Lecture 10 — Divisibility

Table of contents

Learning goals . . . 1
The definition, and why $d \neq 0$ . . . 2
Worked: finding counterexamples . . . 2
Worked: prove or disprove . . . 3
Every integer $n > 1$ is a product of primes . . . 4
Unique Factorisation Theorem for the integers . . . 5
Worked: the factored form of 1400 . . . 6
A lemma by contradiction . . . 9
Theorem: there are an infinite number of primes . . . 9
The $\sqrt{n}$ lemma, by contraposition . . . 10
Which proof method, and why . . . 11
See also . . . 12

Pre-work: Video 013 (Divisibility). 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).

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

The definition, and why $d \neq 0$

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

The definition is a biconditional, because proofs use it in both directions:

$$d \mid n \quad \longleftrightarrow \quad d \neq 0 \text{ and } n = dk \text{ for some integer } k$$

It has an equivalent quotient form:

$$d \mid n \quad \longleftrightarrow \quad \frac{n}{d} \in \mathbb{Z}$$

Why $d \neq 0$. The quotient $\frac{n}{d}$ is the thing that stops making sense at $d = 0$, so the restriction is baked into the definition rather than checked afterwards.

The $\exists k$ form is the one to unfold in a proof — every proof below that starts from a divisibility hypothesis immediately rewrites it, $c \mid a$ becoming $a = ck$. The quotient form is the faster one for *testing* a specific pair, which is how it gets used in the counterexample and prove-or-disprove questions below.

The relation is **not** symmetric: $d \mid n$ says n is the multiple, not d. All four 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

Non-divisibility is written with the slashed bar: $d \nmid n$.

Worked: 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 $m \mid (a-b)$? More than one of the six below does.

A conditional has four patterns. `T → T`, `F → T` and `F → F` are true; only `T → F` is false. That is what "counterexample" means here. As a truth table:

$m \mid (a+b)$	$m \mid (a-b)$	$m \mid (a+b) \rightarrow m \mid (a-b)$
T	T	T
T	**F**	**F** ← the only false row
F	T	T

F	F	T

So a counterexample needs the hypothesis **true** and the conclusion **false** — a row where $m \mid (a+b)$ holds but $m \mid (a-b)$ fails. Rows where the hypothesis already fails are useless, however wrong the conclusion looks.

	$m \mid (a+b)$	$m \mid (a-b)$	$m \mid (a+b) \to m \mid (a-b)$
(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. (c) is the trap: the conclusion column is T, but the hypothesis is F, so the conditional is vacuously true and nothing has been disproved.

Worked: 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 $4 \mid 6m(2m+10m^2)$.

The second-last sentence is there to say *why the other factor is an integer.* Producing the factor of 4 is not enough on its own: the definition demands $n = dk$ **with** k **an integer**, so the proof has to say that the cofactor is one. It is the step that is 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.

The order of the arguments matters: $a \mid b \iff \frac{b}{a} \in \mathbb{Z}$, so $10 \nmid 5$ — the quotient to test is $\frac{5}{10}$, which is not an integer, not $\frac{10}{5}$. The divisor goes on the **left** of the bar, the multiple on the **right**.

(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 $c \mid a$. 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 $c \mid ab$. //

The shape of this proof is the transferable part. The hypothesis *in the statement* — from $\forall a, b, c \in \mathbb{Z}$ through *a is a multiple of c* — gives the first line of the proof, its **initial hypotheses**. The **conclusion** in the statement — *ab is a multiple of c* — gives the last line. Neither of those two lines is a choice — the statement writes them. The only invention in a direct proof is the middle. Either end mark closes a proof: the double slash // used here, or the □ on the proofs below. math1061-diagram-notation[2] records both marks as sanctioned.

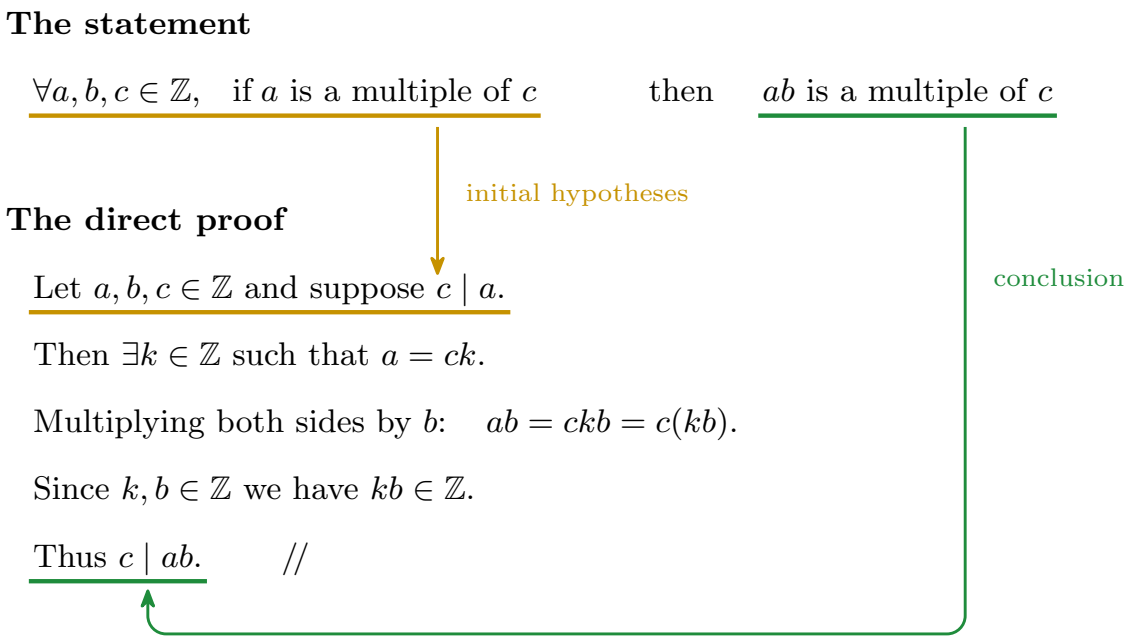

Figure 1: How the statement dictates the first and last lines of a direct proof. One arrow runs from the underlined hypothesis — $\forall a, b, c \in \mathbb{Z}$, *if a is a multiple of c* — down onto *Let* $a, b, c \in \mathbb{Z}$ *and suppose* $c \mid a$, and one from the underlined conclusion *ab is a multiple of c* round onto *Thus* $c \mid ab$. Both ends of the proof are fixed before any work starts; the three lines between them are the whole content.

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

Theorem: every integer $n > 1$ can be written as a product of primes.

[2] courses/math1061/math1061-diagram-notation.pdf

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 number n. A smallest such n exists by the well-ordering principle (see strong-induction-and-the-well-ordering-principle[3]). 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 — namely the one-term product $n = p$. 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. □

In Case 2, r and s must be products of primes precisely *because* n was chosen to be the **smallest** counterexample, so nothing strictly between 1 and n can be one. The choice of the smallest bad n is the entire engine of the proof, and it is why the well-ordering principle has to be invoked to make the choice legal.

The proof has three moves. The opening two lines set up the proof by contradiction. The line **Choose the smallest such number** n is legal because a smallest such n exists by the well-ordering principle. Then the proof splits into two cases, using the fact that every integer $n > 1$ is either prime or composite (not both).

Unique Factorisation Theorem for the integers

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

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

where k is a positive integer, $p_1, p_2, \ldots, p_k$ are prime numbers, $e_1, e_2, \ldots, e_k$ are positive integers, and $p_1 < p_2 < \cdots < p_k$.

[3] courses/math1061/strong-induction-and-the-well-ordering-principle.pdf

The strict inequality is part of the definition: the primes go in **increasing** order, which is what makes the form unique rather than merely available.

Worked: 6975 in standard factored form

What is the unique prime factorisation of 6975 in standard factored form? (Q3 of the pre-work questions.)

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

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

Counting the divisors. 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.

For example, choosing one three, no fives and no thirty-ones gives $3 = 3^1 \cdot 5^0 \cdot 31^0$, which is indeed a divisor of 6975. Every divisor is one such choice, and different choices give different divisors — which is why the count is a product.

Lemma: for every integer $n > 1$, if no integer x in the range $1 < x \leq \sqrt{n}$ divides n, then n is prime.

This is what licenses stopping trial division at $\sqrt{n}$. The proof, by contraposition, is further down.

Worked: the factored form of 1400

(a) Standard factored form of 1400.

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

The final step is where the primes get sorted into **increasing** order.

(b) 1400^2**.**

$$1400^2 = (2^3 \cdot 5^2 \cdot 7^1)^2 = 2^6 \cdot 5^4 \cdot 7^2$$

Raising to a power **multiplies** the exponents.

(c) 1400^3**.**

$$1400^3 = (1400)(1400^2) = (2^3 \cdot 5^2 \cdot 7^1)(2^6 \cdot 5^4 \cdot 7^2) = 2^9 \cdot 5^6 \cdot 7^3$$

Multiplying **adds** the exponents, one prime at a time: the 2 in 5^2 and the 4 in 5^4 give the 6 in 5^6.

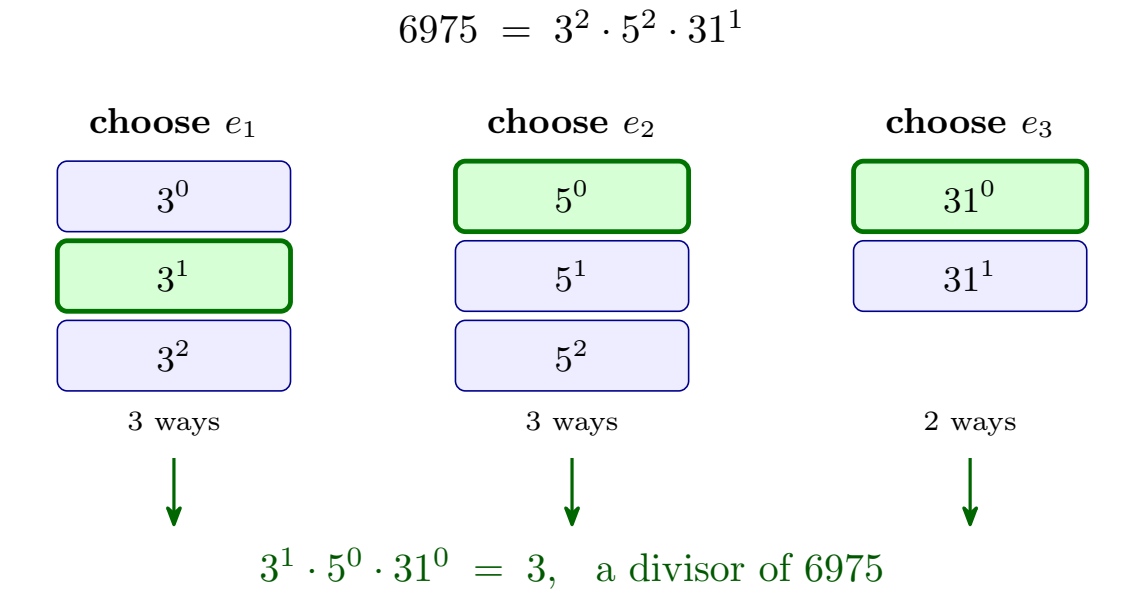

Figure 2: Why 6975 has exactly 18 positive divisors. Picking a divisor of $3^2 \cdot 5^2 \cdot 31^1$ means picking an exponent from each column independently, so the number of divisors is $3 \cdot 3 \cdot 2$. The highlighted row in each column is one worked choice — $e_1 = 1$, $e_2 = 0$, $e_3 = 0$ — which yields the divisor 3.

Both rules are just the index laws, but the standard factored form is what makes them usable: because the form is unique, matching the exponents prime by prime is a legitimate step and not a guess.

(d) How many positive divisors does 1400 have?

$$(3+1)(2+1)(1+1) = 4 \cdot 3 \cdot 2 = 24$$

Same counting rule as Figure 2, one column per prime: the exponent of 2 can be any of $0, 1, 2, 3$ (four choices), the exponent of 5 any of $0, 1, 2$, the exponent of 7 any of $0, 1$. The $+1$ in each bracket is the exponent 0 — the option of leaving that prime out.

(e) List all positive divisors of 1400 that are divisible by 8.

Since $8 = 2^3$ and 1400 only carries 2^3, "divisible by 8" pins the exponent of 2 at exactly 3. So the answer is 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

Six of them, which is the counting rule again with one column frozen: $1 \cdot 3 \cdot 2 = 6$.

(f) Find the smallest positive integer n such that $1400n$ is a perfect square.

$1400n$ is a perfect square if $\exists t \in \mathbb{Z}$ such that $1400n = t^2$. Then

$$t^2 = 2^3 \cdot 5^2 \cdot 7^1 \cdot n = \underbrace{(2^2 \cdot 5^1 \cdot 7^1)}_{t} \cdot \underbrace{(2^1 \cdot 5^1 \cdot 7^0 \cdot n)}_{t}$$

The method: **try to split each power in half, bigger powers on the left.** Both bracketed factors have to equal t, so matching them gives $2^1 \cdot 5^1 \cdot 7^0 \cdot n = 2^2 \cdot 5^1 \cdot 7^1$, hence

$$n = 2^1 \cdot 7^1 = 14$$

> In general: an integer is a perfect square exactly when **every** exponent in its standard factored form is even, so the smallest useful n is the product of precisely the primes whose exponent in 1400 is odd. Here those are 2 (exponent 3) and 7 (exponent 1), giving $n = 2 \cdot 7 = 14$; and $1400 \cdot 14 = 19600 = 140^2$.

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 the proof is set up, 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 every prime, whereas $p \mid 1$ would force $p = \pm 1$. So the assumption was false: $p \nmid (a+1)$.

The technique is to **rewrite as equations**: the two divisibility statements become the lines $a = pk$ and $a + 1 = p\ell$. Then combine them so the unwanted quantity is left on its own. Subtracting kills a and leaves $1 = p(\ell - k)$, which is the only place the contradiction can come from.

In the same proof, the two existentials get **different letters**. k is already spoken for by $p \mid a$; reusing it for $p \mid (a+1)$ would assert $a = a + 1$.

In words the lemma says: no prime can divide two consecutive integers. That is exactly what the next theorem needs.

Theorem: there are an infinite number of primes

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

The pivot is the step $q \mid (N-1)$, *so by the lemma*, $q \nmid N$. The lemma on consecutive integers is the step that closes this proof.

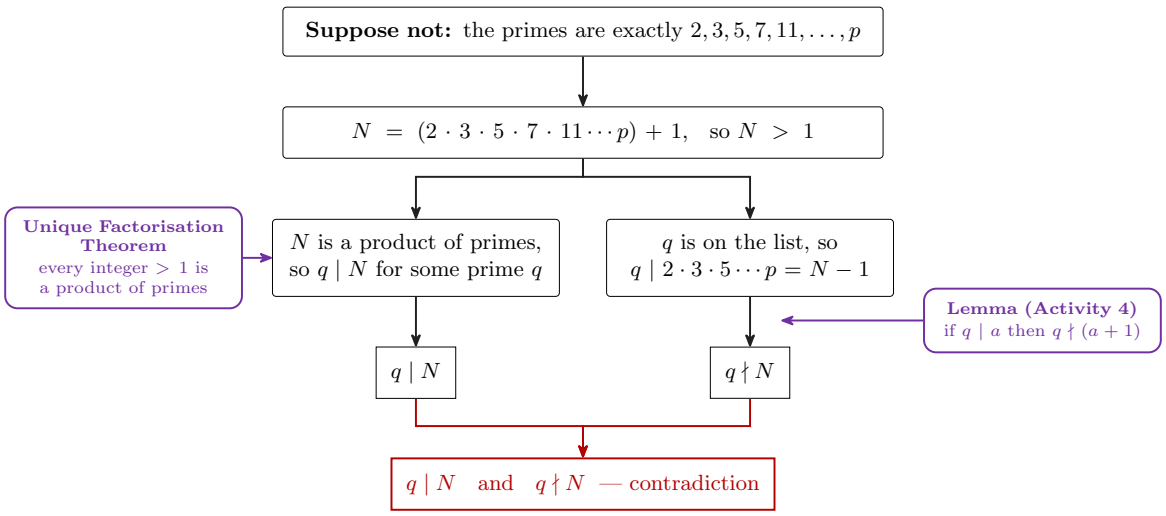

Figure 3: Where each named result plugs into the infinitude-of-primes proof. Two chains start from the same N and reach opposite verdicts about the same prime q: the left needs the Unique Factorisation Theorem to produce q at all, the right needs the lemma on consecutive integers to rule it out, and the contradiction is the collision. The right-hand branch is the step $q \mid (N-1)$, *so by the lemma* $q \nmid N$.

The $\sqrt{n}$ lemma, by contraposition

This closes the loop back to the 6975 factorisation: it is the result that says trial division may stop at $\sqrt{n}$.

Lemma: for every integer $n > 1$, if no integer x in the range $1 < x \leq \sqrt{n}$ divides n, then n is prime.

Proof (by contraposition). The contrapositive of the lemma states:

$\forall n \in \mathbb{Z}^{\geq 2}$, if n is not prime, then $\exists\, x \in \mathbb{Z}$ in the range $1 < x \leq \sqrt{n}$ such that $x \mid n$.

Suppose $n \in \mathbb{Z}^{\geq 2}$ and n is not prime. Then n is composite so (by definition) $\exists\, r, s \in \mathbb{Z}^{+}$ such that $n = rs$ and $1 < r < n$ and $1 < s < n$.

Case 1: $r = s$**.** In this case, we have $r = s = \sqrt{n}$.

Case 2: $r \neq s$**.** In this case, one of r, s is less than $\sqrt{n}$ and the other is greater than $\sqrt{n}$. (To see why this is, note that if both are greater than $\sqrt{n}$ we would have $rs > n$, and if both are less than $\sqrt{n}$ we would have $rs < n$.)

In either case, $\exists\, x \in \{r, s\}$ such that $1 < x \leq \sqrt{n}$ and x divides n (since r and s each divide n). $\square$

Two remarks about the scope of the lemma. The proof never *finds* the factor, it only shows one exists in the range, which is all the lemma claims. And it never rules out a factor above $\sqrt{n}$: $194 = 2 \cdot 97$ has $\sqrt{194} \approx 13.9$, so its factor 97 sits far above the bound while its factor 2 sits below it. The lemma bounds the *smallest* non-trivial factor, which is exactly what trial division meets first, and that is why the search may stop there.

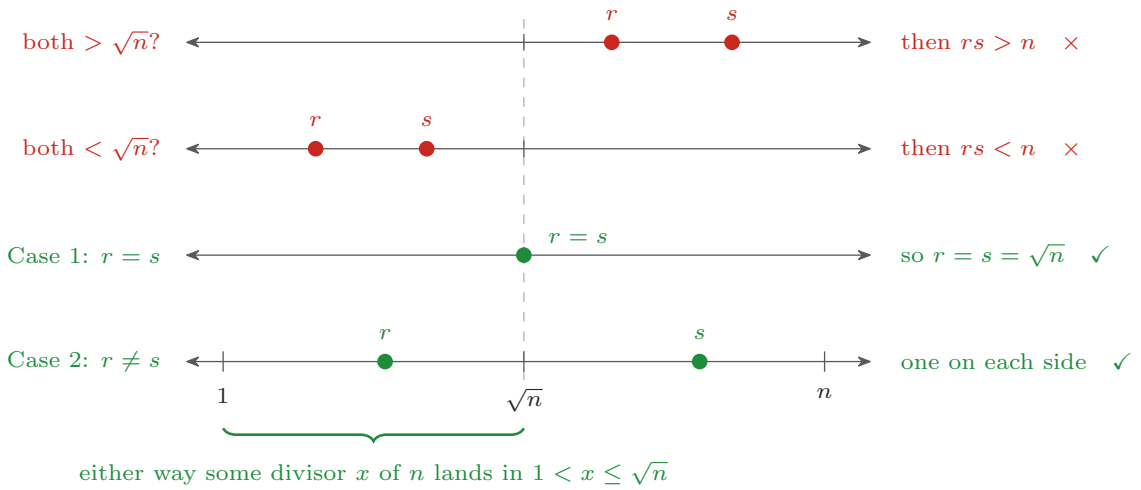

Figure 4: Why a composite $n = rs$ must have a divisor no larger than $\sqrt{n}$ — the parenthetical step in the contraposition proof. The two red rows are the possibilities ruled out by size alone: if both are greater than $\sqrt{n}$ we would have $rs > n$, and if both are less than $\sqrt{n}$ we would have $rs < n$. The two green rows are Case 1 and Case 2 of the proof.

Which proof method, and why

Eight statements are settled above, by four different proof shapes — direct, disproof by counterexample, contradiction and contraposition:

Statement	Method	Why that one
$m \mid (a+b) \to m \mid (a-b)$	counterexample	one row with hypothesis T and conclusion F kills it
$4 \mid 6m(2m+10m^2)$	direct	the conclusion is a single divisibility claim, so produce the factor
$a \mid (b+c) \to a \mid b$ or $a \mid c$	counterexample	a universal claim is disproved by one bad triple

Statement	Method	Why that one
$c \mid a \to c \mid ab$	direct	the hypothesis unfolds to $a = ck$ and the conclusion is one multiplication away
every $n > 1$ is a product of primes	contradiction	needs a *smallest* offender, which only a contradiction setup provides
$p \mid a \to p \nmid (a+1)$	contradiction	the conclusion is a **non**-divisibility, so assume divisibility and break it
infinitely many primes	contradiction	a finite list is something you can build N out of
the $\sqrt{n}$ lemma	contraposition	"no x divides n" is an awkward hypothesis; "n is composite" is a usable one

The pattern worth carrying: a **negative** conclusion ($p \nmid \ldots$, "there is no largest prime") almost always wants contradiction or contraposition, because a negation is hard to build with and easy to break.

See also

- divisibility-and-factorisation[4] · proof-techniques[5]
- strong-induction-and-the-well-ordering-principle[6] — the well-ordering principle the product-of-primes proof leans on
- 2026-08-20-modular-arithmetic[7] — Lecture 11
- practice-problems[8] — §13 Divisibility, with full worked solutions

[4] courses/math1061/divisibility-and-factorisation.pdf
[5] courses/math1061/proof-techniques.pdf
[6] courses/math1061/strong-induction-and-the-well-ordering-principle.pdf
[7] courses/math1061/2026-08-20-modular-arithmetic.pdf
[8] courses/math1061/practice-problems.pdf