

Integers and Division

Though you probably learned about integers and division back in fourth grade, we need formal definitions and theorems to describe the algorithms we use and to verify that they are correct, in general.

1 Divides

If a and b are integers and $a \neq 0$, we say that a *divides* b (or that a is a *factor* of b) if there is an integer c such that $b = ac$.

$a \mid b$ means a divides b .

$a \nmid b$ means a does not divide b .

Theorem 1 *Let a , b , and c be integers, then*

1. *if $a \mid b$ and $a \mid c$ then $a \mid (b + c)$*
2. *if $a \mid b$ then $a \mid bc$ for all integers, c*
3. *if $a \mid b$ and $b \mid c$ then $a \mid c$.*

Proof: Here is a proof of (1); try to prove the others yourself.

Assume that a , b , and c be integers and that $a \mid b$ and $a \mid c$. From the definition of *divides*, there must be integers m and n such that:

$$b = ma \tag{1}$$

$$c = na \tag{2}$$

Adding the left- and right-hand sides of Equations 1 and 2, we obtain

$$b + c = ma + na.$$

By the distributive law and commutativity,

$$b + c = (m + n)a.$$

By the closure of addition, $m + n$ is an integer so, by the definition of *divides*,

$$a \mid (b + c). \quad \square$$

Corollary 1 *If a , b , and c are integers such that $a \mid b$ and $a \mid c$ then $a \mid (mb + nc)$ for all integers m and n .*

2 Primes

A positive integer $p > 1$ is called *prime* if the only positive factors of p are 1 and p . Extremely large prime numbers are used in RSA and other algorithms for public key cryptography. Primes are also used for hash tables and pseudorandom number generators.

2.1 Finding Primes

How can you find prime numbers? The mathematician, Eratosthenes (276-194 BC) invented a prime number sieve, the Sieve of Eratosthenes, which, in modified form, is still used in number theory research. Here is how the sieve works if you want to find all the prime numbers less than or equal to N .

1. Make a list-to-check of the numbers from 2 to N .
2. Make a list-of-primes that starts out empty.
3. Repeat the following until the first number in the list-to-check is $> \sqrt{N}$
 - (a) Put the first number in the list-to-check in the list-of-primes.
 - (b) Remove all multiples of that number from the list-to-check.
4. Put all the numbers still in list-to-check into list-of-primes.

Example

To find all the primes up to $N = 25$, we start with:

list-to-check = 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25

list-of-primes =

Then we put 2 in the list-of-primes and remove all multiples of 2 from the list-to-check. We now have:

list-to-check = 3 5 7 9 11 13 15 17 19 21 23 25

list-of-primes = 2

Now put 3 in the list-of-primes and remove all multiples of 3 from the list-to-check. We now have:

list-to-check = 5 7 11 13 17 19 23 25

list-of-primes = 2 3

Now put 5 in the list-of-primes and remove all multiples of 5 from the list-to-check. We now have:

list-to-check = 7 11 13 17 19 23

list-of-primes = 2 3 5

Since $\sqrt{25} = 5$, we put all the numbers remaining in the list-to-check into the list-of-primes.

list-of-primes (less than or equal to 25) = 2 3 5 7 11 13 17 19 23.

A positive integer $n > 1$ that is not prime is called a *composite*.

Theorem 2 (Fundamental Theorem of Arithmetic) *Every positive integer greater than 1 can be written uniquely as a prime or as the product of two or more primes where the prime factors are written in order of non-decreasing size.*

Example

$$364 = 2 \cdot 2 \cdot 7 \cdot 13 = 2^2 \cdot 7 \cdot 13$$

$$7581 = 7 \cdot 19 \cdot 57$$

$$32768 = 2^{15}$$

$$31752 = 2^3 \cdot 3^4 \cdot 7^2$$

Theorem 3 *There are infinitely many primes.*

Can you prove this?

Want to listen to some primes? Try the Prime Number Listening Guide.

3 Division

Back in elementary school, you probably wrote out division problems like this:

$$7 \overline{) 29} \quad r = 4$$

In this equation, 29 is the *dividend*, 7 is the *divisor*, 4 is the *quotient*, and 1 is the *remainder*. The following theorem tells us that we can always find a quotient and remainder in a division problem.

Theorem 4 (The Division “Algorithm”) *Let a be an integer and b a positive integer. Then there are unique integers q and r , with $0 \leq r < b$, such that $a = b \cdot q + r$.*

3.1 Scheme Functions Related to Division

These definitions and examples are taken from *The Scheme Programming Language, Second Edition* by R. Kent Dybvig.

procedure: (quotient int1 int2)
returns: the integer quotient of int1 and int2
(quotient 45 6) \Rightarrow 7
(quotient 6.0 2.0) \Rightarrow 3.0
(quotient 3.0 -2) \Rightarrow -1.0

The function remainder is similar to but not quite the same as modulo.

procedure: (remainder int1 int2)
returns: the integer remainder of int1 and int2

procedure: (modulo int1 int2)
returns: the integer modulus of int1 and int2

The result of remainder has the same sign as int1.

(remainder 16 4) \Rightarrow 0
(remainder 5 2) \Rightarrow 1
(remainder -45.0 7) \Rightarrow -3.0
(remainder 10.0 -3.0) \Rightarrow 1.0
(remainder -17 -9) \Rightarrow -8

The result of modulo has the same sign as int2.

(modulo 16 4) \Rightarrow 0
(modulo 5 2) \Rightarrow 0
(modulo -45.0 7) \Rightarrow 4.0
(modulo 10.0 -3.0) \Rightarrow -2.0
(modulo -17 -9) \Rightarrow -8

In some computing languages, the functions *quotient* and *modulo* are called *div* and *mod*. Mathematicians write “ $a \bmod b$ ” instead of “(modulo a b).” For more about modular arithmetic refer to our handout *Cryptography and Modular Arithmetic*.

4 Greatest Common Divisor and Least Common Multiple

If a and b be integers, not both 0, the *greatest common divisor* of a and b , $\text{gcd}(a, b)$ is the largest integer d such that $d \mid a$ and $d \mid b$. The *least common multiple* of a and b , $\text{lcm}(a, b)$ is the smallest integer divisible by both a and b .

Examples

$\text{gcd}(75, 21) = 3$
 $\text{gcd}(52, 81) = 1$
 $\text{gcd}(2^2 \cdot 7 \cdot 13, 2^3 \cdot 3^4 \cdot 7^2) = 2^2 \cdot 3^0 \cdot 7 \cdot 13^0$ What is the rule?
 $\text{gcd}(49831, 825579) = ?$ We will soon learn a way to solve this efficiently.
 $\text{lcm}(75, 21) = 75 \cdot 7 = 25 \cdot 21 = 525$

$$\begin{aligned} \text{lcm}(52, 81) &= 52 \cdot 81 = 4212 \\ \text{lcm}(2^2 \cdot 7 \cdot 13, 2^3 \cdot 3^4 \cdot 7^2) &= 2^3 \cdot 3^4 \cdot 7^2 \cdot 13 \quad \text{What is the rule?} \end{aligned}$$

Two integers m and n are said to be *relatively prime* or *coprime* if $\text{gcd}(m, n) = 1$. The integers 52 and 81 are relatively prime.

4.1 Applications of gcd and lcm

The most common applications of the gcd and lcm is in working with fractions. You put them to use whenever you reduce or add fractions and you would use them in the same way if you were implementing a class to represent fractions.

To reduce a fraction to *lowest terms*, we divide the numerator and denominator by their gcd.

$$\frac{84}{36} = \frac{12 \cdot 7}{12 \cdot 3} = \frac{7}{3} \qquad \text{gcd}(84, 36) = 12$$

We use the lcm when we add fractions.

$$\begin{aligned} \frac{3}{5} + \frac{2}{7} &= \frac{21+10}{35} = \frac{31}{35} & \text{lcm}(5, 7) &= 35 \\ \frac{2}{15} + \frac{10}{21} &= \frac{14+50}{105} = \frac{64}{105} & \text{lcm}(15, 21) &= 105 \end{aligned}$$

In both these sums of fractions we see that the denominator of the result is given by the lcm of the denominators in the summands but where did the numbers 14 and 50 come from?

$$14 = 2 \cdot \frac{21}{\text{gcd}(15, 21)} \qquad \text{and} \qquad 50 = 10 \cdot \frac{15}{\text{gcd}(15, 21)}$$

In general, if a , b , c , and d are positive integers then

$$\frac{a}{b} + \frac{c}{d} = \frac{a \cdot d + c \cdot b}{b \cdot d} = \frac{(a \cdot d) / \text{gcd}(b, d) + (c \cdot b) / \text{gcd}(b, d)}{(b \cdot d) / \text{gcd}(b, d)} = \frac{a \cdot (d / \text{gcd}(b, d)) + c \cdot (b / \text{gcd}(b, d))}{\text{lcm}(b, d)}$$

Will the resulting fractions always be reduced? The last equality comes from the following theorem.

Theorem 5 *Let a and b be positive integers. Then $ab = \text{gcd}(a, b) \cdot \text{lcm}(a, b)$.*

We also use the gcd in cryptography. For example, to decrypt a linear cipher

$$a \rightarrow (m \cdot a + b) \bmod n$$

we need a multiplicative inverse for $m \bmod n$. In fact, a multiplicative inverse for $m \bmod n$ exists if and only if $\text{gcd}(m, n) = 1$. If we are working with a large number of letters or blocks, n , we need an efficient way calculate $\text{gcd}(m, n)$ in order to check whether we are using a good multiplier, m .

5 Euclidean Algorithm

How do you find $\gcd(49831, 825579)$ or $\gcd(8094702578291, 7403070229547)$ or the gcd of two hundred-digit numbers? You could factor both numbers but that is a costly operation and will not be feasible if the numbers are too large. The **Euclidean Algorithm** is a method to compute the gcd of two non-zero integers, a and b . The method is based on the Division Algorithm.

Theorem 6 (Euclidean Algorithm) *If r is the remainder when a is divided by b , i.e. $a = q \cdot b + r$, with $0 \leq r < b$, then, $\gcd(a, b) = \gcd(b, r)$.*

Proof: This follows from the Division Algorithm and the definition of *divides*. We know that

$$\gcd(a, b) \mid a \quad \text{and} \quad \gcd(a, b) \mid b$$

so

$$\gcd(a, b) \mid (a - q \cdot b) \quad \text{i.e.} \quad \gcd(a, b) \mid r.$$

Since $\gcd(a, b)$ divides both b and r , $\gcd(a, b) \mid \gcd(b, r)$. A similar argument leads to $\gcd(b, r) \mid \gcd(a, b)$. Hence $\gcd(b, r) = \gcd(a, b)$ \square

5.1 Using the Euclidean Algorithm

Here is a Scheme implementation of the Euclidean Algorithm from Wikipedia, the free encyclopedia.

```
(define (gcd a b)
  (if (= b 0)
      a
      (gcd b (modulo a b))))
```

Examples

$$\gcd(42, 35) = \gcd(35, 7) = \gcd(7, 0) = 7.$$

$$\gcd(612, 1275) = \gcd(1275, 612) = \gcd(612, 51) = \gcd(51, 0) = 51.$$

$$\gcd(49831, 825579)$$

$$= \gcd(825579, 49831) = \gcd(49831, 28283) = \gcd(28283, 21548)$$

$$= \gcd(21548, 6735) = \gcd(6735, 1343) = \gcd(1343, 20)$$

$$= \gcd(20, 3) = \gcd(3, 2) = \gcd(2, 1) = \gcd(1, 0) = 1$$

Notice that it took only 10 applications of mod to compute $\gcd(49831, 825579)$.

5.2 Euclidean Algorithm Links

For further discussion of the Euclidean algorithm, see the Prime Pages glossary.

The Visible Euclidean Algorithm is a tool that computes the gcd of two numbers and shows the steps using repeated applications of the Division Algorithm, i.e., following the proof. (Remember that you are supposed to understand the Euclidean Algorithm and will have to perform it by hand on exams.)

6 Extended Euclidean Algorithm

One of the uses of the Euclidean Algorithm is to find integer solutions to equations of the form $ax + by = c$. Given integers a , b , and c , this is solvable (for x and y integers) whenever the $\gcd(a, b)$ divides c . If you keep track of the quotients in the Euclidean Algorithm while finding $\gcd(a, b)$, you can reverse the steps to find x and y . This method is called the **Extended Euclidean Algorithm**. It is especially useful when a and b are relatively prime. Then we can solve $ax + by = 1$ and x will be the multiplicative inverse of $a \bmod b$ and y will be a multiplicative inverse of $b \bmod a$. It will be easier to understand how this works by looking at some examples.

Examples

If we use the Division Algorithm repeatedly to compute $\gcd(6735, 1343)$, the steps look like this.

1. $6735 - 5 \cdot 1343 = 20$
2. $1343 - 67 \cdot 20 = 3$
3. $20 - 6 \cdot 3 = 2$
4. $3 - 1 \cdot 2 = 1$
5. $2 - 2 \cdot 1 = 0$

So $\gcd(6735, 1343) = 1$.

We want to find integers x and y such that $x \cdot 6735 + y \cdot 1343 = 1$. We start with line 4 of the calculation above and work backwards:

$$3 - 1 \cdot 2 = 1$$

Use line 3 above to substitute for 2 in this expression then rearrange the result so it looks like $u \cdot 20 + v \cdot 3 = 1$ where u and v are integers.

$$3 - 1 \cdot (20 - 6 \cdot 3) = 1$$

$$-1 \cdot 20 + 7 \cdot 3 = 1$$

Now use line 2 above to substitute for 3 in this expression then rearrange the result so it looks like $u \cdot 1343 + v \cdot 20 = 1$ where u and v are integers.

$$-1 \cdot 20 + 7 \cdot (1343 - 67 \cdot 20) = 1$$

$$7 \cdot 1343 - (1 + 67 \cdot 7) \cdot 20 = 1$$

$$7 \cdot 1343 - 470 \cdot 20 = 1$$

Finally, use line 1 above to substitute for 20 in this expression then rearrange the result so it looks like $u \cdot 6735 + v \cdot 1343 = 1$ where u and v are integers.

$$7 \cdot 1343 - 470 \cdot (6735 - 5 \cdot 1343) = 1$$

$$-470 \cdot 6735 + 2357 \cdot 1343 = 1$$

We have found a solution for $x \cdot 6735 + y \cdot 1343 = 1$, $x = -470$ and $y = 2357$.

You must be very careful not to just add everything up. It is important to keep the successive remainders intact when you substitute and rearrange. You can see additional examples at

http://en.wikipedia.org/wiki/Extended_Euclidean_algorithm

Our calculations have also led to a multiplicative inverse for $6735 \bmod 1343$: $-470 \cdot 6735 \bmod 1343 = 1$. If you want a positive inverse, just use $1343 - 470 = 873$.