

So \$23 can be paid by paying sixty-nine \$7 coins and then asking for a change of ninety-two \$5 coins. Of course this is too bad, but we can improve it by observing that five \$7 coins have equal amount as seven \$5 coins. So one can pay $5 \times 13 = 65$ fewer \$7 coins, the number of \$5 coins to be given as change can be reduced by $7 \times 13 = 91$. Thus we get

$$5(-1) + 7(4) = 23\,,$$

i.e. \$23 can be paid by four \$7 coins with a change of one \$5 coin.

In general, since $5(-4) + 7(3) = 1$, we have $5(-4N) + 7(3N) = N$ for any integer N. So any integer amount can be paid.

Example 2.3.

(IMO 1959) Prove that the fraction $\dfrac{21n+4}{14n+3}$ is irreducible for every natural number n.

Solution.

By (4) of Theorem 2.1, we have $(21n+4, 14n+3) = (7n+1, 14n+3) = (7n+1, 1) = 1$ for every natural number n. This means that $21n+4$ and $14n+3$ have no common divisor, and hence the fraction is irreducible.

3. Primes

As we remarked in the introduction, prime numbers are important in the sense that they 'generate' all the positive integers. In this section, we will study the properties concerning prime numbers.

Definition 3.1.

An integer $p > 1$ is said to be **prime** if it has no positive divisors other than 1 and itself. Two or more integers are said to be **relatively prime** or **co-prime** if their G.C.D. is 1, and **pairwise relatively prime** if the G.C.D. of any two of them is 1.

Illustrations. 23, 37 are primes. 8 and 9 are relatively prime. 4, 5, 6 are relatively prime but not pairwise relatively prime. 8, 9, 11 are both relatively prime and pairwise relatively prime.

In school, we learnt to express positive integers as products of prime factors. Indeed, we have the following theorem which guarantees the existence and uniqueness of such expression.

Theorem 3.1. (The Fundamental Theorem of Arithmetic)

Every integer $n > 1$ can be expressed as a product of primes. Such an expression is unique up to permutation of the prime factors.

Illustrations. $90 = 2 \times 3 \times 3 \times 5$, $1998 = 2 \times 3 \times 3 \times 3 \times 37$.

Remark. It is customary to use index notation in the prime factorization of an integer. So we usually write $90 = 2 \times 3^2 \times 5$ and $1998 = 2 \times 3^3 \times 37$.

The above theorem is as important in its own right as in its applications. In many contexts we will have to consider the prime factorizations of certain integers in solving a problem. The following theorem is one of the important results concerning prime factorizations.

Theorem 3.2.

Let *m* and *n* be positive integers greater than 1 with prime factorizations

$$m = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k} \text{ and } n = p_1^{b_1} p_2^{b_2} \cdots p_h^{b_h}.$$

(1) *n* divides *m* if and only if $b_j \le a_j$ for all *j* (we regard the power to be 0 if a prime number is not in the prime factorization).

(2) *m* has exactly $(a_1+1)(a_2+1)\cdots(a_k+1)$ positive divisors. Each corresponds to a choice of the power c_j of the prime number p_j satisfying $0 \le c_j \le a_j$ for all *j*.

(3) The sum of the positive factors of *m* is

$$(1+p_1+p_1^2+\cdots+p_1^{a_1})(1+p_2+p_2^2+\cdots+p_2^{a_2})\cdots(1+p_k+p_k^2+\cdots+p_k^{a_k}).$$

Proof.

(1) Obvious.

(2) In view of (1), every positive divisor of *m* is of the form

$$p_1^{c_1} p_2^{c_2} \cdots p_k^{c_k}$$

where $0 \le c_i \le a_i$ for *i* = 1, 2, …, *k*. There are a_i+1 choices for c_i so the total number of positive divisors is $(a_1+1)(a_2+1)\cdots(a_k+1)$.

(3) In view of (2), the sum of the positive factors of *m* is given by

$$\sum_{\substack{0\le c_i\le a_i \\ 1\le i\le k}} p_1^{c_1} p_2^{c_2} \cdots p_k^{c_k} = (1+p_1+p_1^2+\cdots+p_1^{a_1})(1+p_2+p_2^2+\cdots+p_2^{a_2})\cdots(1+p_k+p_k^2+\cdots+p_k^{a_k}).$$

Illustrations. Since $90 = 2\times 3^2 \times 5$, 90 has $(1+1)(2+1)(1+1)=12$ positive divisors. The sum of the positive factors is $(1+2)(1+3+3^2)(1+5)=252$.

Example 3.1.

(IMO 1989 HK Prelim) Find the prime numbers *p* and *q* if it is known that the equation

$$x^4 - px^3 + q = 0$$

has an integral root.

Solution.

Let *N* be the integral root.

Then $N^4 - pN^3 + q = 0$, or $q = N^3(p - N)$.

Since q is prime, either $N^3 = \pm 1$ or $p - N = \pm 1$.

If $p - N = \pm 1$, then $N^3 = \pm q$, which is not possible since no prime is a perfect cube. So $N^3 = \pm 1$. If $N = -1$, $p - N = \pm q$, i.e. $q = -1 - p < 0$, which is again not possible.

Thus $N = 1$, so $q = p - 1$ and hence we must have $p = 3$, $q = 2$.

Example 3.2.

Prove that there are infinitely many prime numbers.

Solution.

Assume there are only finitely many primes, $p_1, p_2, \ldots, p_k$. Let $P = p_1 p_2 \cdots p_k + 1$. Clearly, P is larger than all the prime numbers, so it is not prime. But P is not divisible by any of the prime numbers, since $P - 1$ is divisible by all the primes and 1 cannot be divisible by any prime. This is a contradiction. So there must be infinitely many primes.

Example 3.3.

(IMO 1985) Given a set M of 1985 distinct positive integers, none of which has a prime divisor greater than 26. Prove that M contains at least one subset of four distinct elements whose product is the fourth power of an integer.

Solution.

Note that each element in M has at most 9 distinct prime factors, namely, 2, 3, 5, 7, …, 23. Given an element in M, consider its prime factorization and the parity of the power of each of the 9 prime factors. There are altogether $2^9 = 512$ possibilities. Thus, among any 513 elements in M, we can find two with exactly the same parity patterns, and so whose product is a square. Remove these pairs one at a time. Take 513 such pairs (since $1985 - 512 \times 2 > 512$, we can take so many pairs). Each has product b_i^2, where b_i is a positive integer with at most 9 distinct prime factors. Repeating the above trick, we can find two b_i's whose product is a square. Hence the four numbers in the two pairs have product equal to a fourth power.

Example 3.4.

How many pairs of integers (x, y) satisfy $x^2 - y^2 = 1125$?

Solution.

Rewrite the equation as $(x+y)(x-y)=1125$.

Since $1125=3^2\times5^3$, 1125 has $(2+1)(3+1)=12$ positive divisors, and in total 24 divisors if we also count the negative ones.

Each choice of a divisor of 1125 corresponds to an integral value of $x+y$, which automatically assigns an integral value to $x-y$. Since $x+y$ and $x-y$ are both odd, each assignment corresponds to an integral value of x and y. Conversely, it is clear each integer solution to the equation in turn corresponds to a divisor of 1125 by considering the value of $x+y$.

Since 1125 has 24 divisors, there are 24 such pairs.

The theory of prime numbers is very deep. A huge number of fascinating results and conjectures have come up throughout the years. For example, J. Bertrand conjectured in 1845 that for every positive integer n there is a prime between n and $2n$ inclusive. This was proved by the Russian mathematician P. L. Tchebychef in 1852. We will come across some of these interesting results in the exercises as well as in later units.

4. Exercises

1. The six-digit number $\overline{2639xy}$ is divisible by both 4 and 13. Find x and y.

2. Find the smallest positive multiple of 1998, all of whose digits are the same.

3. Is it true that an integer is divisible by 27 if and only if its sum of digits is divisible by 27?

4. Let p be a prime number, and n, k be positive integers.
   (a) If $p \mid n^k$, show that $p^k \mid n^k$. Is the converse true?
   (b) If $p^k \mid n$, show that $p \mid n$. Is the converse true?

5. Prove by number theoretic (and not combinatorial) arguments that the number

$$C_k^n = \frac{n!}{k!(n-k)!} = \frac{n(n-1)\cdots(n-k+2)(n-k+1)}{k(k-1)\cdots(2)(1)}$$

is an integer.

6. Find the number of ending zeros when 2003! is expressed in decimal notation.

7. Let $m > 1$ be an integer and $m = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$ be the prime factorization of m. Find the sum of the positive divisors of m.

8. Let n be a natural number. If $2n$ has 28 positive divisors and $3n$ has 30, how many does $6n$ have?

9. Let p_n denote the n-th prime number, i.e. $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, etc.

   (a) Using Bertrand's postulate, show that $p_n \le 2^n$ for all n. When does equality occur?

   (b) Using induction, show that $p_n \le 2^{2^{n-1}}$ for all n.

   (c) Show that for all natural numbers n, there exist $n+1$ primes less than 2^{2^n}.

10. Show that for all positive integers n, there exist n consecutive composite numbers, i.e. 'gaps' between consecutive primes can be arbitrarily close. (Hint: Consider $n!$.)

11. Let $n > 1$ be an integer.

    (a) Show that

    $$1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n}$$

    is not an integer.

    (b) Show that

    $$1 + \frac{1}{3} + \frac{1}{5} + \cdots + \frac{1}{2n-1}$$

    is not an integer.

12. Describe the test of divisibility by 11 you learnt in school and explain how it works.

13. (a) A test of divisibility by 7 is given as follows:

> To check whether a number is divisible by 7, remove the last digit, multiply the removed digit by 2 and subtract the product from the remaining number. The original number is divisible by 7 if and only if the difference is divisible by 7.

For instance, to check whether 462 is divisible by 7, remove the last digit 2, then multiply by 2 to get 4. Subtract 4 from 46 to get 42. Since $7 \mid 42$, we conclude that $7 \mid 462$.

Explain how the test works.

(b) Suggest a similar test of divisibility by 13.

14. (a) Another test of divisibility by 7 is given as follows:

> To check whether a number is divisible by 7, remove the last three digits. The original number is divisible by 7 if and only if the difference between the removed portion and the remaining portion is divisible by 7.

For instance, to check whether 58408 is divisible by 7, remove '408', leaving '58'. Since $408 - 58 = 350$ is divisible by 7, 58408 is also divisible by 7.

Explain how the test works.

(b) The above test also applies to divisibility by two other numbers between 10 and 20. What are the two numbers?

15. (a) A test of divisibility by 11 is given below:

> To test whether a number is divisible by 11, divide the number into segments of two digits from the right. The original number is divisible by 11 if and only if the sum of the segments is divisible by 11.

For instance, since $1 + 23 + 45 + 63 = 132$ is divisible by 11, so $11 \mid 1234563$.

(b) Suggest similar tests of divisibility by 99, 101 and 111.

16. (a) Show that the sum of any 7 consecutive integers is divisible by 7.

(b) Is it true that every integer divisible by 7 can be written as the sum of 7 consecutive integers?

(c) Is it true that for all natural numbers *n*, the sum of any *n* consecutive integers is divisible by *n*?

(d) In how many different ways can 2002 be expressed as the sum of two or more consecutive integers? In how many different ways can it be expressed as the sum of two or more consecutive *positive* integers?

(e) Find all integers which *cannot* be expressed as the sum of two or more consecutive integers.

(f) (IMO 1990 proposal) Observe that $9 = 4 + 5 = 2 + 3 + 4$. Is there an integer n which can be written as a sum of 1990 consecutive positive integers and which can be written as a sum of (more than one) consecutive positive integers in exactly 1990 ways?

17. (IMO 1971) Let m and n be non-negative integers. Prove that

$$\frac{(2m)!(2n)!}{m!n!(m+n)!}$$

is an integer.

18. (APMO 1998) Determine the largest of all integers n with the property that n is divisible by all positive integers that are less than $\sqrt[3]{n}$.

19. (IMO 2002) Let n be an integer greater than 1. The positive divisors of n are d_1, d_2, …, d_k where $1 = d_1 < d_2 < \ldots < d_k = n$.

Define $D = d_1d_2 + d_2d_3 + \cdots + d_{k-1}d_k$.

(a) Prove that $D < n^2$.

(b) Determine all n for which D is a divisor of n^2.