

4. Divisibility and divisors

Let $a, b \in \mathbf{Z}$, with $a \neq 0$. By the Division Theorem, we can find integers q, r such that $b = qa + r$, and $0 \leq r < a$. If $r = 0$, we say that a divides b . We may also say that a is a divisor of b , or a is a factor of b . We may say that b is a multiple of a .

In such a case, we write $a \mid b$. Otherwise, we write $a \nmid b$.

Note that $a \mid b$ if and only if $b = qa$, for some integer q . This version is the most convenient in calculations,

Examples

$3 \mid 12$ as $12 = 4 \cdot 3$ (and $4 \in \mathbf{Z}$)

$5 \nmid 12$ as $12 = 2 \cdot 5 + 2$, so we have a *non-zero* remainder.

Observe that, if $a \mid b$, then $b = qa$, and $q \in \mathbf{Z}$, so $|a| \leq |b|$. Thus we can find all divisors of a given number by trial and error – they all lie in the range $-|b|, \dots, |b|$.

For example the divisors of 12 are $\pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 12$.

Note

$a \mid b$ represents the mathematical statement “ a divides b ”.

It is NOT the fraction a/b .

Fact 1 For any $b \in \mathbf{Z}$, $1 \mid b$ and, if b is non-zero, $b \mid b$.

Proof

The first follows as $b = b \cdot 1$, i.e. b is a multiple of 1; the second as $b = 1 \cdot b$.

Fact 2 For any non-zero a in \mathbf{Z} , $a \mid 0$.

Proof

This follows as $0 = 0 \cdot a$.

Fact 3 Given $a, b \in \mathbf{Z}$, with $a \mid b$ we have $a \mid -b$, $-a \mid b$, $-a \mid -b$.

Proof

As $a \mid b$, $b = qa$ with $q \in \mathbf{Z}$.

These follow as $-b = (-q)a$, $b = (-q)(-a)$, $-b = q(-a)$, respectively.

After Fact 3, questions about divisibility can be answered by discussing only *positive* integers (and the integer 0).

Example Show that, if a is a non-zero integer, then $|a|$ divides a .

Solution

From Fact 1, $a \mid a$. Then Fact 3 shows that $-a \mid a$.

As $|a|$ is equal to either a or $-a$, we have $|a| \mid a$.

Fact 4 If $a \mid b$, with b non-zero, then $|a| \leq |b|$.

Proof

As $a \mid b$, $b = ka$, with $k \in \mathbf{Z}$. Hence $|b| = |ka| = |a| \cdot |k|$

As b is non-zero, k is non-zero. Thus, as $k \in \mathbf{Z}$, $|k| \geq 1$.

We then have $|b| = |a| \cdot |k|$, with $|k| \geq 1$.

Thus, $|a| \leq |b|$, as required.

Note. From Fact 4, if $|a| > |b|$, we *cannot* have $a \mid b$, i.e. we *must* have $a \nmid b$. This means that, if we are searching for the divisors of a non-zero integer b , we can restrict our attention to the range $-|b|, \dots, |b|$. If we also consider Fact 3, we see that all the divisors are of the form $\pm d$, with d in the range $1, \dots, |b|$. Also, after Fact 1, we know that ± 1 and $\pm b$ *do* appear in the list of divisors.

Fact 5 If $a \mid b$ and $b \mid c$, then $a \mid c$.

Proof

As $a \mid b$, $b = ka$, with $k \in \mathbf{Z}$.

As $b \mid c$, $c = mb$, with $m \in \mathbf{Z}$.

Then $c = mb = m(ka) = (mk)a$.

As $k, m \in \mathbf{Z}$. $n = mk \in \mathbf{Z}$.

Thus c is of the form na , with $n \in \mathbf{Z}$, so that $a \mid c$.

Fact 6 If $a \mid b$ and $a \mid c$, then $a \mid (b+c)$.

Proof

As $a \mid b$, $b = ka$, with $k \in \mathbf{Z}$.

As $a \mid c$, $c = ma$, with $m \in \mathbf{Z}$.

Thus $b+c = ka + ma = (k+m)a$.

As $k, m \in \mathbf{Z}$, $n = (k+m) \in \mathbf{Z}$.

Thus $b+c = na$, with $n \in \mathbf{Z}$, so that $a \mid (b+c)$,

The greatest common divisor of two integers

Definition The integer d is a *common divisor* of integers a and b if $d \mid a$ and $d \mid b$.

For example, 3 is a common divisor of 15 and 33.

By Fact 2, if $a = b = 0$, then *any* integer d is a common divisor of a and b . On the other hand, if, say, b is non-zero, then any divisor of b is in the range $-|b|, \dots, |b|$. See the note after Fact 4 above. Then any *common* divisor of a and b must also lie in this range. It follows that there are only a *finite* number of common divisors. Now, 1 is always a common divisor of any two integers, so the set of common divisors of a and b is a non-empty finite set. It must therefore have a greatest member, and this is positive.

Definition If a and b are integers, not *both* zero, then the *greatest common divisor of a and b* is the greatest integer d , with $d \mid a$ and $d \mid b$. It is denoted by $\gcd(a,b)$.

Provided a and b are not both zero, the remark before the definition shows that $\gcd(a,b)$ is well-defined (and positive).

Example Determine $\gcd(6,9)$.

Solution

We know that the positive divisors of 6 lie in the range $1, \dots, 6$. By trial and error, we see that the only positive divisors are 1, 2, 3 and 6. Similarly, the only positive divisors of 9 are 1, 3 and 9. Thus the only common divisors are ± 1 and ± 3 . Hence $\gcd(6,9) = 3$.

Later, we find a systematic *and fast* method for finding the gcd of two integers.

Example Show that, if $a \neq 0$, then $\gcd(a,0) = |a|$.

Solution

We know that *any* positive integer divides 0. The positive divisors of a are in the range $1, \dots, |a|$. From an earlier example, we know that $|a|$ divides a , so this must be the greatest common divisor.

Fact 1 If a and b are integers, not both zero, then $\gcd(a,b) = \gcd(|a|,|b|)$.

Proof

From Fact 3, a and $-a$ have the same set of divisors. Similarly for b and $-b$. Thus $\{a,b\}$, $\{-a,b\}$, $\{a,-b\}$ and $\{-a,-b\}$ have the *same set* of common divisors, and so each pair has the same greatest common divisor. In other words

$$\gcd(a,b) = \gcd(-a,b) = \gcd(a,-b) = \gcd(a,-b).$$

Now, $|a| = a$ or $-a$, and $|b| = b$ or $-b$, so that $\gcd(|a|,|b|)$ is in the above list, and hence is equal to $\gcd(a,b)$.

After this fact, we can concentrate on finding the greatest common denominator for two *positive* integers.

The next result is very important in what follows, so we describe it as a Theorem.

Theorem 1

Let $a, b, c \in \mathbf{Z}$, with $a \mid b$ and $a \mid c$. Then for *any* $m, n \in \mathbf{Z}$, $a \mid (mb+nc)$.

Proof

As $a \mid b$ and $a \mid c$, we have $b = ua$, and $c = va$, with $u, v \in \mathbf{Z}$.

Then $mb+nc = mua + nva = (mu+nv)a$.

As $m, n, u, v \in \mathbf{Z}$, $w = mu+nv \in \mathbf{Z}$.

Thus $mb+nc = wa$, with $w \in \mathbf{Z}$, so that $a \mid (mb+nc)$.

This generalises to any length of sum

Theorem 1a

Suppose that a is an integer, and that for each i with $1 \leq i \leq n$, b_i and m_i are integers with $a \mid b_i$, then $a \mid (m_1b_1+ m_2b_2+ \dots + m_nb_n)$.

We omit the proof, it is very similar to that of Theorem 1.

We can paraphrase this as saying that “if an integer a divides each of a set of integers, then it divides any linear combination of these integers”.

We now look at a type of example which is very common in tutorials, tests and examinations! It depends on knowledge of Theorem 1. Given two complicated integers, we look at a combination which is somehow simpler.

Example Show that, for any integer a , $\gcd(12a+7, 11a+5)$ always divides 17.

Solution

Suppose that $d \mid (12a+7)$ and $d \mid (11a+5)$.

By Theorem 1, $d \mid \{11(12a+7) - 12(11a+5)\}$, i.e. $d \mid (77-60) = 17$.

Thus *any* common divisor of $12a+7$ and $11a+5$ also divides 17, so the *greatest* common divisor must do so.

Notes.

- (1) We chose the combination of $12a+7$ and $11a+5$ to obtain an integer which does not depend on a . This gives a numerical handle on d .
- (2) By trial and error, the only positive divisors of 17 are 1 and 17, so that $\gcd(12a+7, 11a+5)$ must be one of these. A little experimentation shows that is frequently equal to 1 – try $a = 0, 1, 2, 3$. But it *can* be 17 – try $a = 15$.

Example Show that, for any integer n , $\gcd(n^2+1, n+1)$ is 1 or 2.

Solution

Suppose that $d \mid n^2+1$ and $d \mid n+1$.

Comment The most complicated term in these two numbers is n^2 . We know that $d \mid (a.(n^2+1)+b.(n+1))$ for *any* integers a, b . We choose a and b to eliminate n^2 from the combination. One suitable choice is $a = -1, b = n$.

Then $d \mid (-1.(n^2+1)+n.(n+1)) = n-1$.

We now know that d divides $n+1$ and $n-1$, as well as n^2+1 .

Comment We choose a combination of $n+1$ and $n-1$ which does not involve n . This is similar to the tactic in the last example.

We have $d \mid (1.(n+1)-1.(n-1)) = 2$.

Thus *any* common divisor of $n+1$ and $n-1$ divides 2.

This must be true of the *greatest* common divisor, $\gcd(n^2+1, n+1)$.

Since $\gcd(n^2+1, n+1)$ is *positive*, it must be equal to 1 or 2.

Note.

A perfectly satisfactory answer would consist of the above solution *without the comments*.

Exercise to the reader

By considering separately the cases n odd, n even, determine the values of n for which $\gcd(n^2+1, n+1) = 1$.

Our next result is also important. It is the key to the vital euclidean algorithm. It depends crucially on Theorem 1.

Theorem 2

Suppose that $a, b, q, r \in \mathbb{Z}$, with $a \neq 0$ and $b = qa + r$. Then $\gcd(a, b) = \gcd(a, r)$.

Proof

Note that $b = qa + r = qa + 1 \cdot r$. Then, by Theorem 1, if $d \mid a$ and $d \mid r$, then $d \mid b$. Thus the common divisors of a and r are also common divisors of a and b .

Now rearrange $b = qa+r$ as $r = qa-b = qa+(-1) \cdot b$. Again we can apply Theorem 1 to see that the common divisors of a and b are also common divisors of a and r .

Hence we see that $\{a, b\}$ and $\{a, r\}$ have the same set of common divisors, and hence the same greatest common divisor. Thus $\gcd(a, b) = \gcd(a, r)$.

Example Find $\gcd(100, 203)$.

Solution

Observe that $203 = 2 \cdot 100 + 3$. Then, by Theorem 2, $\gcd(100, 203) = \gcd(100, 3)$.

Now the only positive divisors of 3 are 1 and 3. Of these, only 1 divides 100. Thus the only, and hence greatest, common divisor of 100 and 3 is 1. Hence $\gcd(100, 203) = \gcd(100, 3) = 1$.