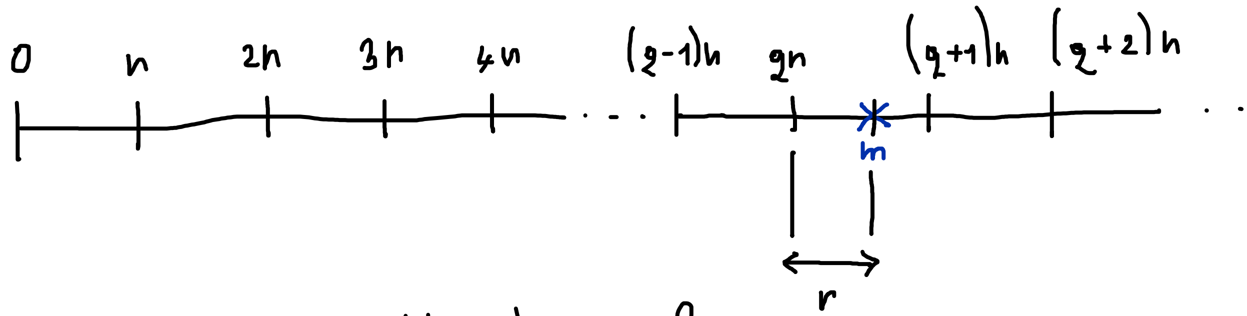
Division in the integers

If m and n are nonnegative integers and n is not zero, we can plot the nonnegative integer multiple of n on a half-line and locate m as in figure:



If m is a multiple of n, say $m = qn$, then we can write $m = qn + r$, where $r = 0$. On the other hand, if m is not a multiple of n, we let qn be the first multiple of n lying to the left of m, and let r be $m - qn$. Then r is the distance between qn and m, so clearly $0 < r < n$, and again we have $m = qn + r$.

Theorem 1. *If $n \neq 0$ and m are nonnegative integers, we can write $m = qn + r$ for some nonnegative integers q and r with $0 \leq r < n$. Moreover, there is just one way to do this.* ◆

Example.

(a) If $m = 16$, and $n = 3 \Rightarrow m = 3 \cdot 5 + 1$

(b) If $m = 3$, and $n = 10 \Rightarrow m = 0 \cdot 10 + 3$

Divisibility

If the r in "Theorem 1" is zero, so that m is a multiple of n, we write $n \mid m$, which is read "n divides m". If m is not a multiple of n ($r \neq 0$), we write $n \nmid m$, which is read "n does not devide m"

Properties of divisibility

Theorem 2.

Let a, b and c be integers.

(a) $a \mid b \wedge a \mid c \Rightarrow a \mid (b+c)$

(b) $a \mid b \wedge a \mid c \wedge b > c \Rightarrow a \mid (b-c)$

(c) $a \mid b \vee a \mid c \Rightarrow a \mid (b \cdot c)$

(d) $a \mid b \wedge b \mid c \Rightarrow a \mid c$

Prime number

A number $p > 1$ in $\mathbb{Z}^+$ is called prime if the only positive integers that divide p are p and 1.

Example: 2, 3, 5, 7, 11, 13 are primes, while 1, 4, 6, 8, 9, 10, 12, 14, 15, 16 are not.

It is easy to write a set of steps, or an **algorithm**[1], to determine if a positive integer $n > 1$ is a prime number. First we check to see if n is 2. If $n > 2$, we could divide n by every integer from 2 to $n - 1$, and if none of these is a divisor of n, then n is prime. To make the process more efficient, we note that if $mk = n$, then either m or k is less than or equal to $\sqrt{n}$. This means that if n is not prime, it has a divisor k satisfying the inequality $1 < k \leq \sqrt{n}$, so we need only test for divisors in this range. Also, if n has any even number as a divisor, it must have 2 as a divisor. Thus, after checking for divisibility by 2, we may skip all even integers.

Theorem 3. *Every positive integer $n > 1$ can be written uniquely as $p_1^{k_1} p_2^{k_2} \cdots p_s^{k_s}$, where $p_1 < p_2 < \cdots < p_s$ are distinct primes that divide n and the k's are positive integers giving the number of times each prime occurs as a factor of n.* ◆

Example

$9 = 3 \cdot 3 = 3^2$

$24 = 2 \cdot 2 \cdot 2 \cdot 3 = 2^3 \cdot 3$

$30 = 2 \cdot 3 \cdot 5$

Greatest common divisor

If a, b & $K \in Z^{+} \wedge K|a \wedge K|b$, we say that K is a common divisor of a and b. If d is the largest such K, is called the greatest common divisor, or GCD, of a and b, and we write $d = GCD(a,b)$. The GCD is a multiple of each other common divisors. Also, can be writen as a combination of a & b

Theorem 4. *If d is GCD(a, b), then*

(a) $d = sa + tb$ *for some integers s and t (these are not both positive).*

(b) *If c is any other common divisor of a and b, then $c \mid d$.*

Proof: Let x be the smallest positive integer that can be written as $sa + tb$ for some integers s and t, and let c be a common divisor of a and b. Since $c \mid a$ and $c \mid b$, we know from Theorem 2 that $c \mid x$, so $c \leq x$. If we can show that x is a common divisor of a and b, it will then be the greatest common divisor of a and b, and both parts of the theorem will have been proved. By Theorem 1, $a = qx + r$ with $0 \leq r < x$. Solving for r, we have $r = a - qx = a - q(sa + tb) = a - qsa - qtb = (1 - qs)a + (-qt)b$. If r is not zero, then since $r < x$ and r is a multiple of a and a multiple of b, we will have a contradiction to the fact that x is the smallest positive number that is a sum of multiples of a and b. Thus r must be 0 and $x \mid a$. In the same way we can show that $x \mid b$, and this completes the proof. ◆

Example 4.

(a) Common divisors of 12 & 30 are. 2, 3, 6

$12 = 2 \cdot 2 \cdot 3$

$30 = 2 \quad 3 \cdot 5$

$\Rightarrow GCD(12, 30) = 6$ & $6 = 3 \cdot 12 - 1 \cdot 30$

(b) $17 = 17$

$95 = 5 \cdot 19$

common divisors 1

$\Rightarrow GCD(17, 95) = 1$ & $1 = 28 \cdot 17 - 5 \cdot 95$

$= 476 - 475$

If GCD$(a, b) = 1$, as in Example 4(b), we say that a and b are **relatively prime**.

Euclidean algorithm

To find $GCD(a,b)$ Suppose $a > b > 0$, (otherwise $a \leftrightarrow b$). Then, by theorem 1:

$a = k_1 b + r_1$, $k_1, r_1 \in \mathbb{Z}^+ \wedge 0 \leq r_1 < b$

Now, theorem 2: $n | a \wedge n | b \Rightarrow n | r_1$, $r_1 = a - k_1 b$

If $n | b \wedge n | r_1 \Rightarrow n | a$

$\Rightarrow$ common divisors of a & b are the same for b & r_1 $\Rightarrow GCD(a,b) = GCD(b, r_1)$

We now continue using Theorem 1 as follows:

divide b by r_1:	$b = k_2 r_1 + r_2$	$0 \leq r_2 < r_1$
divide r_1 by r_2:	$r_1 = k_3 r_2 + r_3$	$0 \leq r_3 < r_2$
divide r_2 by r_3:	$r_2 = k_4 r_3 + r_4$	$0 \leq r_4 < r_3$
$\vdots$	$\vdots$	$\vdots$
divide r_{n-2} by r_{n-1}:	$r_{n-2} = k_n r_{n-1} + r_n$	$0 \leq r_n < r_{n-1}$
divide r_{n-1} by r_n:	$r_{n-1} = k_{n+1} r_n + r_{n+1}$	$0 \leq r_{n+1} < r_n$.

Since $a > b > r_1 > r_2 > r_3 > r_4 > \cdots$, the remainder will eventually become zero, so at some point we have $r_{n+1} = 0$.

We now show that $r_n = \mathrm{GCD}(a, b)$. We saw previously that

$$\mathrm{GCD}(a, b) = \mathrm{GCD}(b, r_1).$$

Repeating this argument with b and r_1, we see that

$$\mathrm{GCD}(b, r_1) = \mathrm{GCD}(r_1, r_2).$$

Upon continuing, we have

$$\mathrm{GCD}(a, b) = \mathrm{GCD}(b, r_1) = \mathrm{GCD}(r_1, r_2) = \cdots = \mathrm{GCD}(r_{n-1}, r_n)$$

Since $r_{n-1} = k_{n+1} r_n$, we see that $\mathrm{GCD}(r_{n-1}, r_n) = r_n$. Hence $r_n = \mathrm{GCD}(a, b)$.

Example 5. $a = 34$, $b = 190$,

$a < b$, interchange $a = 190$, $b = 34$

$$190 = 5 \cdot 34 + 20$$
$$34 = 20 + 14$$
$$20 = 14 + 6$$
$$14 = 2 \cdot 6 + 2$$
$$6 = 3 \cdot 2 + 0.$$
$$\Rightarrow \mathrm{GCD}(190, 34) = 2$$

$$= 14 - 2\,6 = 14 - 2(20 - 14)$$
$$= 3 \cdot 14 - 2\,20$$
$$= 3\,(34 - 20) - 2 \cdot 20$$
$$= 3 \cdot 34 - 5(190 - 5 \cdot 34)$$
$$= 28 \cdot 34 - 5 \cdot 190.$$

In Theorem 4(a), we observed that if $d = \text{GCD}(a, b)$, we can find integers s and t such that $d = sa + tb$. The integers s and t can be found as follows. Solve the next-to-last equation in (2) for r_n:

$$r_n = r_{n-2} - k_n r_{n-1}. \tag{3}$$

Now solve the second-to-last equation in (2), $r_{n-3} = k_{n-1}r_{n-2} + r_{n-1}$, for r_{n-1}:

$$r_{n-1} = r_{n-3} - k_{n-1}r_{n-2}.$$

Substitute this expression in (3):

$$r_n = r_{n-2} - k_n[r_{n-3} - k_{n-1}r_{n-2}].$$

Continue to work up through the equations in (2) and (1), replacing r_i by an expression involving r_{i-1} and r_{i-2} and finally arriving at an expression involving only a and b.

Example 6: $a = 108$, $b = 60$

$108 = 60 + 48$

$60 = 48 + 12$

$48 = 4 \cdot 12 + 0$ $\quad$ $\text{GCD}(108, 60) = 12$

$12 = 60 - 48 = 60 - (108 - 60) = 2 \cdot 60 - 108$

Theorem 5. *If a and b are in Z^+, then* $\mathrm{GCD}(a, b) = \mathrm{GCD}(b, b \pm a)$.

Proof: If c divides a and b, it divides $b \pm a$, by Theorem 2. Since $a = b - (b - a) = -b + (b + a)$, we see, also by Theorem 2, that a common divisor of b and $b \pm a$ also divides a and b. Since a and b have the same common divisors as b and $b \pm a$, they must have the same greatest common divisor. ◆

Example: $a = 72$, $b = 48$

$72 = 48 + 24$

$48 = 2 \cdot 24 + 0$

$\mathrm{GCD}(72, 48) = 24$

$a = 120$, $b = 48$

$120 = 2 \cdot 48 + 24$

$48 = 2 \cdot 24 + 0$

Least common multiple

If a, b, and k are in Z^+, and $a \mid k$, $b \mid k$, we say k is a **common multiple** of a and b. The smallest such k, call it c, is called the **least common multiple** or LCM, of a and b, and we write $c = \mathrm{LCM}(a, b)$. The following result shows that we can obtain the least common multiple from the greatest common divisor, so we do not need a separate procedure for finding the least common multiple.

Theorem 6. *If a and b are two positive integers, then* $\mathrm{GCD}(a,b) \cdot \mathrm{LCM}(a,b) = ab$.

Proof: Let $p_1, p_2, \ldots, p_k$ be all the prime factors of either a or b. Then we can write

$$a = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k} \quad \text{and} \quad b = p_1^{b_1} p_2^{b_2} \cdots p_k^{b_k}$$

where some of the a_i and b_i may be zero. It then follows that

$$\mathrm{GCD}(a, b) = p_1{}^{\min(a_1, b_1)} p_2{}^{\min(a_2, b_2)} \cdots p_k{}^{\min(a_k, b_k)}$$

and

$$\mathrm{LCM}(a, b) = p_1{}^{\max(a_1, b_1)} p_2{}^{\max(a_2, b_2)} \cdots p_k{}^{\max(a_k, b_k)}.$$

Hence

$$\begin{aligned} \mathrm{GCD}(a, b) \cdot \mathrm{LCM}(a, b) &= p_1^{a_1 + b_1} p_2{}^{a_2 + b_2} \cdots p_k^{a_k + b_k} \\ &= (p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}) \cdot (p_1^{b_1} p_2^{b_2} \cdots p_k^{b_k}) \\ &= ab. \end{aligned}$$

◆

Example 7.

$a = 540$

$b = 504$

$a = 2 \cdot 2 \cdot 5 \cdot 3 \cdot 3 \cdot 3 = 2^2 \cdot 3^3 \; 5$

$b = 2 \cdot 2 \cdot 2 \cdot 7 \; 3 \; 3 = 2^3 \cdot 3^2 \; 7$

$p_1 = 2 ; p_2 = 3 ; p_3 = 5 , p_4 = 7$

$$\Rightarrow \begin{cases} a = 2^2 \cdot 3^3 \; 5^1 \cdot 7^0 \\ b = 2^3 \cdot 3^2 \cdot 5^0 \cdot 7^1 \end{cases}$$

$GCD(540, 504) = 2^2 \; 3^2 \cdot 5^0 \cdot 7^0$

$= 4 \cdot 9 = 36$

$LCM(540, 504) = 2^3 \; 3^3 \cdot 5^1 \; 7^1 =$

$= 8 \; 27 \cdot 5 \cdot 7 =$

$= 280 \cdot 27 = 7560$

$36 \cdot 7560 = 272{,}160$ ✓

$540 \cdot 504 = 272{,}160$ ✓

$$\begin{array}{r} 40 \\ \times \; 7 \\ \hline 280 \\ \times \; 27 \\ \hline 1960 \\ 560 \; \\ \hline 7560 \\ \times \; 36 \\ \hline 45360 \\ 22680 \; \\ \hline 272160 \end{array}$$

$$\begin{array}{r} 540 \\ 504 \\ \hline 2160 \\ 000 \; \\ 2700 \; \; \\ \hline 272160 \end{array}$$

Modulus

If $a \neq 0$ and b are nonnegative integers, Theorem 1 tells us that we can write $b = qa + r$, $0 \leq r < a$. Sometimes the remainder r is more important than the quotient q. Note that $0 \leq r < a$.

Example 8. If the time is now 4 o'clock, what time will it be 101 hours from now?

Solution: Let $a = 12$ and $b = 4 + 101$, or 105. Then we have $105 = 8 \cdot 12 + 9$. The remainder 9 answers the question. In 101 hours it will be 9 o'clock. ◆

In this case we call a the **modulus** and write $b \equiv r \pmod{a}$, read "b is **congruent** to r mod a."

Example 9.

(a) $29 \equiv 4 \pmod{5}$

(b) $172 \equiv 7 \pmod{11}$

(c) $3 \equiv 3 \pmod{6}$

Note that if $b \equiv r \pmod{a}$, then $0 \leq r < a$, and $b - r$ is a multiple of a; that is, a divides $b - r$, but also $b + (a - r)$.

Mod-n function

For each $n \in Z^+$, we define a function f_n, the mod-n function, as follows: If z is a nonnegative integer, then $f_n(z) = r$, where $z \equiv r \pmod{n}$ and $0 \leq r < n$.

Example 10.

$f_3(14) = 2$

$f_7(153) = 6$

Pseudocode 4 GCD

FUNCTION GCD(X, Y)

1. **WHILE** ($X \neq Y$)
    a. **IF** ($X > Y$) **THEN**
        1. $X \leftarrow X - Y$
    b. **ELSE**
        1. $Y \leftarrow Y - X$
1. **RETURN** (X)

END OF FUNCTION GCD