

Divisibility asks a simple question: does one integer split evenly into another? In this handout we turn that idea into a precise definition and then use it, together with factoring, to prove some general facts about integers.

Definition. Let N and m be integers. We say that m is a **divisor** (or **factor**) of N if there exists an integer k such that

$$N = mk.$$

When this happens, we also say that N is **divisible** by m , or that N is a **multiple** of m . The notation for this is $m \mid N$, read “ m divides N .”

For example, $7 \mid 21$, because there is an integer (namely 3) with $21 = 7 \cdot 3$. On the other hand, $5 \nmid 12$, since no integer k satisfies $12 = 5k$.

Factoring Out a Common Divisor

Here is a typical claim we can now make precise: if 20 and 35 are both divisible by 5, then so are their sum and their difference. Indeed,

$$20 + 35 = 55 = 5 \cdot 11 \quad \text{and} \quad 35 - 20 = 15 = 5 \cdot 3.$$

This is not a coincidence, and the reason is exactly the kind of factoring we have been practicing: if m is a common factor of two numbers, we can factor m out of their sum or difference.

Example 1. Suppose a and b are integers, and both are divisible by 7. Prove that $a + b$ and $a - b$ are also divisible by 7.

Proof. Since $7 \mid a$, there is an integer p with $a = 7p$. Since $7 \mid b$, there is an integer q with $b = 7q$. Then

$$a + b = 7p + 7q = 7(p + q),$$

and since $p + q$ is an integer, this shows $7 \mid (a + b)$. Likewise,

$$a - b = 7p - 7q = 7(p - q),$$

and since $p - q$ is an integer, $7 \mid (a - b)$. ■

Nothing about 7 was special here – the same argument works for any common divisor.

Example 2. Suppose a and b are integers, and both are divisible by m . Prove that $a + b$ and $a - b$ are also divisible by m .

Proof. Since $m \mid a$, there is an integer p with $a = mp$. Since $m \mid b$, there is an integer q with $b = mq$. Then

$$a + b = mp + mq = m(p + q),$$

and since $p + q$ is an integer, this shows $m \mid (a + b)$. Likewise,

$$a - b = mp - mq = m(p - q),$$

and since $p - q$ is an integer, $m \mid (a - b)$. ■

A word of caution. This example shows that $m \mid a$ and $m \mid b$ together force $m \mid (a + b)$. The *converse* is false: knowing that $m \mid (a + b)$ tells us nothing about whether m divides a and b individually. For instance, $5 \mid (2 + 3)$, since $2 + 3 = 5$, yet 5 divides neither 2 nor 3.

We just handled the sum and the difference of a and b – what about their *product*? We leave that question for you to work out, in the Practice Problems below.

Representing a Remainder

Not every integer is divisible by 3 – but every integer is *close* to being divisible by 3, in the sense that dividing by 3 always leaves a remainder of 0, 1, or 2. This is called the **Division Algorithm**: for any integer n , there exist unique integers q and r , with $0 \leq r < 3$, such that

$$n = 3q + r.$$

Sorting integers by their remainder gives us a convenient algebraic form for each group.

- Remainder 0: these are the multiples of 3, and they all have the form $3k$.
- Remainder 1: these numbers have the form $3k + 1$.
- Remainder 2: these numbers have the form $3k + 2$.

Example 3. Show that the expression $3k + 1$, as k ranges over all integers, produces exactly the integers that leave a remainder of 1 when divided by 3.

Solution. First, plug in a few integer values of k :

k	−1	0	1	2	3
$3k + 1$	−2	1	4	7	10

Each of these numbers does leave a remainder of 1 when divided by 3: for instance, $10 = 3 \cdot 3 + 1$. Conversely, if an integer n leaves a remainder of 1 when divided by 3, then by the Division Algorithm $n = 3q + 1$ for some integer q – which is exactly the form $3k + 1$, with $k = q$. So the two descriptions, “leaves remainder 1 when divided by 3” and “has the form $3k + 1$ for some integer k ,” describe the same set of integers. ■

Example 4. Prove that no square number leaves a remainder of 3 when it is divided by 4.

Proof. Every integer leaves a remainder of 0, 1, 2, or 3 when divided by 4, so every integer n has one of the forms $4k$, $4k + 1$, $4k + 2$, or $4k + 3$. We check what remainder n^2 leaves in each case.

form of n	n^2	remainder of n^2
$4k$	$16k^2 = 4(4k^2)$	0
$4k + 1$	$16k^2 + 8k + 1 = 4(4k^2 + 2k) + 1$	1
$4k + 2$	$16k^2 + 16k + 4 = 4(4k^2 + 4k + 1)$	0
$4k + 3$	$16k^2 + 24k + 9 = 4(4k^2 + 6k + 2) + 1$	1

In every case, the remainder is 0 or 1 – it is never 3 (in fact, it is never 2 either). So no square number leaves a remainder of 3 when divided by 4. ■

Example 5. Find the smallest positive integer that gives a remainder of 1 when divided by 2, a remainder of 2 when divided by 3, a remainder of 3 when divided by 4, a remainder of 4 when divided by 5, and a remainder of 5 when divided by 6.

Solution. In every one of these conditions, the remainder is exactly 1 less than the divisor. So if n is the number we want, then $n + 1$ leaves a remainder of 0 – that is, $n + 1$ is evenly divisible – when divided by each of 2, 3, 4, 5, and 6. In other words, $n + 1$ is a common multiple of 2, 3, 4, 5, 6, and we want the smallest *positive* n , so we are looking for the least common multiple of 2, 3, 4, 5, and 6, which is 60. So $n + 1 = 60$, which gives $n = 59$. Checking: $59 = 2 \cdot 29 + 1 = 3 \cdot 19 + 2 = 4 \cdot 14 + 3 = 5 \cdot 11 + 4 = 6 \cdot 9 + 5$, exactly as required. ■

Notice that every divisor in the puzzle above paired with a remainder that was exactly one less than that divisor – in other words, each of those numbers was “just before” a multiple of its divisor. That idea turns out to have a nice consequence for squares.

Example 6. Prove that if an integer n leaves a remainder of 4 when divided by 5, then n^2 leaves a remainder of 1 when divided by 5.

Proof. Since n leaves a remainder of 4 when divided by 5, we can write $n = 5k + 4$ for some integer k . Then

$$n^2 = (5k + 4)^2 = 25k^2 + 40k + 16 = 25k^2 + 40k + 15 + 1 = 5(5k^2 + 8k + 3) + 1.$$

Since $5k^2 + 8k + 3$ is an integer, n^2 leaves a remainder of 1 when divided by 5. ■

A general pattern. This example is not special to the divisor 5. For instance, $3 = 4 - 1$ leaves a remainder of 3 when divided by 4, and $3^2 = 9 = 4 \cdot 2 + 1$ leaves a remainder of 1. Likewise, $6 = 7 - 1$ leaves a remainder of 6 when divided by 7, and $6^2 = 36 = 7 \cdot 5 + 1$ leaves a remainder of 1. In general: if an integer n leaves a remainder of $m - 1$ (one less than the divisor) when divided by m , then n has the form $n = mk - 1$ for some integer k , and

$$n^2 = (mk - 1)^2 = m^2k^2 - 2mk + 1 = m(mk^2 - 2k) + 1.$$

Since $mk^2 - 2k$ is an integer, n^2 always leaves a remainder of 1 when divided by m .

We will use this same idea – representing a whole family of integers with one algebraic expression – with a different divisor: every integer is either **even** (divisible by 2, of the form $2k$) or **odd** (remainder 1, of the form $2k + 1$).

Example 7. Prove that if n is an odd integer, then $n^2 - 1$ is divisible by 8.

Proof. Since n is odd, we may write $n = 2k + 1$ for some integer k . Then

$$n^2 - 1 = (2k + 1)^2 - 1 = (4k^2 + 4k + 1) - 1 = 4k^2 + 4k = 4k(k + 1).$$

Now look at the factor $k(k+1)$: it is a product of two *consecutive* integers, so one of them is even. That means $k(k+1) = 2j$ for some integer j . Substituting this back in,

$$n^2 - 1 = 4k(k + 1) = 4 \cdot 2j = 8j.$$

Since j is an integer, this shows $8 \mid (n^2 - 1)$. ■



Enrichment

Prime numbers are the building blocks every integer is made of. A natural question is whether the supply of primes ever runs out. The ancient Greek mathematician Euclid answered this over two thousand years ago – and the proof uses nothing more than the fact that a common divisor of two numbers also divides their difference.

Theorem (Euclid). There are infinitely many prime numbers.

Proof. Suppose, for the sake of contradiction, that there are only finitely many primes, and call them $p_1, p_2, \dots, p_n$. Consider the number

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

Since $N > 1$, it has at least one prime factor; call it p . Because we assumed $p_1, \dots, p_n$ is the list of *all* primes, p must be one of them – say $p = p_i$.

Now, p_i certainly divides the product $p_1 p_2 \cdots p_n$, since it is one of the factors in that product. And by our choice of p , p_i also divides N . Since a common divisor of two numbers also divides their difference, p_i must then divide the difference of N and $p_1 p_2 \cdots p_n$ as well:

$$N - p_1 p_2 \cdots p_n = 1.$$

But no prime number divides 1. This is a contradiction, so our assumption must be false: there is no finite list containing all the primes. In other words, there are infinitely many primes. ■

Notice that the whole contradiction came down to the fact that a common divisor of two numbers also divides their difference – the same small idea we started this handout with turns out to be exactly what is needed to prove one of the oldest theorems in mathematics.



Practice Problems

1. Suppose a and b are integers, both divisible by m . Prove that ab is divisible by m^2 .
2. Suppose a and b are integers, both divisible by 9. Prove that $4a - 7b$ is also divisible by 9.
3. (a) Write the general form, in terms of an integer k , of all integers that leave a remainder of 3 when divided by 4.
(b) List the four smallest positive integers of this form.
4. Suppose a leaves a remainder of 2 when divided by 7, and b leaves a remainder of 5 when divided by 7. Prove that $a + b$ is divisible by 7.
5. Prove: if n is an integer divisible by 3, then n^2 is divisible by 9.
6. Prove that there is no square number that is divisible by 3 but not by 9.
7. Prove that no square number leaves a remainder of 2 when it is divided by 5.
8. Prove: if n is an odd integer, then $n^2 + n$ is even. *Hint:* factor $n^2 + n$.
9. Find the smallest positive integer that gives a remainder of 3 when divided by 4, a remainder of 4 when divided by 5, and a remainder of 6 when divided by 7.
10. Prove that no square number ends in the digit 2.



Answers

1. Write $a = mp$ and $b = mq$ for integers p, q . Then $ab = (mp)(mq) = m^2(pq)$, and since pq is an integer, $m^2 \mid ab$.
2. Write $a = 9p$ and $b = 9q$ for integers p, q . Then $4a - 7b = 4(9p) - 7(9q) = 9(4p - 7q)$, and $4p - 7q$ is an integer, so $9 \mid (4a - 7b)$.
3. a) $4k + 3$ b) 3, 7, 11, 15
4. Write $a = 7p + 2$ and $b = 7q + 5$ for integers p, q . Then $a + b = 7p + 7q + 7 = 7(p + q + 1)$, and since $p + q + 1$ is an integer, $7 \mid (a + b)$.
5. Write $n = 3k$. Then $n^2 = 9k^2$, and since k^2 is an integer, $9 \mid n^2$.
6. Suppose a square n^2 is divisible by 3. Since 3 is prime, and $n^2 = n \cdot n$, 3 must divide one of the two factors – but both factors are n , so $3 \mid n$. Then $n = 3k$ for some integer k , which gives $n^2 = 9k^2$, so $9 \mid n^2$ as well. So a square cannot be divisible by 3 without also being divisible by 9.
7. Checking all five forms $5k, 5k + 1, 5k + 2, 5k + 3, 5k + 4$, their squares leave remainders 0, 1, 4, 4, 1 respectively when divided by 5. The remainder 2 never occurs.
8. Write $n = 2k + 1$. Then $n^2 + n = n(n + 1) = (2k + 1)(2k + 2) = 2(2k + 1)(k + 1)$, which is even because it is 2 times an integer.
9. Each remainder is 1 less than its divisor, so $n + 1$ must be a common multiple of 4, 5, and 7. Since 4, 5, 7 share no common factors, $\text{lcm}(4, 5, 7) = 4 \cdot 5 \cdot 7 = 140$, so $n + 1 = 140$ and $n = 139$.
10. The last digit of an integer is just the remainder it leaves when divided by 10, so this is the same process as problem 7, with 10 cases instead of 5: check n of the forms $10k, 10k + 1, \dots, 10k + 9$. Their squares leave remainders (last digits) 0, 1, 4, 9, 6, 5, 6, 9, 4, 1 respectively – the digit 2 never occurs, so no square number ends in 2.

Remark. The work in problem 10 can be cut down further. Since $(10k + r)^2 = 100k^2 + 20kr + r^2$ and $(10k - r)^2 = 100k^2 - 20kr + r^2$ differ only in the sign of the middle term, both leave the same remainder when divided by 10 – namely, the remainder of r^2 . So it is enough to check n of the forms $10k, 10k \pm 1, 10k \pm 2, 10k \pm 3, 10k \pm 4$, and $10k + 5$: just six squares ($0^2, 1^2, 2^2, 3^2, 4^2, 5^2$) instead of ten.