Lecture 10 — Divisibility

Table of contents

Pre-work: Video 013 (Divisibility). First lecture with Dr Katie Clinch. See divisibility-and-factorisation[1] for the reference definitions, the Unique Factorisation Theorem and the standard proofs.

Learning goals

1. Understand the definition of "is divisible by" and how to formulate it mathematically.
2. Understand and apply the Unique Factorisation Theorem.
3. Gain fluency in proof techniques (direct proof, proof by contradiction and proof by contraposition).

Important note: in the definition of "n is divisible by d", n and d are integers **and** $d \neq 0$.

$$d \mid n \iff \frac{n}{d} \in \mathbb{Z}$$

All of these say the same thing: d divides n; d is a divisor of n; d is a factor of n; n is a multiple of d.

[1] courses/math1061/divisibility-and-factorisation.pdf

Student questions and comments

In the proof from the video that every integer greater than 1 can be written as a product of primes — why must r and s be products of primes? Revisited below.

Activity 1 — finding counterexamples

Which collections of values for a, b and m give a counterexample disproving $\forall a, b, m \in \mathbb{Z}$, if $m \mid (a+b)$ then $m \mid (a-b)$? (Multiple answer.)

Recall the conditional is **false only when** the hypothesis is T and the conclusion is F:

	$m \mid (a+b)$	$m \mid (a-b)$	$m \mid (a+b) \to m \mid (a-b)$
(a) $m=5, a=20, b=10$	$5 \mid 30$ T	$5 \mid 10$ T	T
(b) $m=5, a=21, b=13$	$5 \mid 34$ F	$5 \mid 8$ F	T
(c) $m=5, a=27, b=7$	$5 \mid 34$ F	$5 \mid 20$ T	T
(d) $m=5, a=19, b=-9$	$5 \mid 10$ T	$5 \mid 28$ F	**F**
(e) $m=5, a=23, b=12$	$5 \mid 35$ T	$5 \mid 11$ F	**F**
(f) $m=5, a=-10, b=-3$	$5 \mid -13$ F	$5 \mid -7$ F	T

So **(d) and (e)** provide counterexamples.

Activity 2 — prove or disprove

(a) $\forall m \in \mathbb{Z}$, $6m(2m+10m^2)$ is divisible by 4. — True.

Direct proof. Suppose $m \in \mathbb{Z}$. Then

$$6m(2m+10m^2) = 2(3m) \cdot 2(m+5m^2) = 4(3m(m+5m^2)).$$

Since $m \in \mathbb{Z}$ we have that $3m(m+5m^2)$ is also an integer. Thus $4 \mid 6m(2m+10m^2)$. □

Saying *why the other factor is an integer* is the step that's easy to skip and shouldn't be.

(b) $\forall a, b, c \in \mathbb{Z}$, if $a \mid (b+c)$ then $a \mid b$ or $a \mid c$. — False.

Counterexample. Let $a=3$, $b=4$, $c=2$. Then $a \mid (b+c)$ because $3 \mid 6$, but $a \nmid b$ and $a \nmid c$ because $3 \nmid 4$ and $3 \nmid 2$. Thus the statement is false. □

(Recall $a \mid b \iff \frac{b}{a} \in \mathbb{Z}$ — so $10 \nmid 5$, since $\frac{5}{10} \notin \mathbb{Z}$. Watch the order.)

(c) $\forall a, b, c \in \mathbb{Z}$, if a is a multiple of c, then ab is a multiple of c. — True.

Direct proof. Let $a, b, c \in \mathbb{Z}$ and suppose $c \mid a$. $\leftarrow$ *initial hypotheses* Then $\exists k \in \mathbb{Z}$ such that $a = ck$. Multiplying both sides by b gives $ab = ckb = c(kb)$. Since $k, b \in \mathbb{Z}$ we have that $kb \in \mathbb{Z}$. Thus $c \mid ab$. $\leftarrow$ *conclusion* $\square$

Every integer $n > 1$ is a product of primes

Theorem (from the video): every integer $n > 1$ can be written as a product of primes.

Proof (by contradiction). Suppose the theorem is false. Then there exists an integer $n > 1$ that is not a product of primes.

Choose the smallest such n. A smallest such n exists by the well-ordering principle (covered in a later lecture). We choose this n so that we can use the fact that every integer less than n (but greater than 1) *can* be written as a product of primes.

Either n is prime or n is composite — splitting into two cases using the fact that every integer $n > 1$ is one or the other, not both.

Case 1: if n is prime, then n is a product of primes ($n = p$) — a contradiction already.

Case 2: if n is composite, then $n = rs$ for some positive integers r and s where $r \neq 1$ and $s \neq 1$. This implies $1 < r < n$ and $1 < s < n$. Because we chose n to be the smallest integer greater than 1 that is *not* a product of primes, both r and s — which are smaller than n — must be products of primes: $r = p_1 p_2 \cdots p_k$ and $s = q_1 q_2 \cdots q_\ell$. Therefore $n = rs = p_1 \cdots p_k q_1 \cdots q_\ell$ is a product of primes also.

So regardless of whether n is prime or composite, n *is* a product of primes. This contradicts our choice of n, and hence the theorem is proved. $\square$

That answers the student question above: r and s must be products of primes precisely *because* n was chosen to be the smallest counterexample, so nothing smaller than n can be one.

Unique Factorisation Theorem for the integers

Given any integer $n > 1$, the **standard factored form** of n is

$$n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$$

where k is a positive integer, $p_1, p_2, \ldots, p_k$ are prime numbers, $e_1, \ldots, e_k$ are positive integers, and $p_1 < p_2 < \cdots < p_k$.

Q3 from the pre-work questions

What is the unique prime factorisation of 6975 in standard factored form?

Try dividing by primes $2, 3, 5, 7, 11, ...$, keeping in mind you **only have to go as far as** $\sqrt{6975} = 83.51...$ due to the lemma below.

$$6975 = 3 \cdot 2325 = 3 \cdot 3 \cdot 775 = 3 \cdot 3 \cdot 5 \cdot 155 = 3 \cdot 3 \cdot 5 \cdot 5 \cdot 31 = 3^2 \cdot 5^2 \cdot 31$$

The prime factorisation of a positive divisor of 6975 has 0, 1 or 2 threes; 0, 1 or 2 fives; and 0 or 1 thirty-ones. Thus there are $3 \cdot 3 \cdot 2 = 18$ positive divisors.

Lemma: for every integer $n > 1$, if no integer x in the range $1 < x \leq \sqrt{n}$ divides n, then n is prime. (Optional activity — proof by contraposition given in divisibility-and-factorisation[2].)

Activity 3 — working with the factored form

(a) Standard factored form of 1400:

$$1400 = 2(700) = 2 \cdot 2(350) = 2 \cdot 2(35)(10) = 2^2(5 \cdot 7)(2 \cdot 5) = 2^3 \cdot 5^2 \cdot 7^1$$

— note the primes in increasing order.

(b) $1400^2 = (2^3 \cdot 5^2 \cdot 7^1)^2 = 2^6 \cdot 5^4 \cdot 7^2$ — raising to a power **multiplies** the exponents.

(c) $1400^3 = 1400 \cdot 1400^2 = (2^3 \cdot 5^2 \cdot 7^1)(2^6 \cdot 5^4 \cdot 7^2) = 2^9 \cdot 5^6 \cdot 7^3$ — multiplying **adds** the exponents.

(d) Number of positive divisors of 1400: $(3 + 1)(2 + 1)(1 + 1) = 4 \cdot 3 \cdot 2 = 24$.

(e) Positive divisors of 1400 divisible by 8: all factors of the form $2^3 \cdot 5^* \cdot 7^*$ —

	7^0	7^1
5^0	8	56
5^1	40	280
5^2	200	1400

(f) Smallest positive integer n **such that** $1400n$ **is a perfect square**: $1400n$ is a perfect square if $\exists t \in \mathbb{Z}$ with $1400n = t^2$. Then

$$t^2 = 2^3 \cdot 5^2 \cdot 7^1 \cdot n.$$

Split each power in half, bigger powers on the left: $t = 2^2 \cdot 5^1 \cdot 7^1$ paired against $2^1 \cdot 5^1 \cdot 7^0 \cdot n$, so $n = 2 \cdot 7 = 14$.

[2] courses/math1061/divisibility-and-factorisation.pdf

Activity 4 — a lemma by contradiction

Lemma: for any integer a and any prime number p, if $p \mid a$ then $p \nmid (a+1)$. *Hint: once you've set up the proof, write $(a+1) - a$ in terms of p.*

> *Proof (by contradiction).* Let $a \in \mathbb{Z}$, let p be prime, and suppose $p \mid a$ and — for a contradiction — assume $p \mid (a+1)$. Since $p \mid a$ there exists $k \in \mathbb{Z}$ such that $a = pk$. Since $p \mid (a+1)$ there exists $\ell \in \mathbb{Z}$ such that $a + 1 = p\ell$. So
>
> $$1 = (a+1) - a = p\ell - pk = p(\ell - k).$$
>
> Since $\ell, k \in \mathbb{Z}$ we have $\ell - k \in \mathbb{Z}$. Thus $1 = p(\ell - k)$ means $p \mid 1$ — which is a contradiction, because $p \geq 2$ for any prime, whereas $p \mid 1$ would force $p = \pm 1$. So the assumption was false: $p \nmid (a+1)$. $\square$

The technique worth keeping: rewrite the divisibility hypotheses as *equations*, then combine them so the unwanted quantity appears on its own.

Theorem: there are an infinite number of primes

> *Proof (by contradiction).* Suppose the number of primes is finite. Then some prime p is the largest, and we can list the primes in ascending order: $2, 3, 5, 7, 11, \ldots, p$.
>
> Let N be 1 more than the product of all the primes: $N = (2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdots p) + 1$.
>
> Then $N > 1$, so by the Unique Factorisation Theorem N can be written as a product of primes, and hence is divisible by some prime q. Because q is prime, it must equal one of the primes in our list.
>
> Thus q divides $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdots p$ — that is, $q \mid (N-1)$ — and so, by the lemma above, q does not divide $(2 \cdot 3 \cdots p) + 1 = N$.
>
> Hence q divides N and q does not divide N: a contradiction. We conclude the original statement must be true. $\square$

See also

- divisibility-and-factorisation[3] · proof-techniques[4]
- 2026-08-20-modular-arithmetic[5] — Lecture 11
- practice-problems[6] — §13 Divisibility, with full worked solutions

[3] courses/math1061/divisibility-and-factorisation.pdf
[4] courses/math1061/proof-techniques.pdf
[5] courses/math1061/2026-08-20-modular-arithmetic.pdf
[6] courses/math1061/practice-problems.pdf