# Prime Numbers and Unique Factorization

*Why every integer factors into primes in exactly one way, and why the primes never end*

Image: Own rendering

**By the end of this unit, I should be able to answer these questions:**

- Why does every integer greater than 1 have at least one prime factor, and why does a composite number have one at most equal to its square root?
- How did Euclid prove that there are infinitely many primes, and why does his proof give no formula for them?
- Why can 360 be written as a product of primes in only one way, apart from the order of the factors?
- In the numbers 1, 5, 9, 13, 17, and so on, why does 441 factor in two different ways, and what does that tell me about the ordinary integers?
- How does the sieve of Eratosthenes find every prime below 100, and why can it stop crossing out after 7?
- How many zeros does \(100!\) end with, and how can I count them without computing it?
- Why can a number with 41 million digits be proved prime while a number with 300 digits cannot be factored?

Anyone can check in a minute that $59 \times 509 = 30031$. Going the other way, from 30031 back to 59 and 509, takes a long time by hand, and for a product of two primes with a few hundred digits in all, no computer on Earth has managed it so far. That one-way quality of multiplication is the subject of this unit. It begins with the definition of a prime, proves that every integer is built from primes in exactly one way, shows how to find the primes below any bound, proves that they never run out, and ends with a question that still shapes computing: why deciding whether a number is prime is so much easier than taking it apart.

## 1 Primes and composites

Unit 2 introduced the notation $a \mid b$, which says that $a$ divides $b$, that is, $b = ac$ for some integer $c$. An integer $n > 1$ is called **prime** if its only positive divisors are 1 and $n$ itself, and **composite** if it has a divisor $d$ with $1 < d < n$. The first primes are $2, 3, 5, 7, 11, 13$, and the first composites are $4, 6, 8, 9, 10, 12$. The number 2 is the only even prime, because every larger even number has the divisor 2.

The number 1 is neither prime nor composite, and this is a deliberate convention. If 1 counted as a prime, every integer would have infinitely many factorizations into primes, such as $6 = 2 \cdot 3 = 1 \cdot 2 \cdot 3 = 1 \cdot 1 \cdot 2 \cdot 3$, and the theorem of Section 3, which says that the factorization is unique, would be false as stated. Keeping 1 out of the primes keeps the theorem clean.

The definition says what a prime is, and the first theorem says that every integer greater than 1 has one as a factor. To prove this, let $n > 1$ and consider the set of divisors of $n$ that are greater than 1. The set

is not empty, because $n$ belongs to it, so by the well-ordering principle of Unit 1, which says that every non-empty set of positive integers has a smallest element, it has a smallest element $d$. This smallest divisor $d$ must be a prime, for the following reason. If it were composite, it would have a divisor $a$ with $1 < a < d$, and since $a \mid d$ and $d \mid n$, the number $a$ would be a divisor of $n$ greater than 1 and smaller than $d$, which contradicts the choice of $d$.

**KEY RESULT The smallest divisor is prime**

For every integer $n > 1$, the smallest divisor $d > 1$ of $n$ is a prime.

In particular every integer greater than 1 has at least one prime factor. The statement holds for primes as well, where the smallest divisor greater than 1 is $n$ itself.

A second observation decides how much work it is to test a number. Suppose $n$ is composite, so $n = ab$ with $1 < a \le b < n$. Then $a \cdot a \le a \cdot b = n$, which gives $a \le \sqrt{n}$, and the smallest prime factor $p$ of $a$, which is also a prime factor of $n$ because $p \mid a$ and $a \mid n$, satisfies $p \le a \le \sqrt{n}$. Figure 1 shows the idea as a rectangle. Its area is $n$, and a rectangle cannot have both sides longer than the side of the square of the same area, so the shorter side is at most $\sqrt{n}$.

**KEY RESULT A composite number has a small prime factor**

$$n \text{ composite} \quad \Longrightarrow \quad n \text{ has a prime factor } p \le \sqrt{n}$$

Turned around, if no prime up to $\sqrt{n}$ divides $n$, then $n$ is prime. This is the basis of **trial division**, the oldest primality test: divide $n$ by $2, 3, 5, 7, \ldots$ up to $\sqrt{n}$ and watch for a remainder of zero.

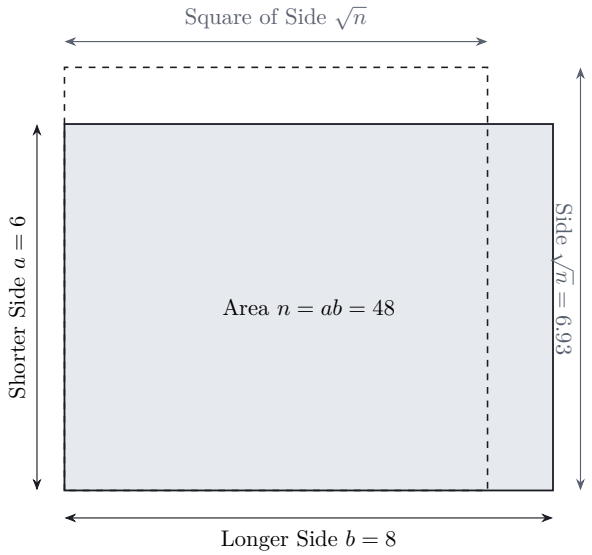



**Figure 1.** A composite number $n = ab$ drawn as a rectangle, here $48 = 6 \times 8$, together with the square of the same area. The shorter side $a$ never exceeds $\sqrt{n}$, so the smallest prime factor of $n$ is at most $\sqrt{n}$, which for 48 means at most 6.

Trial division does two jobs at once, because if a prime divides $n$, the quotient is a smaller number, the same procedure continues on it, and so the same method also factors $n$ completely. The next example does both jobs by hand.

**WORKED EXAMPLE Factoring 360 and 1001 by trial division**

For $n = 360$, the prime 2 divides it three times, since $360 = 2 \cdot 180$, $180 = 2 \cdot 90$, and $90 = 2 \cdot 45$. The quotient 45 is odd, and 3 divides it twice, $45 = 3 \cdot 15$ and $15 = 3 \cdot 5$. The last quotient, 5, is prime, so

$$360 = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 3 \cdot 5 = 2^3 \cdot 3^2 \cdot 5.$$

For $n = 1001$, the primes 2, 3, and 5 leave the remainders 1, 2, and 1. The prime 7 divides it, with $1001 = 7 \cdot 143$. The new quotient 143 needs to be tested only by primes up to $\sqrt{143} = 11.96\ldots$, and the primes below 7 need not be tried again, since they did not divide 1001. The prime 7 itself must be tried once more, because a prime can divide a number several times; here 7 leaves the remainder 3 on division of 143, while 11 divides it, with $143 = 11 \cdot 13$. Since 13 is prime, the factorizations are $360 = 2^3 \cdot 3^2 \cdot 5$ and $1001 = 7 \cdot 11 \cdot 13$.

The second example answers a yes-or-no question and shows how the bound $\sqrt{n}$ limits the work.

**WORKED EXAMPLE Is 10007 prime?**

Since $100^2 = 10000 < 10007 < 10201 = 101^2$, the square root of 10007 lies between 100 and 101, and only the primes up to 100 have to be tried. There are 25 of them (Section 2 lists them), and the remainders of 10007 on division by each are

1 (by 2), 2 (by 3), 2 (by 5), 4 (by 7), 8 (by 11), 10 (by 13), 11 (by 17), 13 (by 19), 2 (by 23), 2 (by 29), 25 (by 31), 17 (by 37), 3 (by 41), 31 (by 43), 43 (by 47), 43 (by 53), 36 (by 59), 3 (by 61), 24 (by 67), 67 (by 71), 6 (by 73), 53 (by 79), 47 (by 83), 39 (by 89), 16 (by 97).

None of the remainders is zero, so 10007 is prime. Twenty-five divisions settled a five-digit number. For a number with twenty digits the same method needs every prime up to $10^{10}$, of which there are about 455 million, and every two further digits multiply that count by nearly 10, and this is why Section 6 looks for something better.

**CHECK YOUR UNDERSTANDING Question 1**

None of the primes 2, 3, 5, 7, 11, 13, and 17 divides 437. What follows about 437?

(A) 437 is prime, because 17 is the last prime that needs to be tried

(B) 437 is prime, because $17 \times 17 = 289$ lies below 437, so no larger prime needs to be tried

(C) Nothing yet, because 19 is at most $\sqrt{437}$ and has not been tried

(D) Nothing yet, because every prime up to 437/2 must be tried

The solution is at the end of the unit.

## 2 The sieve of Eratosthenes

Trial division tests one number at a time. To list all the primes below a bound $N$, a different arrangement of the same work is far more efficient, and it is named after Eratosthenes of Cyrene (around 276 to 194 BC), the head of the library of Alexandria, who also measured the circumference of the Earth. The earliest surviving description is in the textbook Introduction to Arithmetic by Nicomachus of Gerasa (around AD 100), who attributes the method to Eratosthenes.

The **sieve of Eratosthenes** works as follows. Write down the integers from 2 to $N$. The smallest of

them, 2, is a prime; cross out all its multiples beyond itself. The smallest number still standing above 2 is 3, again a prime; cross out its multiples beyond itself, and continue in the same way. At every round the smallest number still standing that has not yet been used is a prime, because if it were composite it would be a multiple of some smaller number, and all those multiples have already been crossed out; its own multiples are crossed out next. Every number crossed out is a multiple of a smaller number and therefore composite, and every composite number is crossed out, because it is a multiple of its smallest prime factor, which is smaller than it. The numbers left standing at the end are exactly the primes up to $N$.

Two shortcuts follow from the observations of Section 1. When the multiples of a prime $p$ are crossed out, the crossing can start at $p^2$, because a smaller multiple $kp$ with $k < p$ has the factor $k$, every prime factor of $k$ is smaller than $p$, and so $kp$ was already crossed out in an earlier round. The same fact ends the sieve early. Once the current prime $p$ satisfies $p^2 > N$, every composite number up to $N$ has a prime factor below $p$ and has already been crossed out, so the sieve may stop. For $N = 100$ the sieve stops after the multiples of 7, since $11^2 = 121 > 100$.

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 1 | **2** | **3** | 4 | **5** | 6 | **7** | 8 | 9 | 10 |
| **11** | 12 | **13** | 14 | 15 | 16 | **17** | 18 | **19** | 20 |
| 21 | 22 | **23** | 24 | 25 | 26 | 27 | 28 | **29** | 30 |
| **31** | 32 | 33 | 34 | 35 | 36 | **37** | 38 | 39 | 40 |
| **41** | 42 | **43** | 44 | 45 | 46 | **47** | 48 | 49 | 50 |
| 51 | 52 | **53** | 54 | 55 | 56 | 57 | 58 | **59** | 60 |
| **61** | 62 | 63 | 64 | 65 | 66 | **67** | 68 | 69 | 70 |
| **71** | 72 | **73** | 74 | 75 | 76 | 77 | 78 | **79** | 80 |
| 81 | 82 | **83** | 84 | 85 | 86 | 87 | 88 | **89** | 90 |
| 91 | 92 | 93 | 94 | 95 | 96 | **97** | 98 | 99 | 100 |

Crossed Out: By 2 By 3 By 5 By 7

**Figure 2.** The sieve of Eratosthenes on the numbers 1 to 100. Each composite number is shaded in the grey of the prime that crossed it out first, and the 25 numbers left standing in black are the primes below 100. The number 1 is left out of the sieve. Own computation.

**WORKED EXAMPLE The sieve up to 100 step by step**

The list $2, 3, \ldots, 100$ has 99 entries. The multiples of 2 from 4 to 100 are 49 numbers, and crossing them out leaves 50. The smallest survivor above 2 is 3, and its multiples not yet crossed out are the odd multiples from 9 on, namely $9, 15, 21, \ldots, 99$, which are 16 numbers, so 34 remain. The next survivor is 5, whose multiples still standing are $25, 35, 55, 65, 85, 95$, and after these 6 are gone, 28 remain. The prime 7 removes 49, 77, and 91, leaving 25. The next survivor is 11, and $11^2 = 121$ exceeds 100, so the sieve stops. The survivors are

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97,$$

and there are 25 primes below 100. Figure 2 shows the same computation with the four rounds in four shades of grey.

**CHECK YOUR UNDERSTANDING Question 2**

The sieve of Eratosthenes is run on the numbers up to 1000. After the multiples of which prime have been crossed out may it stop?

(A) 29
(B) 31
(C) 37
(D) 499

The solution is at the end of the unit.

The sieve is also the simplest way to see how irregular the primes are. Figure 3 marks the 46 primes below 200 on a number line. Pairs that differ by 2, called twin primes, such as 101 and 103 or 197 and 199, sit next to stretches with no prime at all, such as the 13 composite numbers between 113 and 127. There is no visible rule for where the next prime falls, and no usable formula is known that produces the primes in order. What can be said is how many there are on average. The sieve gives 25 primes below 100, 168 below 1000, 1229 below 10,000, and 78,498 below one million, so the primes thin out, but slowly; Unit 8 says how many primes there are below a given size and why.

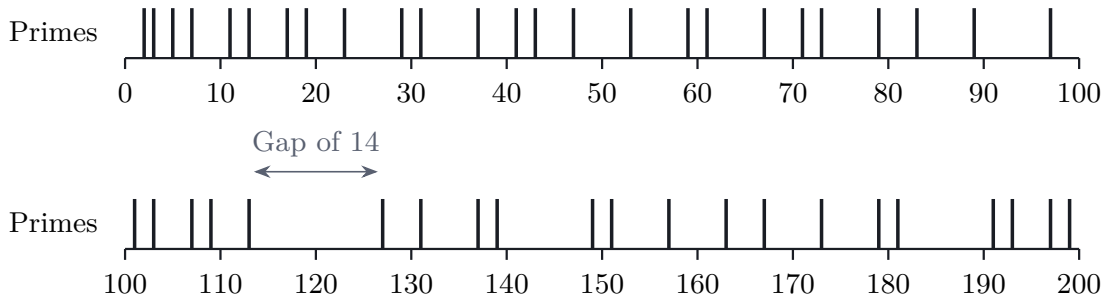



**Figure 3.** The primes below 200, found by the sieve, marked on a number line. The longest run without a prime below 200 is the gap of 14 between 113 and 127, while 197 and 199 differ by only 2. Own computation.

**INTERACTIVE The sieve of Eratosthenes**

| | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | **2** | **3** | 4 | **5** | 6 | **7** | 8 | **9** | 10 | **11** | 12 | **13** | 14 | **15** | 16 | **17** | 18 | **19** | 20 |
| **21** | 22 | **23** | 24 | **25** | 26 | **27** | 28 | **29** | 30 | **31** | 32 | **33** | 34 | **35** | 36 | **37** | 38 | **39** | 40 |
| **41** | 42 | **43** | 44 | **45** | 46 | **47** | 48 | **49** | 50 | **51** | 52 | **53** | 54 | **55** | 56 | **57** | 58 | **59** | 60 |
| **61** | 62 | **63** | 64 | **65** | 66 | **67** | 68 | **69** | 70 | **71** | 72 | **73** | 74 | **75** | 76 | **77** | 78 | **79** | 80 |
| **81** | 82 | **83** | 84 | **85** | 86 | **87** | 88 | **89** | 90 | **91** | 92 | **93** | 94 | **95** | 96 | **97** | 98 | **99** | 100 |
| **101** | 102 | **103** | 104 | **105** | 106 | **107** | 108 | **109** | 110 | **111** | 112 | **113** | 114 | **115** | 116 | **117** | 118 | **119** | 120 |
| **121** | 122 | **123** | 124 | **125** | 126 | **127** | 128 | **129** | 130 | **131** | 132 | **133** | 134 | **135** | 136 | **137** | 138 | **139** | 140 |
| **141** | 142 | **143** | 144 | **145** | 146 | **147** | 148 | **149** | 150 | **151** | 152 | **153** | 154 | **155** | 156 | **157** | 158 | **159** | 160 |
| **161** | 162 | **163** | 164 | **165** | 166 | **167** | 168 | **169** | 170 | **171** | 172 | **173** | 174 | **175** | 176 | **177** | 178 | **179** | 180 |
| **181** | 182 | **183** | 184 | **185** | 186 | **187** | 188 | **189** | 190 | **191** | 192 | **193** | 194 | **195** | 196 | **197** | 198 | **199** | 200 |

Choose how far the sieve runs and press the button once for every prime: the multiples of the current prime are crossed out in a new shade, starting at its square. Watch the count of numbers still standing and the moment the square of the next prime exceeds the bound, after which nothing more is crossed out and every survivor is a prime.

Click the picture or this link to try it in the online version of this unit.

## 3 The fundamental theorem of arithmetic

Figure 4 shows two ways of breaking 360 into factors. One starts with $360 = 36 \times 10$, the other with $360 = 8 \times 45$, and the two trees look different at every level, yet both end with the same primes: three 2s, two 3s, and one 5. Everyone who has factored numbers at school takes this for granted. It is a theorem, and its proof needs a fact about primes that is far from obvious.

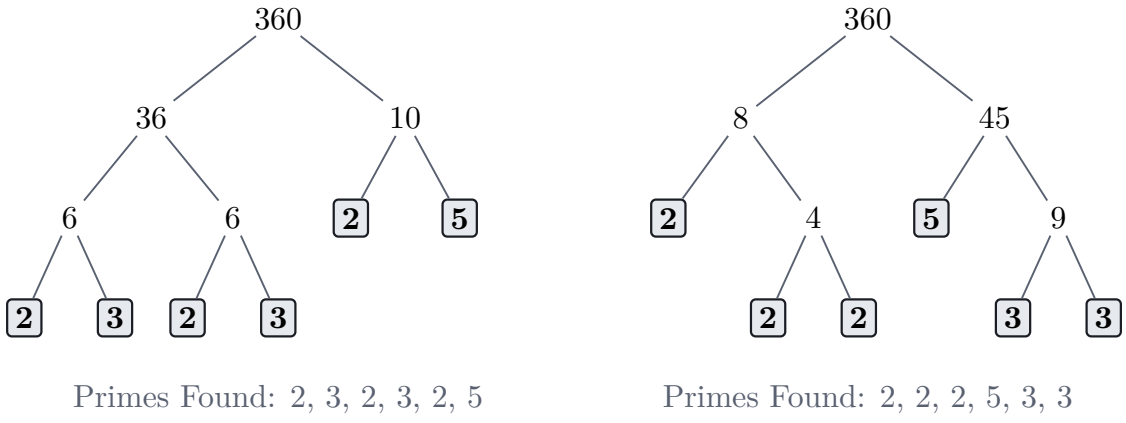



**Figure 4.** Two factor trees of 360. The splits differ at every level, but both trees end with the primes $2, 2, 2, 3, 3, 5$, as the fundamental theorem of arithmetic promises.

The fact is this: a prime that divides a product must divide one of the factors. For composite numbers the corresponding statement is false, since 6 divides $4 \cdot 9 = 36$ and divides neither 4 nor 9. For primes it is true, and it goes back to Book VII of Euclid's Elements.

**THEOREM Euclid's lemma**

If a prime $p$ divides a product $ab$ of two integers, then $p \mid a$ or $p \mid b$. More generally, if $p$ divides a product $a_1 a_2 \cdots a_k$, then $p$ divides at least one of the factors.

The proof uses Bézout's identity from Unit 2 in the form proved there: if $d \mid ab$ and $\gcd(d, a) = 1$, then $d \mid b$. Suppose $p \mid ab$ and $p \nmid a$. The only positive divisors of $p$ are 1 and $p$, and $p$ is not a divisor of $a$, so $\gcd(p, a) = 1$, and the result from Unit 2 gives $p \mid b$. The statement for $k$ factors follows by induction on $k$, since $p \mid a_1(a_2 \cdots a_k)$ means that $p$ divides $a_1$ or divides the product of the remaining $k - 1$ factors, and in the second case the statement for $k - 1$ factors, already proved, names one of them.

With the lemma in hand, the theorem that gives the unit its title can be stated and proved. It appears in Euclid's Elements only in special cases; the first complete statement and proof are in the book Disquisitiones Arithmeticae (1801) of Carl Friedrich Gauss (1777-1855).

**THEOREM The fundamental theorem of arithmetic**

Every integer $n > 1$ can be written as a product of primes,

$$n = p_1 p_2 \cdots p_k \qquad (k \geq 1),$$

and this representation is unique apart from the order of the factors: if also $n = q_1 q_2 \cdots q_m$ with primes $q_j$, then $m = k$ and the $q_j$ are the $p_i$ in some order.

The theorem has two halves, existence and uniqueness, and they are proved by different means. Existence uses strong induction, which Unit 1 introduced, and uniqueness uses Euclid's lemma.

**PROOF Proof of the fundamental theorem of arithmetic**

*Existence, by strong induction on $n$.* The base case is $n = 2$, which is a prime and hence a product of one prime. For the induction step let $n > 2$ and assume that every integer from 2 to $n - 1$ is a product of primes. If $n$ is prime, it is a product of one prime. If $n$ is composite, then $n = ab$ with $1 < a, b < n$, and by the assumption both $a$ and $b$ are products of primes. Writing the two products one after the other gives $n$ as a product of primes.

*Uniqueness, by matching the factors one by one.* Suppose that

$$p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_m$$

with all $p_i$ and $q_j$ prime, and suppose that $k \leq m$, which costs nothing, since otherwise the two sides can be swapped. The prime $p_1$ divides the left side, so it divides the product on the right, and by Euclid's lemma it divides one of the $q_j$. Renumber the $q_j$ so that $p_1 \mid q_1$. Since $q_1$ is prime, its only divisor greater than 1 is $q_1$ itself, so $p_1 = q_1$. Cancelling this common factor leaves

$$p_2 \cdots p_k = q_2 \cdots q_m,$$

an equation with fewer factors on each side. Repeating the argument matches $p_2$ with one of the remaining $q_j$, then $p_3$, and so on. After $k$ steps the left side has become the empty product, which by convention equals 1, and the right side is $q_{k+1} \cdots q_m$. A product of primes is at least 2 unless it is empty, so $m = k$, and every $p_i$ has been matched with a $q_j$. The two factorizations therefore agree apart from order, which completes the proof.

The argument deserves a second look at the one place where it could fail. In the uniqueness half, $p_1 \mid q_1 q_2 \cdots q_m$ had to force $p_1$ to divide a single $q_j$. That step is Euclid's lemma, which rests on Bézout's identity, which rests on division with remainder, and the whole theorem hangs on that chain. The excursion below shows a number system in which the chain breaks.

Because the factors can be collected, the theorem has a standard shorthand. Grouping equal primes and

ordering them by size gives the **canonical factorization**.

**KEY RESULT Canonical factorization**

$$n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}, \qquad p_1 < p_2 < \cdots < p_k \text{ primes}, \quad e_i \geq 1$$

Every integer $n > 1$ has exactly one such representation. For $n = 1$ the product is empty. The exponent of a prime $p$ in $n$ is written $v_p(n)$ (later courses call it the $p$-adic valuation of $n$), with $v_p(n) = 0$ when $p \nmid n$; for example $360 = 2^3 \cdot 3^2 \cdot 5$ has $v_2(360) = 3$, $v_5(360) = 1$, and $v_7(360) = 0$.

The exponent notation obeys one rule that is used constantly. For positive integers $a$ and $b$, the factorization of $ab$ is the product of the factorizations of $a$ and $b$, and by uniqueness it is the only factorization of $ab$, so

$$v_p(ab) = v_p(a) + v_p(b) \qquad \text{for every prime } p. \tag{1}$$

**EXCURSION** *Where unique factorization fails*

A small example of a kind that David Hilbert (1862-1943) used in his lectures on number theory in the 1890s shows that uniqueness is not a law of nature. Take only the numbers $1, 5, 9, 13, 17, 21, \ldots$, that is, the positive integers that leave the remainder 1 on division by 4. The product of two such numbers is again such a number, because $(4a+1)(4b+1) = 4(4ab+a+b)+1$, so multiplication never leaves the set. Call a number in the set other than 1 "unbreakable" if it is not a product of two smaller numbers of the set. The numbers $5, 9, 13, 17, 21$ are unbreakable, since for example $9 = 3 \cdot 3$ and $21 = 3 \cdot 7$ use factors outside the set, and so is 49, since $49 = 7 \cdot 7$ and 7 is not in the set. Every number in the set is a product of unbreakable ones, by the same strong induction as above. Uniqueness, however, fails:

$$441 = 9 \times 49 = 21 \times 21,$$

and 9, 21, and 49 are three different unbreakable numbers. The failure sits exactly where the proof said it would. Euclid's lemma is false in this set, because 9 divides $21 \times 21$ without dividing 21. The reason it fails is that the set has no division with remainder. There is no way to write $21 = 9q + r$ with $q$ and $r$ in the set and $r < 9$, since $q = 1$ leaves $r = 12$ and $q = 5$ already overshoots, so the chain that led from division with remainder to Bézout's identity and from there to the lemma cannot even start.

Hilbert's set is artificial, but the same failure occurs in number systems that mathematicians need. Among the numbers $a + b\sqrt{-5}$ with integers $a$ and $b$, where $\sqrt{-5}$ is an imaginary number whose square is $-5$, the number 6 has the two factorizations $6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$, and none of the four factors can be split further. Such number systems are where the nineteenth century looked for a proof of Fermat's Last Theorem and where the search went wrong until the failure of uniqueness was understood. That theory lies beyond this unit, but the moral belongs here. In the ordinary integers, unique factorization is a theorem, and the proof above is the reason it holds.

**CHECK YOUR UNDERSTANDING Question 3**

In the set 1, 5, 9, 13, 17, and so on, the number 441 has the two factorizations $9 \times 49$ and $21 \times 21$. Which step of the uniqueness proof fails for these numbers?

(A) The existence of a factorization into unbreakable numbers

(B) The strong induction that builds factorizations of larger numbers

(C) Euclid's lemma: 9 divides $21 \times 21$ but divides neither factor

(D) The well-ordering principle that gives a smallest divisor

The solution is at the end of the unit.

# 4 Reading the factorization

Once $n$ is written in canonical form, questions about its divisors become questions about exponents. The link is that an integer $d > 0$ divides $n$ if and only if $v_p(d) \le v_p(n)$ for every prime $p$. In one direction, if $d \mid n$, then $n = dc$ and Equation (1) gives $v_p(n) = v_p(d) + v_p(c) \ge v_p(d)$. In the other direction, if all exponents of $d$ are at most those of $n$, then $n/d$ is the integer with exponents $v_p(n) - v_p(d)$, so $d$ divides $n$. So the divisors of $n = p_1^{e_1} \cdots p_k^{e_k}$ are exactly the numbers $p_1^{f_1} \cdots p_k^{f_k}$ with $0 \le f_i \le e_i$. For example, the divisor $18 = 2^1 \cdot 3^2 \cdot 5^0$ of $360 = 2^3 \cdot 3^2 \cdot 5$ chooses the exponents 1, 2, and 0. For each prime there are $e_i + 1$ choices of exponent, and the choices are independent, which counts the divisors at once.

**KEY RESULT The number of divisors**

$$d(n) = (e_1 + 1)(e_2 + 1) \cdots (e_k + 1) \qquad \text{for } n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$$

Here $d(n)$ is the number of positive divisors of $n$. For example $360 = 2^3 \cdot 3^2 \cdot 5$ has $4 \cdot 3 \cdot 2 = 24$ divisors. Unit 6 develops this function and its relatives.

## 4.1 Greatest common divisor and least common multiple

A common divisor $d$ of $a$ and $b$ must satisfy $v_p(d) \le v_p(a)$ and $v_p(d) \le v_p(b)$ for every $p$, and the largest such $d$ takes the smaller of the two exponents at each prime. A common multiple must have exponents at least as large as both, and the smallest takes the larger of the two.

**KEY RESULT Greatest common divisor and least common multiple from exponents**

$$v_p\big(\gcd(a,b)\big) = \min\big(v_p(a), v_p(b)\big), \qquad v_p\big(\operatorname{lcm}(a,b)\big) = \max\big(v_p(a), v_p(b)\big)$$

The rule holds for every prime $p$, including the primes that divide only one of the numbers, where the smaller exponent is 0. Since $\min(x,y) + \max(x,y) = x + y$ for any two numbers, the identity $\gcd(a,b) \cdot \operatorname{lcm}(a,b) = ab$ of Unit 2 follows at once.

**WORKED EXAMPLE The gcd and lcm of 360 and 84 in two ways**

Trial division gives $360 = 2^3 \cdot 3^2 \cdot 5$ and $84 = 2^2 \cdot 3 \cdot 7$. Taking the smaller exponent of each prime, the greatest common divisor is $2^2 \cdot 3^1 \cdot 5^0 \cdot 7^0 = 12$, and taking the larger, the least common multiple is $2^3 \cdot 3^2 \cdot 5 \cdot 7 = 2520$. Euclid's algorithm of Unit 2 confirms the first value without any factoring: $360 = 4 \cdot 84 + 24$, then $84 = 3 \cdot 24 + 12$, then $24 = 2 \cdot 12$, so the last non-zero

remainder is 12. The identity $\gcd \cdot \operatorname{lcm} = ab$ confirms the second, since $360 \cdot 84/12 = 2520$. Hence $\gcd(360, 84) = 12$ and $\operatorname{lcm}(360, 84) = 2520$.

For two numbers of modest size, the exponent rule and Euclid's algorithm cost about the same. For two numbers of three hundred digits the difference is enormous: Euclid's algorithm finishes in at most 1500 steps by Lamé's bound of Unit 2, which allows five steps for every decimal digit, whereas nobody can factor the numbers. The exponent rule is a way of understanding the gcd, and Euclid's algorithm is the way of computing it.

## 4.2 Square roots

Unit 1 proved that $\sqrt{2}$ is irrational by an argument about even and odd numbers. Unique factorization turns that argument into a rule for every integer. Suppose $\sqrt{n} = a/b$ with positive integers $a$ and $b$. Squaring and clearing the denominator gives $nb^2 = a^2$, and Equation (1) applied to both sides gives, for every prime $p$,

$$v_p(n) + 2\,v_p(b) = 2\,v_p(a).$$

The right side is even and $2v_p(b)$ is even, so $v_p(n)$ is even for every prime $p$, which means that $n$ is the square of the integer $\prod p^{v_p(n)/2}$, the product over the primes dividing $n$ of each prime raised to half its exponent (the product sign $\prod$ is the one Unit 1 introduced). In words, the square root of a positive integer is either an integer or irrational, and nothing in between. For example, $12 = 2^2 \cdot 3$ has $v_3(12) = 1$, which is odd, so $\sqrt{12}$ is irrational, and the same reasoning with cube roots and $3v_p(b)$ shows that $\sqrt[3]{n}$ is irrational unless $n$ is a cube.

## 4.3 The exponent of a prime in a factorial

How many times does $p$ divide the factorial $n! = 1 \cdot 2 \cdot 3 \cdots n$? Among the factors $1, 2, \ldots, n$, every $p$-th one is a multiple of $p$, so there are $\lfloor n/p \rfloor$ of them, where $\lfloor x \rfloor$ is the floor of $x$, the largest integer not exceeding $x$ (Unit 1). That is not the whole count, because the multiples of $p^2$ contribute a second factor $p$ each, the multiples of $p^3$ a third, and so on. Adrien-Marie Legendre (1752-1833) wrote the resulting formula in his book Essai sur la théorie des nombres (second edition, 1808).

**THEOREM Legendre's formula**

For a prime $p$ and a positive integer $n$,

$$v_p(n!) = \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \cdots,$$

where the sum ends as soon as $p^k > n$, since from then on every term is 0.

**PROOF Proof of Legendre's formula**

By Equation (1), applied to the product $1 \cdot 2 \cdots n$, the exponent $v_p(n!)$ is the sum of $v_p(m)$ over $m = 1, 2, \ldots, n$. Count this sum in a different order. A factor $m$ with $v_p(m) = j$ is a multiple of $p$, of $p^2$, and so on up to $p^j$, so it is counted once in each of the first $j$ of the sets

$$\{m \le n : p \mid m\}, \quad \{m \le n : p^2 \mid m\}, \quad \{m \le n : p^3 \mid m\}, \quad \ldots$$

and in no later set. Adding the sizes of all these sets therefore counts every $m$ exactly $v_p(m)$ times, and the total is $v_p(n!)$. The $k$-th set consists of the multiples $p^k, 2p^k, \ldots$ up to $n$, and there are $\lfloor n/p^k \rfloor$ of them, which gives the formula and completes the proof.

**WORKED EXAMPLE The number of zeros at the end of 100!**

A number ends with as many zeros as the number of times $10 = 2 \cdot 5$ divides it, and since every factor 10 needs one 2 and one 5, that number is the smaller of $v_2$ and $v_5$. Legendre's formula gives

$$v_5(100!) = \left\lfloor \frac{100}{5} \right\rfloor + \left\lfloor \frac{100}{25} \right\rfloor + \left\lfloor \frac{100}{125} \right\rfloor = 20 + 4 + 0 = 24$$

and

$$v_2(100!) = \left\lfloor \frac{100}{2} \right\rfloor + \left\lfloor \frac{100}{4} \right\rfloor + \left\lfloor \frac{100}{8} \right\rfloor + \left\lfloor \frac{100}{16} \right\rfloor + \left\lfloor \frac{100}{32} \right\rfloor + \left\lfloor \frac{100}{64} \right\rfloor = 50 + 25 + 12 + 6 + 3 + 1 = 97.$$

The factor 5 is the scarcer one, so 100! is divisible by $10^{24}$ and not by $10^{25}$, and it ends with 24 zeros. The number itself has 158 digits, about two lines of this page; the last 24 are known without writing down a single one of the others.

Beyond this unit, Legendre's formula serves in a different role, as a tool for estimating how many primes there are below a given size. For now it is the first example of a principle that runs through the whole subject: a statement about a huge number, here 100!, can often be settled by counting its prime factors instead of computing it.

**CHECK YOUR UNDERSTANDING Question 4**

What is $v_2(20!)$, the exponent of 2 in the factorization of 20!?

(A) 10
(B) 15
(C) 18
(D) 20

The solution is at the end of the unit.

## 5 Euclid's theorem

The sieve produces as many primes as patience allows, but no amount of sieving shows that the supply never ends. The proof that it does not is Proposition 20 of Book IX of Euclid's Elements (around 300 BC), and it is one of the oldest proofs in mathematics that is still taught in its original form.

**THEOREM Euclid's theorem**

There are infinitely many primes. Equivalently, no finite list of primes contains all of them.

**PROOF Euclid's proof**

Let $p_1, p_2, \ldots, p_k$ be any finite list of primes, and form the number

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

Since $N > 1$, the Key Result of Section 1 gives $N$ a prime factor $q$. This $q$ is not in the list. For if $q$ were one of the $p_i$, then $q$ would divide the product $p_1 p_2 \cdots p_k$, and since $q$ also divides $N$, it would divide the difference $N - p_1 p_2 \cdots p_k = 1$, which no prime does. So every finite list of primes misses at least one

prime, which means the primes cannot be listed in full, and this completes the proof.

Euclid (active around 300 BC) stated the result as "prime numbers are more than any assigned multitude of prime numbers" and proved it for a list of three primes, which is the general case in the notation of his time. His argument is not a proof by contradiction, although it is often retold as one. It is a direct construction: given any primes, it points at a number whose prime factors are new. The construction does not say that $N$ itself is prime, and usually it is not.

**WORKED EXAMPLE The numbers of Euclid's proof**

Starting from the first primes, the numbers $N$ are $2+1=3$, then $2\cdot3+1=7$, then $2\cdot3\cdot5+1=31$, then 211, then 2311, and all five are prime. The sixth is

$$2\cdot3\cdot5\cdot7\cdot11\cdot13+1=30031,$$

and trial division up to $\sqrt{30031}=173.3\ldots$ finds the factor 59, with $30031=59\cdot509$, and 509 is prime. So $30031=59\times509$ is composite, and its two prime factors are new, exactly as the proof requires. The proof never promised more. It guarantees a new prime among the factors of $N$, and gives no rule for finding that prime other than factoring $N$, which is why Euclid's theorem produces no formula for the primes.

The same idea reaches a little further. Every odd prime leaves the remainder 1 or 3 on division by 4, because the remainders 0 and 2 belong to even numbers, and the list $3, 7, 11, 19, 23, 31, \ldots$ of primes with remainder 3 is also endless.

**PROOF Infinitely many primes of the form 4k + 3**

Let $p_1, \ldots, p_k$ be a finite list of primes that leave the remainder 3 on division by 4, and form

$$N=4p_1p_2\cdots p_k-1.$$

Then $N$ is odd and leaves the remainder 3 on division by 4, because $N+1$ is a multiple of 4. Write $N$ as a product of primes. All of them are odd, so each leaves the remainder 1 or 3. They cannot all leave the remainder 1, because a product of numbers of the form $4a+1$ is again of that form, as the excursion of Section 3 showed, and $N$ is not. So some prime factor $q$ of $N$ leaves the remainder 3. This $q$ is not in the list, because if it were one of the $p_i$, it would divide both $N$ and $N+1$, hence their difference 1. Thus every finite list of such primes misses one, which completes the proof.

The primes with remainder 1, namely $5, 13, 17, 29, \ldots$, are also infinite in number, but the trick with $N$ does not reach them, and a different idea is needed, which is beyond this unit. The general statement, that every progression $a, a+q, a+2q, \ldots$ with $\gcd(a,q)=1$ contains infinitely many primes (the condition is needed, since otherwise every term is divisible by $\gcd(a,q)$), is Dirichlet's theorem on primes in arithmetic progressions, proved by Peter Gustav Lejeune Dirichlet (1805-1859) in 1837 with tools from analysis that lie far beyond this masterclass.

## 6 Recognizing primes and factoring them

Two questions look alike and are not. The first asks whether a given $n$ is prime; the second asks for its factors. Trial division answers both, but at a price of up to about $\sqrt{n}$ divisions, and $\sqrt{n}$ grows by a factor of 10 for every two digits added to $n$. A 50-digit number needs $10^{25}$ divisions, which no computer will finish; at a billion divisions a second, that would take about 300 million years. This section shows that the first question has a fast answer, that the second does not, as far as anyone knows, and that the gap between the two is what modern cryptography is built on.

## 6.1 Mersenne primes and the Lucas-Lehmer test

Nearly every record prime of the computer age has the form $2^p - 1$; such numbers are named **Mersenne numbers** after Marin Mersenne (1588-1648), a French monk who corresponded with most of the mathematicians of his time and published a list of the exponents he believed gave primes. If $2^n - 1$ is prime, then $n$ must be prime; Unit 6 proves this with an algebraic identity. The converse, that $2^p - 1$ is prime for every prime $p$, is false, as the example $2^{11} - 1 = 2047 = 23 \times 89$ shows. The reason these numbers are the record holders is that a prime of this special form can be recognized far faster than a general number of the same size.

**KEY RESULT The Lucas-Lehmer test**

$$s_0 = 4, \qquad s_{k+1} \equiv s_k^2 - 2 \pmod{M_p},$$
$$M_p = 2^p - 1 \text{ is prime} \iff s_{p-2} \equiv 0 \pmod{M_p}$$

The notation $x \equiv y \pmod{M_p}$ means that $x$ and $y$ leave the same remainder on division by $M_p$; Unit 4 develops it. For an odd prime $p$, compute the sequence $s_k$ modulo $M_p$, keeping only remainders, for $p - 2$ steps. The Mersenne number $M_p$ is prime exactly when the last remainder is 0. The test was devised by Édouard Lucas (1842-1891) and put into this form by Derrick Henry Lehmer (1905-1991) in 1930; its proof needs algebra beyond this unit.

For $p = 7$ and $M_7 = 127$ the remainders are $s_0 = 4$, $s_1 = 14$, $s_2 = 194 - 127 = 67$, $s_3 = 67^2 - 2 = 4487 \equiv 42$, $s_4 = 42^2 - 2 = 1762 \equiv 111$, and $s_5 = 111^2 - 2 = 12319 = 97 \cdot 127 \equiv 0$, so 127 is prime. Five squarings replaced the trial divisions. For $p = 136{,}279{,}841$ the test needs about 136 million squarings of numbers with 41 million digits, which is a large computation and a possible one, whereas trial division of a number of that size is not possible in the lifetime of the universe. Table 1 lists a selection of the 52 Mersenne primes known in October 2024, with the largest known prime, $2^{136279841} - 1$, at the end.

| Exponent $p$ | Digits | Year | Found By | Method |
|---|---|---|---|---|
| 17 | 6 | 1588 | P. Cataldi | trial division |
| 31 | 10 | 1772 | L. Euler | trial division |
| 127 | 39 | 1876 | É. Lucas | Lucas's test, by hand |
| 521 | 157 | 1952 | R. Robinson | Lucas-Lehmer, SWAC |
| 11,213 | 3376 | 1963 | D. Gillies | Lucas-Lehmer, ILLIAC II |
| 1,398,269 | 420,921 | 1996 | J. Armengaud, GIMPS | Lucas-Lehmer, home PC |
| 82,589,933 | 24,862,048 | 2018 | P. Laroche, GIMPS | Lucas-Lehmer, home PC |
| 136,279,841 | 41,024,320 | 2024 | L. Durant, GIMPS | probable-prime test, GPUs |

**Table 1.** Eight of the 52 known Mersenne primes $2^p - 1$, with the number of decimal digits of each, from the first proved by trial division to the largest known prime, found on 12 October 2024. Data from the GIMPS list of known Mersenne primes, mersenne.org.

## 6.2 Recognizing against factoring

A Mersenne number is a special case. For a general $n$, the fast tests in use rest on Fermat's little theorem, which Unit 5 proves: for a prime $p$ and an integer $a$ not divisible by $p$, the power $a^{p-1}$ leaves the remainder 1 on division by $p$. A number that fails this for some $a$ is certainly composite, and the test says so without producing a factor. Unit 5 shows how the idea is refined into the tests with which software finds primes of 300 digits, the building blocks of the RSA keys that encrypt internet traffic, which Unit 5 also explains, in a fraction of a second each.

Factoring has no such shortcut. The best known methods are far better than trial division, but they still take time that grows faster than any power of the number of digits. The record for a number with two prime factors of equal size is RSA-250, a number of 250 decimal digits (829 binary digits), factored

in February 2020 by a team of French and American researchers. The computation took about 2700 core-years, which means that a single processor core would have needed 2700 years, and the work was spread over thousands of cores for several months. For comparison, the primality of a 250-digit number is decided in milliseconds.

The scale of the two tasks is best described with the number of digits of $n$, which Unit 1 wrote as $\lfloor \log_{10} n \rfloor + 1$. An algorithm runs in **polynomial time** if the number of steps it needs is bounded by a fixed power of the number of digits, such as the square or the cube. Adding, multiplying, and Euclid's algorithm are all polynomial. Trial division is not, since $\sqrt{n}$ is about $10^{D/2}$ for a $D$-digit number, which grows faster than any power of $D$. The fast primality tests based on Fermat's theorem are polynomial, but for decades every one of them either used random choices or relied on an unproved conjecture. Whether primality could be decided in polynomial time with no randomness and no conjecture was an open question until 2002, and it is the subject of the research spotlight below.

RESEARCH SPOTLIGHT

**Manindra Agrawal** *Indian Institute of Technology Kanpur*

**Deciding whether a number is prime in polynomial time, without factoring it**

In August 2002 Manindra Agrawal of IIT Kanpur and two of his undergraduate students, Neeraj Kayal and Nitin Saxena, announced an algorithm that decides whether a number $n$ is prime in a number of steps bounded by a power of the number of digits of $n$, with no random choices and no unproved assumption. The paper appeared in the Annals of Mathematics in 2004 as "PRIMES is in P", P being the name computer scientists give to the problems solvable in polynomial time.

The test rests on a cousin of Fermat's little theorem: for a prime $n$ and an integer $a$ coprime to $n$, the polynomial $(X + a)^n$ agrees with $X^n + a$ once all coefficients are reduced modulo $n$, whereas for a composite $n$ some coefficient survives. For example, $(X + 1)^3 = X^3 + 3X^2 + 3X + 1$, and the two middle coefficients are multiples of 3, so modulo 3 only $X^3 + 1$ remains. Checking all $n$ coefficients would take far too long, so the authors reduce both sides modulo $X^r - 1$ for a small $r$ and prove, by counting arguments, that a composite $n$ cannot pass the reduced test for all the small values of $a$ they prescribe. The published version needs a number of steps bounded by roughly the tenth and a half power of the number of digits (the exponent is 10.5, up to logarithmic factors), and a variant by Lenstra and Pomerance of 2005 brought the exponent down to 6. The result matters for what it settles: primality can be decided efficiently in the strictest sense, while factoring, as far as anyone knows, cannot. The introduction of the paper, a survey of a century of primality tests, can be read with the knowledge of this unit.

**Read the paper:** Agrawal, Kayal, and Saxena (2004), PRIMES is in P, Annals of Mathematics 160, 781 to 793




**Figure 5.** Lehmer sieves at the Computer History Museum in Mountain View, California. Each loop or wheel in such a machine stands for one small modulus and carries holes at the remainders that are allowed; the machine advances all of them in step and signals when a hole of every one lines up. Credit: Carlo Nardone, Wikimedia Commons, CC BY-SA 2.0.

### EXCURSION *Hunting the largest prime*

On 10 January 1876 Lucas announced that $2^{127} - 1$, a number of 39 digits, is prime. He had invented the test on which the squarings described above are based, and he carried it out by hand. The number remained the largest known prime until 1951, and it is still the largest prime ever proved by hand.

The next tools were mechanical. Derrick Henry Lehmer, following an idea of his father Derrick Norman Lehmer (1867-1938), who had published tables of primes and factors up to ten million, built a series of sieving machines at Berkeley from 1926 on. The first, of 1926, used bicycle chains of different lengths turning on a shaft, with pegs on the links that closed electrical contacts; a version of 1932 used gear wheels with holes that let a beam of light through only when all the wheels were in the right position, and one of 1936 used loops of 16 millimetre film. Figure 5 shows machines of this family. They searched for numbers that satisfied many conditions on remainders at once, thousands of candidates per second, and the Lehmers used them to find factors of Mersenne numbers and of other numbers of special form.

Electronic computers took over in 1952, when Raphael Robinson found five Mersenne primes in one year on the SWAC, an early electronic computer in Los Angeles. Since 1996 the Great Internet Mersenne Prime Search (GIMPS), a network of volunteers running free software on their own machines, has found every new record, eighteen primes so far. The current record, $2^{136279841} - 1$ with 41,024,320 digits, was found by Luke Durant on 12 October 2024 on a cloud of graphics processors in 17 countries, the first record prime not found on an ordinary personal computer since 1996. Printed at 3500 digits a page, the number would fill about 12,000 pages.

### KEY POINTS

- An integer $n > 1$ is prime if its only positive divisors are 1 and $n$; the number 1 is neither prime nor composite. Every $n > 1$ has a prime factor, and if $n$ is composite, it has one at most $\sqrt{n}$.
- The sieve of Eratosthenes lists all primes up to $N$ by crossing out multiples, starting at $p^2$ for

each prime $p$, and may stop as soon as $p^2 > N$. There are 25 primes below 100 and 168 below 1000.

- The fundamental theorem of arithmetic: every integer greater than 1 is a product of primes in exactly one way apart from order. Existence comes from strong induction, uniqueness from Euclid's lemma, which comes from Bézout's identity.
- From the exponents $v_p(n)$ one reads off the divisors, $d(n) = \prod(e_i + 1)$, the gcd and lcm by min and max, whether $\sqrt{n}$ is rational, and, by Legendre's formula $v_p(n!) = \sum_k \lfloor n/p^k \rfloor$, the exponent of $p$ in $n!$.
- Euclid's theorem: the primes never end, because $p_1 \cdots p_k + 1$ has a prime factor outside any finite list, although it need not be prime itself ($30031 = 59 \times 509$).
- Deciding whether $n$ is prime is fast, in polynomial time since 2002, while factoring $n$ is not known to be; the largest known prime has 41 million digits, the factoring record 250.

Solutions to the questions in the text: 1-C, 2-B, 3-C, 4-C. The online version of this unit explains each answer.