

---

## Divisibility

An integer  $d$  **divides** an integer  $n$  if  $n \% d = 0$ . In that situation  $n$  is a **multiple** of  $d$ . The notation is

$$d|n$$

For example

$$5|10 \quad 35|105 \quad 2 \nmid 5$$

where the last illustrates the slash to denote *does not divide*.

In more colloquial terms, to say  $d$  divides  $n$  is to say that  $d$  divides  $n$  *evenly*, but for us that qualification is always implied.

A **proper divisor**  $d$  of  $n$  is a divisor of  $n$  in the range

$$1 < d < n$$

An integer  $p > 1$  with no proper divisors is a **prime**. It is a universal convention, and is very convenient, to say that 1 is *not* prime.

That is,  $N$  is prime if there is no  $d$  in the range  $1 < d < N$  with  $d|N$ , and if  $N > 1$ .

Non-prime numbers bigger than 1 are called **composite**. The number 1 is neither prime nor composite, evidently.

**Theorem:** *unique factorization of integers into primes:* for a positive integer  $n$  there is a unique expression

$$n = p_1^{e_1} p_2^{e_2} \dots p_t^{e_t}$$

where the  $p_i$  are primes with

$$p_1 < p_2 < \dots < p_t$$

and the exponents  $e_i$  are positive integers.

For example,

2	=	prime
3	=	prime
4	=	$2^2$
5	=	prime
6	=	$2 \cdot 3$
7	=	prime
8	=	$2^3$
9	=	$3^2$
10	=	$2 \cdot 5$
11	=	prime
12	=	$2^2 \cdot 3$
13	=	prime
14	=	$2 \cdot 7$
15	=	$3 \cdot 5$
16	=	$2^4$
17	=	prime
18	=	$2 \cdot 3^2$
19	=	prime
20	=	$2^2 \cdot 5$
21	=	$3 \cdot 7$

## **Trial division**

*Trial division* is the basic method *both* to test whether integers are prime or not, and to obtain the factorization of integers into primes.

This is basically a brute force search for proper divisors, but knowing when we can stop. Note that, if  $d < N$  and  $d|N$  and  $d > \sqrt{N}$ , then  $\frac{N}{d}$  is *also* a divisor of  $N$  and  $1 < \frac{N}{d} \leq \sqrt{N}$ . Thus, in looking for *proper* divisors it suffices to stop looking at  $d \leq \sqrt{N}$ .

Thus, for example, to test whether  $N$  is *prime*

Compute  $N \% 2$

If  $N \% 2 = 0$ , stop,  $N$  composite

Else if  $N \% 2 \neq 0$ , continue

Initialize  $d = 3$ .

While  $d \leq \sqrt{N}$ :

    Compute  $N \% d$

    If  $N \% d = 0$ , **stop**,  $N$  composite

    Else if  $N \% d \neq 0$ ,

        Replace  $d$  by  $d + 2$ , continue

If reach  $d > \sqrt{N}$  without termination,

$N$  is prime

This takes at worst  $\sqrt{N}/2$  steps to confirm or deny the primality of  $N$ .

For example, to test  $N = 59$  for primality:

Compute  $59 \% 2 = 1$

Since  $59 \% 2 \neq 0$ , continue

Initialize  $d = 3$ .

While  $d \leq \sqrt{59}$ :

    Compute  $59 \% d$

    Compute  $59 \% 3 = 2$

    Since  $59 \% 3 \neq 0$ ,

        replace  $d = 3$  by  $d + 2 = 5$ , continue

    Still  $d = 5 \leq \sqrt{59}$ , so continue

    Compute  $59 \% 5 = 4$

    Since  $59 \% 5 \neq 0$ ,

        replace  $d = 5$  by  $d + 2 = 7$ , continue

    Still  $d = 7 \leq \sqrt{59}$ , so continue

    Compute  $59 \% 7 = 3$

    Since  $59 \% 7 \neq 0$ ,

        replace  $d = 7$  by  $d + 2 = 9$ , continue

But  $9 > \sqrt{59}$ , so

    59 is prime

This approach is infeasible for integers  $\sim 10^{30}$  and larger.

To **factor into primes** an integer  $N$

Initialize  $n = N$

While  $2|n$ , add 2 to list of prime factors  
and replace  $n$  by  $n/2$

Initialize  $d = 3$

While  $d \leq \sqrt{n}$ :

While  $d|n$ , add  $d$  to list  
and replace  $n$  by  $n/d$

When  $d$  does not divide  $n$   
replace  $d$  by  $d + 2$

When  $d > \sqrt{n}$

If  $n = 1$  the list of prime factors  
of the original  $N$  is complete

If  $n > 1$  then add  $n$  to the list

The nature of the process assures that the  $d$ s  
obtained are primes.

For example, to factor 153

Initialize  $n = 153$

2 does not divide  $n$ , so

Initialize  $d = 3$

$3 \leq \sqrt{153}$  and  $3|153$ , so

put 3 on the list (now (3))

replace  $n$  by  $n = 153/3 = 51$

$3 \leq \sqrt{51}$  and  $3|51$ , so

put 3 on the list again (now (3, 3))

replace  $n$  by  $n = 51/3 = 17$

Now 3 does not divide  $n = 17$ , so

replace  $d = 3$  by  $d = 3 + 2 = 5$

$5 > \sqrt{17}$  so

17 is prime, add it to the list

which is now (3, 3, 17)

The prime factorization of 153 is

$$153 = 3^2 \cdot 17$$

---

## gcd's and lcm's

The **greatest common divisor**  $\gcd(x, y)$  of two integers  $x, y$  is the largest positive integer  $d$  which divides both  $x, y$ , that is,  $d|x$  and  $d|y$ . For example,

$$\gcd(3, 5) = 1 \quad \gcd(24, 36) = 12$$

$$\gcd(56, 63) = 7 \quad \gcd(105, 70) = 35$$

The **least common multiple**  $\text{lcm}(x, y)$  of two integers is the smallest positive integer  $m$  which is a multiple of both  $x, y$ . For example,

$$\text{lcm}(3, 5) = 15 \quad \text{lcm}(24, 36) = 72$$

$$\text{lcm}(56, 63) = 504 \quad \text{lcm}(105, 49) = 210$$

We can compute **lcm** and **gcd** *if* we have the prime factorizations of  $x$  and  $y$ :

The prime factorization of  $\gcd(x, y)$  has primes that occur in *both* factorizations, with corresponding exponents equal to the *minimum* of the exponents in the two.

The prime factorization of  $\text{lcm}(x, y)$  has primes that occur in *either* factorization, with corresponding exponents equal to the *maximum* of the exponents in the two.

For example, with

$$\begin{aligned}x &= 1001 = 7 \cdot 11 \cdot 13 \\y &= 735 = 3 \cdot 5 \cdot 7^2\end{aligned}$$

$$\begin{aligned}\gcd(1001, 735) &= \\&= 3^{\min(0,1)} 5^{\min(0,1)} 7^{\min(1,2)} 13^{\min(0,1)} \\&= 3^0 5^0 7^1 13^0 = 7\end{aligned}$$

**But you should use this *only* with very very small integers!**

---

## The Euclidean Algorithm

This is a wonderful and efficient 2000-year-old algorithm to compute the *gcd* of two integers  $x, y$  **without factoring**.

To compute  $\gcd(x, y)$  with  $x \geq y$  takes  $\leq 2 \log_2 y$  steps.

To compute  $\gcd(x, y)$ :

Initialize  $X = x, Y = y, R = X \% Y$

while  $R > 0$

    replace  $X$  by  $Y$

    replace  $Y$  by  $R$

    replace  $R$  by  $X \% Y$

When  $R = 0, Y = \gcd(x, y)$

Roughly, this works because

**Theorem:**  $\gcd(x, y)$  is the smallest positive integer expressible as  $rx + sy$  for integers  $r, s$ .

Surely this is a strange picture of *gcd*.

*(The gcd of two integers  $x, y$  (not both 0) is the smallest positive integer expressible as  $rx + sy$  with integers  $r, s$ .)*

*Proof:* Let  $g = rx + sy$  be the smallest such positive value. On one hand, if  $d|x$  and  $d|y$  then there is an integer  $m$  such that  $x = dm$  and an integer  $n$  such that  $y = dn$ . Then

$$rx + sy = r(dm) + s(dn) = d(rm + sn)$$

so  $rx + sy$  is a multiple of  $d$ , which is to say that  $d$  divides it.

On the other hand, by the Division Algorithm  $x = qg + R$  with  $0 \leq R < g$ . And

$$\begin{aligned} R &= x - qg = x - q(rx + sy) \\ &= (1 - qr)x + (-qs)y \end{aligned}$$

which is of that same form. Since  $g$  was smallest positive of this form and  $0 \leq R < g$ , it must be that  $R = 0$ . That is,  $g|x$ . Similarly,  $g|y$ . ///

For example, for  $\gcd(6497, 7387)$

$$\begin{aligned}7387 - 1 \cdot 6497 &= 890 \\6497 - 7 \cdot 890 &= 267 \\890 - 3 \cdot 267 &= 89 \\267 - 3 \cdot 89 &= 0\end{aligned}$$

so  $\gcd(6497, 7387) = 89$ , the last non-zero entry on the right. As another example, for  $\gcd(738701, 649701)$

$$\begin{aligned}738701 - 1 \cdot 649701 &= 89000 \\649701 - 7 \cdot 89000 &= 26701 \\89000 - 3 \cdot 26701 &= 8897 \\26701 - 3 \cdot 8897 &= 10 \\8897 - 889 \cdot 10 &= 7 \\10 - 1 \cdot 7 &= 3 \\7 - 2 \cdot 3 &= 1 \\3 - 3 \cdot 1 &= 0\end{aligned}$$

So the gcd is 1, the last non-zero entry on the right.

Much faster than factoring and comparing.

---

## Multiplicative inverses mod $m$ via Euclid

A **(multiplicative) inverse of  $x$  modulo  $m$**  (both integers) is an *integer*  $y$  (if it exists) such that

$$(x \cdot y) \% m = 1$$

For example, 3 is a multiplicative inverse of 2 modulo 5 because

$$(2 \cdot 3) \% 5 = 6 \% 5 = 1$$

For example, 7 is a multiplicative inverse of 3 modulo 10 because

$$(3 \cdot 7) \% 10 = 21 \% 10 = 1$$

Also  $-3$  is a multiplicative inverse of  $3$  modulo  $10$  because

$$(3 \cdot -3) \% 10 = -9 \% 10 = 1$$

Also  $17$  is a multiplicative inverse of  $3$  modulo  $10$  because

$$(3 \cdot 17) \% 10 = 51 \% 10 = 1$$

Also  $27$  is a multiplicative inverse of  $3$  modulo  $10$  because

$$(3 \cdot 27) \% 10 = 81 \% 10 = 1$$

*How do we find these multiplicative inverses?*

In a moment we will use the Euclidean algorithm, but for now we do this to illustrate **brute force**: to find the multiplicative inverse of 3 modulo 7:

Try 1:	$(3 \cdot 1) \% 7 = 3 \neq 1$	no
Try 2:	$(3 \cdot 2) \% 7 = 6 \neq 1$	no
Try 3:	$(3 \cdot 3) \% 7 = 2 \neq 1$	no
Try 4:	$(3 \cdot 4) \% 7 = 5 \neq 1$	no
Try 5:	$(3 \cdot 5) \% 7 = 1$	yes

That is, just proceeding systematically but unimaginatively we will inevitably find a multiplicative inverse.

If  $\gcd(x, m) = 1$ , then by the strange characterization of the *gcd* there are integers  $r, s$  such that

$$rx + sm = \gcd(x, m) = 1$$

Reduce both sides of the equation modulo  $m$

$$rx \% m = 1$$

(since adding the multiple  $sm$  of  $m$  will not change the reduction mod  $m$ ).

That is,  $r$  is a multiplicative inverse of  $x$  modulo  $m$ .

And, yes, also  $s$  is a multiplicative inverse of  $m$  modulo  $x$ .

The (*extended*) Euclidean Algorithm gives a fast way to determine the integers  $r, s$  above.

With 101 and 87

$$\begin{aligned}101 - 1 \cdot 87 &= 14 \\87 - 6 \cdot 14 &= 3 \\14 - 4 \cdot 3 &= 2 \\3 - 1 \cdot 2 &= 1 \\2 - 2 \cdot 1 &= 0\end{aligned}$$

**Going backward:**

$$\begin{aligned}1 &= (1)3 + (-1)2 \\&= (1)3 + (-1)(14 - 4 \cdot 3) \text{ [sub for 2]} \\&= (-1)14 + (5)3 \quad \text{[simplify]} \\&= (-1)14 + (5)(87 - 6 \cdot 14) \text{ [sub for 3]} \\&= (5)87 + (-31)14 \quad \text{[simplify]} \\&= (5)87 + (-31)(101 - 1 \cdot 87) \text{ [sub 14]} \\&= (-31)101 + (36)87 \quad \text{[simplify]}\end{aligned}$$

Thus,  $-31 \cdot 101 + 36 \cdot 87 = 1$ , and thus  $-31$  is a multiplicative inverse of 101 modulo 87, while 36 is a multiplicative inverse of 87 modulo 101.

If you like, since  $-31 \% 87 = 56$ , also 56 is a multiplicative inverse of 101 modulo 87.

With 131 and 101:

$$\begin{aligned}131 - 1 \cdot 101 &= 30 \\101 - 3 \cdot 30 &= 11 \\30 - 2 \cdot 11 &= 8 \\11 - 1 \cdot 8 &= 3 \\8 - 2 \cdot 3 &= 2 \\3 - 1 \cdot 2 &= 1 \\2 - 2 \cdot 1 &= 0\end{aligned}$$

$$\begin{aligned}1 &= (1)3 + (-1)2 \quad [\text{simplify}] \\&= (1)3 + (-1)(8 - 2 \cdot 3) \quad [\text{subst}] \\&= (-1)8 + (3)3 \quad [\text{simplify}] \\&= (-1)8 + (3)(11 - 1 \cdot 8) \quad [\text{subst}] \\&= (3)11 + (-4)8 \quad [\text{simplify}] \\&= (3)11 + (-4)(30 - 2 \cdot 11) \quad [\text{subst}] \\&= (-4)30 + (11)11 \quad [\text{simplify}] \\&= (-4)30 + (11)(101 - 3 \cdot 30) \quad [\text{subst}] \\&= (11)101 + (-37)30 \quad [\text{simplify}] \\&= (11)101 + (-37)(131 - 1 \cdot 101) \quad [\text{subst}] \\&= (-37)131 + (48)101\end{aligned}$$

So  $-37 \cdot 131 + 48 \cdot 101 = 1$ .

---

## Why Euclid works

A step in Euclid's algorithm is of the form

$$x - q \cdot y = r$$

If  $d|x$  and  $d|y$  then  $d|r$ , from above. But also, by rearranging,

$$r + qy = x$$

so if  $d|r$  and  $d|y$  then  $d|x$ . Thus

$$\gcd(x, y) = \gcd(y, r)$$

This persists through the algorithm. The last two lines are of the form

$$x' - q' \cdot y' = r'$$

$$y' - q'' \cdot r' = 0$$

We know that the gcd of the original two numbers is equal

$$\gcd(x', y') = \gcd(y', r') = \gcd(r', 0)$$

so the last non-zero right-hand value is the gcd of the two original numbers. ///

---

## Proof that division works

Given positive integer  $m$  and integer  $x$ , there are unique integers  $q$  and  $r$  such that  $0 \leq r < m$  and

$$x = qm + r$$

*Proof:* Let  $t = x - \ell m$  be the smallest non-negative integer of the form  $x - qm$  with integer  $q$ . If  $t < m$  we're done. If  $t \geq m$ , then  $t - m \geq 0$ , and  $x - (\ell + 1)m$  is a non-negative integer smaller than  $x - \ell m$ , contradiction. Thus, it could not have been that  $t \geq m$ . ///

Underlying this all is the **Well-ordering Principle**, that every non-empty set of non-negative integers has a smallest element. This is a defining *axiom* for the integers.

---

## The crucial property of primes

To *prove* Unique Factorization of integers into primes, the crucial property which must be proved *beforehand* is

*For prime  $p$  if  $p|ab$  then either  $p|a$  or  $p|b$ .*

*Proof:* Let  $ab = mp$  for integer  $m$ . If  $p|a$ , we're done, so suppose not. Then  $\gcd(p, a) < p$ , and is a positive divisor of  $p$ , so  $\gcd(p, a) = 1$  since  $p$  is prime. From above, there are  $r, s$  such that

$$rp + sa = 1$$

Using this and  $ab = mp$

$$\begin{aligned} b &= b \cdot 1 = b \cdot (rp + sa) \\ &= brp + bsa = brp + smp = p(br + sm) \end{aligned}$$

That is,  $b$  is a multiple of  $p$ . ///

This proof is probably not intuitive... but is the right thing!

A more functional characterization of  $gcd$ .

**Theorem:**  $gcd(x, y)$  has the property that it is the *unique* positive integer which divides  $x$  and  $y$  and such that if  $d$  divides both  $x$  and  $y$  then  $d$  divides  $gcd(x, y)$ .

*Proof:* If  $d$  divides  $x$  and  $y$ , then  $d$  divides  $rx + sy$  for *any*  $r, s$ . Since (from above)  $gcd(x, y)$  is of this form,  $d$  divides  $gcd(x, y)$ . To prove uniqueness, if  $g$  and  $h$  were two positive integers with that property, then  $g|h$  and  $h|g$ . That is, for some positive integers  $a, b$   $g = ah$  and  $h = bg$ . Then  $g = ah = a(bg)$ , so  $(1 - ab)g = 0$ . Thus,  $ab = 1$ , which for positive integers implies  $a = b = 1$ . So  $g = h$ . ///

An analogous characterization of  $lcm$ .

**Theorem:**  $lcm(x, y)$  is the *unique* positive integer divisible by  $x$  and  $y$  such that if  $m$  is divisible by both  $x$  and  $y$  then  $lcm(x, y) | m$ .

*Proof:* Let  $L = lcm(x, y)$ . Let  $m$  be a multiple of  $x$  and  $y$ . From above, let  $r, s$  be such that

$$\gcd(L, m) = r \cdot L + s \cdot m$$

Let  $L = Ax$  and  $m = Bx$  for integers  $A, B$ .  
Then

$$\gcd(L, m) = r(Ax) + s(Bx) = (rA + sB) \cdot x$$

shows that the  $gcd$  is a multiple of  $x$ . Likewise it is a multiple of  $y$ . As  $L$  is the *smallest* positive integer with this property,  $L \leq \gcd(L, m)$ . But the  $gcd$  divides  $L$ , so  $L = \gcd(L, m)$ . That is,  $L | m$ . And any other positive integer  $L'$  with this property must satisfy  $L' | L$  and  $L | L'$ , so  $L = L'$ .

///

---

## lcm versus gcd

For two integers  $x, y$

$$\text{lcm}(x, y) = \frac{x \cdot y}{\text{gcd}(x, y)}$$

*Proof:* Certainly

$$\frac{x \cdot y}{\text{gcd}(x, y)} = x \cdot \frac{y}{\text{gcd}(x, y)}$$

and  $y/\text{gcd}(x, y)$  is an integer, so that expression is a multiple of  $x$  (and, symmetrically, of  $y$ ).

On the other hand, suppose  $N$  is divisible by both  $x$  and  $y$ . Let  $N = ax$  and  $N = by$ . From above, let  $r, s$  be integers such that

$$\text{gcd}(x, y) = rx + sy$$

Dividing through by  $\text{gcd}(x, y)$  gives

$$1 = r \frac{x}{\text{gcd}(x, y)} + s \frac{y}{\text{gcd}(x, y)}$$

Then

$$\begin{aligned} N &= N \cdot 1 = N \cdot \left( r \frac{x}{\gcd(x, y)} + s \frac{y}{\gcd(x, y)} \right) \\ &= \frac{Nrx}{\gcd(x, y)} + \frac{Nsy}{\gcd(x, y)} \\ &= \frac{(by)rx}{\gcd(x, y)} + \frac{(ax)sy}{\gcd(x, y)} \\ &= (br + as) \cdot \frac{xy}{\gcd(x, y)} \end{aligned}$$

Thus,  $N$  is a multiple of  $xy/\gcd(x, y)$ .

///