MATH 324 Summer 2006
Elementary Number Theory

Notes on Divisibility and Greatest Common Divisor

Department of Mathematical and Statistical Sciences
University of Alberta

Divisibility

In this note we introduce the notion of "divisibility" for two integers a and b then we discuss the division algorithm. First we give a formal definition and note some properties of the division operation.

Definition. If $a, b \in \mathbb{Z}$, then we say that b **divides** a and we write $b \,|\, a$, if and only if $b \neq 0$ and there exists an integer q such that $a = q \cdot b$. In this case, we also say that b is a **divisor** of a, or that a is a **multiple** of b. If b does not divide a, then we write $b \nmid a$.

We have the following properties for the division operation.

Theorem. If $a, b, c \in \mathbb{Z}$, then

(a) $1 \,|\, a$ and $a \,|\, 0$

(b) if $a \,|\, b$ and $b \,|\, a$ then $a = \pm b$

(c) if $a \,|\, b$ and $b \,|\, c$ then $a \,|\, c$

(d) if $a \,|\, b$ then $a \,|\, b \cdot x$ for all $x \in \mathbb{Z}$

(e) if $x = y + z$ and a divides any two of the integers x, y, or z, then a divides the remaining integer

(f) if $a \,|\, b$ and $a \,|\, c$ then $a \,|\, bx + cy$ for all $x, y \in \mathbb{Z}$.

Proof. We will prove part (b), and leave the rest as an exercise.

Suppose that $a \,|\, b$ and $b \,|\, a$, from the definition of the division operation it follows that $a \neq 0$ and $b \neq 0$, and that there exist integers k and ℓ such that

$$a = k \cdot b \qquad \text{and} \qquad b = \ell \cdot a,$$

so that

$$a = k \cdot b = k \cdot \ell \cdot a,$$

and from the cancellation law, since $a \neq 0$, we have $k \cdot \ell = 1$. Since k and ℓ are nonzero integers, then $|k| \geq 1$ and $|\ell| \geq 1$, so we must have either $k = \ell = 1$ or $k = \ell = -1$, that is, either $a = b$ or $a = -b$.

□

Theorem. **(Division Algorithm)** If $a, b \in \mathbb{Z}$ with $b > 0$, then there exist unique integers $q, r \in \mathbb{Z}$ such that

$$a = q \cdot b + r$$

with $0 \leq r < b$. The integer q is called the **quotient** when a is divided by b, and the integer r is called the (**least nonnegative**) **remainder** when a is divided by b.

Proof. If b divides a, that is, $a = q \cdot b$ for some integer q, then $r = 0$ and we are done. Suppose then that b does not divide a, and let

$$S = \{a - tb \,|\, t \in \mathbb{Z},\ a - tb > 0\}.$$

Note that if $a > 0$ and $t = 0$, then

$$a = a - 0 \cdot b \in S,$$

so that $S \neq \emptyset$.

Also, note that if $a \leq 0$ and $t = a - 1$, then

$$a - tb = a - (a - 1)b = a(1 - b) + b > 0$$

since $b \geq 1$, and again $a - tb \in S$, so that $S \neq \emptyset$.

Therefore, for any $a \in \mathbb{Z}$, S is a nonempty set of positive integers, and by the well-ordering principle, S has a smallest element, call it r. Since $r \in S$, then

$$0 < r = a - qb$$

for some $q \in \mathbb{Z}$.

Note that if $r = b$, then $a = (q + 1)b$ and b divides a, which is a contradiction. Also note that if $r > b$, then $r = b + c$ for some $c \in \mathbb{N}^+$, and then

$$a - qb = r = b + c$$

implies that $c = a - (q + 1)b \in S$, and $c = r - b < r$, which contradicts the fact that r is the smallest element of S.

This shows that there exist integers q and r such that

$$a = q \cdot b + r$$

with $0 \leq r < b$.

Now we show that these integers are unique. Suppose that

$$a = q_1 b + r_1 \qquad \text{and} \qquad a = q_2 b + r_2$$

where $q_1, q_2, r_1, r_2 \in \mathbb{Z}$ with $0 \leq r_1, r_2 < b$, then

$$q_1 b + r_1 = q_2 b + r_2 \tag{$*$}$$

and therefore

$$(q_1 - q_2)b = r_2 - r_1,$$

so that

$$|q_1 - q_2|b = |r_1 - r_2| < b. \tag{$**$}$$

If $q_1 \neq q_2$, then $|q_1 - q_2| \geq 1$, and $(**)$ implies that $b < b$, which is a contradiction. Therefore, $q_1 = q_2$, and then from $(*)$ we have $r_1 = r_2$.

$\square$

Note: We can give explicit formulas for the quotient q and the least nonnegative remainder r in the division algorithm when the integer a is divided by the positive integer b. In fact, since $0 \leq r = a - q \cdot b < b$, then

$$q \cdot b \leq a < (q+1) \cdot b,$$

and dividing by the positive integer b, we have

$$q \leq \frac{a}{b} < q + 1,$$

that is, $q = \left\lfloor \frac{a}{b} \right\rfloor$, and $r = a - \left\lfloor \frac{a}{b} \right\rfloor$.

We can use this fact to give a useful property of the floor function.

Theorem. If $n \in \mathbb{Z}^+$ and $x \in \mathbb{R}$, then

$$\left\lfloor \frac{x}{n} \right\rfloor = \left\lfloor \frac{\lfloor x \rfloor}{n} \right\rfloor.$$

Proof. Let $m = \lfloor x \rfloor$, using the division algorithm to divide m by n, we get

$$m = q \cdot n + r$$

where $0 \leq r \leq n - 1$, so that

$$\frac{m}{n} = q + \frac{r}{n}$$

where $0 \leq \frac{r}{n} \leq 1 - \frac{1}{n} < 1$, and therefore $q = \left\lfloor \frac{m}{n} \right\rfloor$.

Now, since $m = \lfloor x \rfloor$, then $m \leq x < m + 1$, so that

$$\frac{m}{n} \leq \frac{x}{n} < \frac{m}{n} + \frac{1}{n},$$

and so

$$q \leq q + \frac{r}{n} \leq \frac{x}{n} < q + \frac{r}{n} + \frac{1}{n} < q + 1$$

since $0 \leq \frac{r}{n} < 1 - \frac{1}{n}$. Therefore, $q = \left\lfloor \frac{x}{n} \right\rfloor$.

□

Note: We defined an integer n to be *even* if and only if $n = 2 \cdot k$ for some integer k, and to be *odd* if and only if $n = 2 \cdot k + 1$ for some integer k. Thus, n is even if and only if it leaves a remainder of 0 when divided by 2, while n is odd if and only if it leaves a remainder of 1 when divided by 2. The division algorithm provides another proof that every integer is either even or odd, but not both.

Definition. An integer n is said to be a **prime** if and only if $n > 1$ and the only positive divisors of n are 1 and n.

A positive integer n is said to be **composite** if and only if $n > 1$ and n is not a prime. Thus, $n > 1$ is composite if and only if there exist integers a and b with $1 < a$, $b < n$ such that $n = a \cdot b$.

As an exercise using the division algorithm, we prove the following:

Theorem. If p and p^2+2 are both primes, then p^2-2 is also a prime.

Proof. Suppose that p is a prime, when the division algorithm is used to divide p by 3,

$$p = 3q + r$$

where $0 \leq r \leq 2$, so the only possible remainders are $r=0,\ r=1,$ and $r=2$.

case 1: If $r=0$, then $p=3q$ for some positive integer q, and since p is prime, we must have $q=1$, so that $p=3$. In this case, $p^2+2=3^2+2=9+2=11$ is a prime, and $p^2-2=9-2=7$ is also a prime. Thus, the implication is true for $p=3$. The implication is also true if $p \neq 3$ and $3 \,\big|\, p$, since in this case the hypothesis is false.

case 2: If $r=1$, then $p=3q+1$ for some positive integer q, and

$$p^2+2=(3q+1)^2+2=9q^2+6q+3=3(3q^2+2q+1)$$

and $3 \,\big|\, p^2+2$. Since the second factor is clearly greater than 1, then p^2+2 is composite in this case, and again the implication is true since the hypothesis is false.

case 3: If $r=2$, then $p=3q+2$ for some positive integer q, and

$$p^2+2=(3q+2)^2+2=9q^2+12q+6=3(3q^2+4q+2)$$

and again $3 \,\big|\, p^2+2$. Since the second factor is clearly greater than 1, then p^2+2 is also composite in this case, and again the implication is true since the hypothesis is false.

Therefore, if p and p^2+2 are both prime, then p^2-2 is also prime.

□

We will show that there are infinitely many primes, in fact, the proof we give is Euclid's original proof.

Lemma. Every positive integer $n>1$ has a prime divisor.

Proof. Let $S=\{n \in \mathbb{Z} \,|\, n>1 \text{ and } n \text{ has no prime divisors}\}$. If $S \neq \emptyset$, since S is bounded below, by the well ordering property S has a smallest element, say $n_0 \in S$.

Since $n_0>1$ and n_0 has no prime divisors, then n_0 is composite, and there exist integers $a_0, b_0 \in \mathbb{Z}$ such that

$$n_0 = a_0 \cdot b_0$$

where $1<a_0<n_0$ and $1<b_0<n_0$.

However, since $1<a_0<n_0$ and n_0 is the smallest element in S, then $a_0 \notin S$, which implies that a_0 has a prime divisor, say $p \,\big|\, a_0$, but then $p \,\big|\, n_0$ also, which is a contradiction.

Therefore, the assumption that $S \neq \emptyset$ leads to a contradiction, and we must have $S=\emptyset$, so that every positive integer $n>1$ has a prime divisor. □

Theorem. There are infinitely many primes.

Proof. Suppose not, suppose that p_1, p_2, …, p_N are the only primes. Now consider the integer

$$M = p_1 \cdot p_2 \cdots p_N + 1,$$

from the previous lemma, M has a prime divisor, and it must therefore be one of the primes p_1, p_2, …, p_N. This is a contradiction, since none of these primes divides M. □

Now we give a theorem to determine whether a positive integer is a prime, that is, a simple *primality test.*

Theorem. If n is a composite integer, then n has a prime divisor p such that $p \leq \sqrt{n}$.

Proof. If n is composite, then $n = a \cdot b$, where $1 < a \leq b < n$. If $a > \sqrt{n}$, then $b \geq a > \sqrt{n}$, and this implies that

$$n = a \cdot b > \sqrt{n} \cdot \sqrt{n} = n$$

which is a contradiction. Therefore, $a \leq \sqrt{n}$ and since $a > 1$, then a has a prime divisor p such that $p \leq a \leq \sqrt{n}$, and since $p \,\big|\, a$ and $a \,\big|\, n$, then $p \,\big|\, n$ also. □

Before the advent of the computer, one of the most efficient methods of constructing tables of primes was the *sieving process*, invented by the Greek mathematician *Eratosthenes* (276-194 B.C.). The method is called the *Sieve of Eratosthenes.*

We illustrate the method by constructing a table containing all primes less that 130. We begin by listing all the integers from 2 to 129 (since 1 is not a prime it is not listed). The work involved in the process is simplified by the previous lemma.

The first number in our list, 2, must be a prime and no multiple of 2 except 2 itself can be prime. We remove all multiples of 2 (except $2 \cdot 1$) from our list. The next remaining number, 3, must be a prime, so we delete all the multiples of 3. We now delete the multiples of 5, the multiples of 7, and the multiples of 11. Because the largest prime less than $\sqrt{130}$ is 11, then from the lemma, all the remaining numbers must be primes. In the table below, rather than delete multiples of 2, 3, 5, 7, 11, we have underlined the integers that were not deleted, thus, all primes less than 130 are all underlined.

		$\underline{2}$	$\underline{3}$	4	$\underline{5}$	6	$\underline{7}$	8	9
10	$\underline{11}$	12	$\underline{13}$	14	15	16	$\underline{17}$	18	$\underline{19}$
20	21	22	$\underline{23}$	24	25	26	27	28	$\underline{29}$
30	$\underline{31}$	32	33	34	35	36	$\underline{37}$	38	39
40	$\underline{41}$	42	$\underline{43}$	44	45	46	$\underline{47}$	48	49
50	51	52	$\underline{53}$	54	55	56	57	58	$\underline{59}$
60	$\underline{61}$	62	63	64	65	66	$\underline{67}$	68	69
70	$\underline{71}$	72	$\underline{73}$	74	75	76	77	78	$\underline{79}$
80	81	82	$\underline{83}$	84	85	86	87	88	$\underline{89}$
90	91	92	93	94	95	96	$\underline{97}$	98	99
100	$\underline{101}$	102	$\underline{103}$	104	105	106	$\underline{107}$	108	$\underline{109}$
110	111	112	$\underline{113}$	114	115	116	117	118	119
120	121	122	123	124	125	126	$\underline{127}$	128	129

The sieve of Eratosthenes can be used to derive a formula for the number of primes less than or equal to n if the primes less than or equal to $\sqrt{n}$ are known. First a standard definition.

Definition. If x is a real number, then $\pi(x)$ denotes the number of prime numbers less than or equal to x.

Theorem. If $p_1, p_2, \ldots, p_k$ are the primes less than $\sqrt{n}$, then

$$\begin{aligned}\pi(n) = n - 1 + \pi(\sqrt{n}) &- \left\{ \left\lfloor \frac{n}{p_1} \right\rfloor + \left\lfloor \frac{n}{p_2} \right\rfloor + \cdots + \left\lfloor \frac{n}{p_k} \right\rfloor \right\} \\ &+ \left\{ \left\lfloor \frac{n}{p_1 p_2} \right\rfloor + \left\lfloor \frac{n}{p_1 p_3} \right\rfloor + \cdots + \left\lfloor \frac{n}{p_1 p_k} \right\rfloor + \left\lfloor \frac{n}{p_2 p_3} \right\rfloor + \cdots + \left\lfloor \frac{n}{p_{k-1} p_k} \right\rfloor \right\} \\ &- \left\{ \left\lfloor \frac{n}{p_1 p_2 p_3} \right\rfloor + \cdots + \left\lfloor \frac{n}{p_{k-2} p_{k-1} p_k} \right\rfloor \right\} + \cdots \\ &+ (-1)^k \left\lfloor \frac{n}{p_1 p_2 \cdots p_k} \right\rfloor\end{aligned}$$

A rigorous proof of this formula follows immediately from the Principle of Inclusion and Exclusion. We will give an informal argument.

Recall the steps in the sieve of Eratosthenes. The number of elements in the original set is $n-1$. The number divisible by p_1 is $\left\lfloor \dfrac{n}{p_1} \right\rfloor$, the number divisible by p_2 is $\left\lfloor \dfrac{n}{p_2} \right\rfloor$. If we delete all the numbers divisible by p_1 (including p_1 itself) and then all the numbers divisible by p_2 (including p_2 itself), we have deleted

$$\left\lfloor \frac{n}{p_1} \right\rfloor + \left\lfloor \frac{n}{p_2} \right\rfloor - \left\lfloor \frac{n}{p_1 p_2} \right\rfloor$$

numbers. If we continue this line of reasoning, we obtain $n-1$ plus the complicated expression involving the greatest integer function for the number of elements remaining in the set. In the process, we have removed the prime numbers $p_1, p_2, \ldots, p_k$ from the list as well as their multiples. When we replace these $\pi(\sqrt{n})$ numbers, we get the correct result, namely, $\pi(n)$.

As an example of the use of this formula, we can calculate the number of primes less than or equal to 129. In this case

$$\pi(\sqrt{n}) = \pi(\sqrt{129}) = 5,$$

and the primes less than or equal to $\sqrt{129}$ are $2, 3, 5, 7, 11$. From the formula in the theorem, we have

$$\begin{aligned}\pi(129) &= 129 - 1 + 5 - \left\lfloor \frac{129}{2} \right\rfloor - \left\lfloor \frac{129}{3} \right\rfloor - \left\lfloor \frac{129}{5} \right\rfloor - \left\lfloor \frac{129}{7} \right\rfloor - \left\lfloor \frac{129}{11} \right\rfloor \\ &\quad + \left\lfloor \frac{129}{2 \cdot 3} \right\rfloor + \left\lfloor \frac{129}{2 \cdot 5} \right\rfloor + \left\lfloor \frac{129}{2 \cdot 7} \right\rfloor + \left\lfloor \frac{129}{2 \cdot 11} \right\rfloor + \left\lfloor \frac{129}{3 \cdot 5} \right\rfloor + \left\lfloor \frac{129}{3 \cdot 7} \right\rfloor \\ &\quad + \left\lfloor \frac{129}{3 \cdot 11} \right\rfloor + \left\lfloor \frac{129}{5 \cdot 7} \right\rfloor + \left\lfloor \frac{129}{5 \cdot 11} \right\rfloor + \left\lfloor \frac{129}{7 \cdot 11} \right\rfloor \\ &\quad - \left\lfloor \frac{129}{2 \cdot 3 \cdot 5} \right\rfloor - \left\lfloor \frac{129}{2 \cdot 3 \cdot 7} \right\rfloor - \left\lfloor \frac{129}{2 \cdot 3 \cdot 11} \right\rfloor - \left\lfloor \frac{129}{2 \cdot 5 \cdot 7} \right\rfloor - \left\lfloor \frac{129}{2 \cdot 5 \cdot 11} \right\rfloor \\ &\quad - \left\lfloor \frac{129}{2 \cdot 7 \cdot 11} \right\rfloor - \left\lfloor \frac{129}{3 \cdot 5 \cdot 7} \right\rfloor - \left\lfloor \frac{129}{3 \cdot 5 \cdot 11} \right\rfloor - \left\lfloor \frac{129}{3 \cdot 7 \cdot 11} \right\rfloor - \left\lfloor \frac{129}{5 \cdot 7 \cdot 11} \right\rfloor \\ &\quad + \left\lfloor \frac{129}{2 \cdot 3 \cdot 5 \cdot 7} \right\rfloor + \left\lfloor \frac{129}{2 \cdot 3 \cdot 5 \cdot 11} \right\rfloor + \left\lfloor \frac{129}{2 \cdot 3 \cdot 7 \cdot 11} \right\rfloor + \left\lfloor \frac{129}{2 \cdot 5 \cdot 7 \cdot 11} \right\rfloor + \left\lfloor \frac{129}{3 \cdot 5 \cdot 7 \cdot 11} \right\rfloor \\ &\quad - \left\lfloor \frac{129}{2 \cdot 3 \cdot 5 \cdot 7 \cdot 11} \right\rfloor \\ &= 129 - 1 + 5 - 64 - 43 - 25 - 18 - 11 + 21 + 12 + 9 + 5 + 8 + 6 + 3 + 3 + 2 + 1 \\ &\quad - 4 - 3 - 1 - 1 - 1 - 0 - 1 - 0 - 0 - 0 + 0 + 0 + 0 + 0 + 0 - 0 \\ &= 31.\end{aligned}$$

We can verify that this is correct by counting the number of primes in the table (the integers that are underlined). Although this formula is very awkward to use, it is the only formula for the exact value of $\pi(n)$.

Greatest Common Divisor

Recall that we introduced the notion of "divisibility" for two integers a and b when we discussed the division algorithm, now we give some properties of the division operation.

Definition. If $a, b \in \mathbb{Z}$, then we say that b **divides** a and we write $b \,\big|\, a$, if and only if $b \neq 0$ and there exists an integer q such that $a = q \cdot b$. In this case, we also say that b is a **divisor** of a, or that a is a **multiple** of b. If b does not divide a, then we write $b \nmid a$.

We have the following properties for the division operation.

Theorem. If $a, b, c \in \mathbb{Z}$, then

(a) $1 \,\big|\, a$ and $a \,\big|\, 0$

(b) if $a \,\big|\, b$ and $b \,\big|\, a$ then $a = \pm b$

(c) if $a \,\big|\, b$ and $b \,\big|\, c$ then $a \,\big|\, c$

(d) if $a \,\big|\, b$ then $a \,\big|\, b \cdot x$ for all $x \in \mathbb{Z}$

(e) if $x = y + z$ and a divides any two of the integers $x,\ y,$ or z, then a divides the remaining integer

(f) if $a \,\big|\, b$ and $a \,\big|\, c$ then $a \,\big|\, bx + cy$ for all $x, y \in \mathbb{Z}$.

Proof. We will prove part (b), and leave the rest as an exercise.

Suppose that $a \,\big|\, b$ and $b \,\big|\, a$, from the definition of the division operation it follows that $a \neq 0$ and $b \neq 0$, and that there exist integers k and ℓ such that

$$a = k \cdot b \qquad \text{and} \qquad b = \ell \cdot a,$$

so that

$$a = k \cdot b = k \cdot \ell \cdot a,$$

and from the cancellation law, since $a \neq 0$, we have $k \cdot \ell = 1$. Since k and ℓ are nonzero integers, then $|k| \geq 1$ and $|\ell| \geq 1$, so we must have either $k = \ell = 1$ or $k = \ell = -1$, that is, either $a = b$ or $a = -b$.

□

Since we are only really interested in *positive* divisors, we make the following definition:

Definition. If $a, b \in \mathbb{Z}$, a positive integer c is said to be a **common divisor** of a and b if and only if $c \,\big|\, a$ and $c \,\big|\, b$.

Example. The common divisors of 42 and 70 are 1, 2, 7, 14, and $d = 14$ is the *greatest* of the common divisors of 42 and 70.

Definition. If $a, b \in \mathbb{Z}$, where at least one of the integers a and b is nonzero, then a positive integer d is called a **greatest common divisor** of a and b if and only if

(i) $d \,\big|\, a$ and $d \,\big|\, b$,

(ii) for any common divisor c of a and b, we have $c \,\big|\, d$.

Any greatest common divisor of a and b is denoted by $\gcd(a, b)$, and we have the following theorem.

Theorem. For any $a, b \in \mathbb{Z}^+$, there exists a unique $d \in \mathbb{Z}^+$ such that d is the greatest common divisor of a and b, that is, $d = \gcd(a, b)$.

Moreover, $d = \gcd(a, b)$ is the smallest positive integer that can be written as a linear combination of a and b, that is, the smallest positive integer d such that

$$d = ax + by$$

for some $x, y \in \mathbb{Z}$.

Proof. Given $a, b \in \mathbb{Z}^+$, let

$$S = \{as + bt \,\big|\, s, t \in \mathbb{Z},\ as + bt > 0\},$$

then S is a nonempty set of positive integers (a and b are in S), and by the well-ordering principle, S has a smallest element, say d. We claim that d is a greatest common divisor of a and b.

Since $d \in S$, then $d = ax + by$ for some $x, y \in \mathbb{Z}$, and if c is a common divisor of a and b, then $c \,\big|\, d$ also.

If $d \not\big| \, a$, then from the division algorithm, there exist integers q and r such that

$$a = q \cdot d + r$$

with $0 < r < d$, so that

$$r = a - q \cdot d = a - q(ax + by) = (1 - qx)a + (-qy)b,$$

and $r \in S$ and $0 < r < d$, which contradicts the choice of d as the least element of S.

Thus, $d \,\big|\, a$, and a similar argument shows that $d \,\big|\, b$.

Therefore, any $a, b \in \mathbb{Z}^+$ have a greatest common divisor.

To prove uniqueness, suppose that d_1 and d_2 are positive integers that satisfy the definition of the greatest common divisor, then $d_1 \,\big|\, d_2$ and $d_2 \,\big|\, d_1$, and since d_1 and d_2 are positive, this implies that $d_1 = d_2$. □

Note: We have shown that any two positive integers a and b have a unique greatest common divisor, which we denote by $\gcd(a, b)$. We define it for other integers as follows:

(i) if $a \in \mathbb{Z}$, with $a \neq 0$, then we define

$$\gcd(a, 0) = |a|,$$

(ii) if $a, b \in \mathbb{Z}^+$, then we define

$$\gcd(-a, b) = \gcd(a, -b) = \gcd(-a, -b) = \gcd(a, b),$$

(iii) $\gcd(0, 0)$ is **not** defined.

Definition. If $a, b \in \mathbb{Z}$, then we say that the integers a and b are **relatively prime** or **coprime** if and only if $\gcd(a, b) = 1$, that is, if and only if

$$ax + by = 1$$

for some $x, y \in \mathbb{Z}$.

Theorem. Any two consecutive Fibonacci numbers are relatively prime.

Proof. The proof is by induction.

Base Case: For $n = 1$, we have $F_1 = 1$ and $F_2 = 1$, and

$$\gcd(F_1, F_2) = \gcd(1, 1,) = 1.$$

Inductive Step: Now assume that F_n and F_{n+1} are relatively prime for some integer $n \geq 1$, since

$$F_{n+2} = F_{n+1} + F_n$$

if d is a positive common divisor of F_{n+1} and F_{n+2}, then $d \,\big|\, F_n$ also, so that d is a positive common divisor of F_n and F_{n+1}. By the inductive hypothesis, F_n and F_{n+1} are relatively prime, so that $d = 1$. Therefore, F_{n+1} and F_{n+2} are also relatively prime.

By the Principle of Mathematical Induction, and two consecutive Fibonacci numbers are relatively prime.

We can also give a proof using Cassini's identity:

$$F_{n+1}F_{n-1} - F_n^2 = (-1)^n.$$

If d is the greatest common divisor of F_n and F_{n+1}, then $d \,\big|\, (-1)^n$, so that $d = 1$.

□

Some results concerning relatively prime integers are given below.

Theorem. If a, b, and c are integers with a and b relatively prime, and if $a \,\big|\, bc$, then $a \,\big|\, c$.

Proof. If a and b are relatively prime, then $d = \gcd(a, b) = 1$, and therefore there exist integers x and y such that

$$1 = ax + by,$$

multiplying this equation by c, we have

$$c = acx + bcy.$$

Clearly $a \,\big|\, acx$, and by assumption $a \,\big|\, bcy$, so that $a \,\big|\, c$ also.

□

Theorem. Let the positive integers a and b be relatively prime. If $a \,\big|\, c$ and $b \,\big|\, c$, then $ab \,\big|\, c$ also.

Proof. Since a and b are relatively prime, there exist integers x and y such that

$$1 = ax + by,$$

and multiplying this equation by c, we have

$$c = acx + bcy.$$

Now, if $a \,\big|\, c$, then $ab \,\big|\, bcy$, and if $b \,\big|\, c$, then $ab \,\big|\, acx$, and therefore $ab \,\big|\, c$.

□

Theorem. If $a, b \in \mathbb{Z}$ and $d = \gcd(a, b)$, then

$$\gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1,$$

that is, $\frac{a}{d}$ and $\frac{b}{d}$ are relatively prime.

Proof. There exist $x, y \in \mathbb{Z}$ such that $d = ax + by$, and therefore

$$\frac{a}{d} \cdot x + \frac{b}{d} \cdot y = 1,$$

and this is the smallest postive integer which is a linear combination of a/d and b/d.

$\square$

Example. Since $\gcd(3, 5) = 1$, then we can find integers x and y such that $3x + 5y = 1$. For example, take $x = 2$ and $y = -1$, then

$$3(2) + 5(-1) = 1.$$

However, for any $k \in \mathbb{Z}$, we have

$$1 = 3(2 - 5k) + 5(-1 + 3k),$$

so the solution for x and y is not unique.

We can define the greatest common divisor for set of integers conaining more than two elements as follows.

Definition. Let $a_1, a_2, \ldots, a_n$ be integers, not all zero, the **greatest common divisor** of $a_1, a_2, \ldots, a_n$, denoted by

$$(a_1, a_2, \ldots, a_n) \qquad \text{or} \qquad \gcd(a_1, a_2, \ldots, a_n)$$

is the largest integer d such that $d \,\big|\, a_k$ for all $1 \leq k \leq n$.

The next lemma shows that we can find the greatest common divisor of more than two integers recursively.

Lemma. If $a_1, a_2, \ldots, a_n$ are integers, not all zero, then

$$(a_1, a_2, \ldots, a_n) = (a_1, a_2, \ldots, a_{n-2}, (a_{n-1}, a_n)).$$

Proof. Note that any common divisor of the integers $a_1, a_2, \ldots, a_n$ is a divisor of a_{n-1} and a_n, and so is a divisor of (a_{n-1}, a_n).

Also, any common divisor of $a_1, a_2, \ldots, a_{n-2}$ and (a_{n-1}, a_n) is a common divisor of $a_1, a_2, \ldots, a_n$.

Therefore, the sets of integers

$$\{a_1, a_2, \ldots, a_n\} \qquad \text{and} \qquad \{a_1, a_2, \ldots, a_{n-2}, (a_{n-1}, a_n)\}$$

have the same common divisors.

$\square$

Example. If $a = 105,\ b = 140,$ and $c = 350$, then

$$(a, b, c) = (a, (b, c))$$

so that

$$(105, 140, 350) = (105, (140, 350)) = (105, 70) = 35.$$

□

Definition. The integers $a_1,\ a_2,\ \ldots,\ a_n$ are **mutually relatively prime** if and only if $(a_1,\ a_2,\ \ldots,\ a_n) = 1$, while they are said to be **pairwise relatively prime** if and only if $(a_i, a_j) = 1$ for $i \neq j$.

Note: If $a_1,\ a_2,\ \ldots,\ a_n$ are pairwise relatively prime, then they must be mutually relatively prime. The converse is false as the next example shows.

Example 4. Let $a = 15,\ b = 21,$ and $c = 35$, then

$$(a, b, c) = (15, 21, 35) = (15, (21, 35)) = (15, 7) = 1,$$

but

$$(15, 21) = 3, \qquad (15, 35) = 5, \qquad (21, 35) = 7,$$

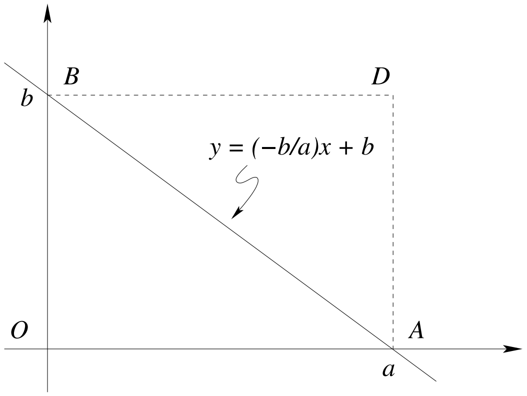
and no pair of the three integers $a,\ b,\ c$ is relatively prime.

To find the greatest common divisor of two positive integers a and b, we can always use brute force to list all their common divisors, and then simply select the largest from this list. There are more efficient methods, for example, the Euclidean algorithm. However, there is also an explict formula for the greatest common divisor which was found by the Brazilian mathematician Marcelo Polezzi in 1997.

Theorem. Let a and b be positive integers, and let $d = \gcd(a, b)$, then

$$d = 2\sum_{k=1}^{a-1} \left\lfloor k\frac{b}{a} \right\rfloor + a + b - ab.$$

Proof. We count the number of lattice points, that is, points with integer coordinates, on and inside the triangle $\triangle AOB$ shown below, in two different ways.



Here the equation of the line joining A and B is $y = -\dfrac{b}{a}\,x + b$.

First note that the number of lattice points on the legs of $\triangle AOB$ is

$$a+b+1,$$

while the number of lattice points inside or on the hypotenuse is

$$\sum_{k=1}^{a-1}\left\lfloor -k\frac{b}{a}+b\right\rfloor=\sum_{k=1}^{a-1}\left\lfloor (a-k)\frac{b}{a}\right\rfloor=\sum_{k=1}^{a-1}\left\lfloor k\frac{b}{a}\right\rfloor.$$

Therefore, if s equals the number of lattice points on or inside $\triangle AOB$, then

$$s=\sum_{k=1}^{a-1}\left\lfloor k\frac{b}{a}\right\rfloor+(a+b+1).$$

Next, note that the number of lattice points on the line segment AB equals the number of points (x,y) where x and $y=-\frac{b}{a}x+b$ are both integers, that is, the number of integers x such that $y=-\frac{b}{a}x+b$ is an integer for $0\le x\le a$. However, this is just the number of integers in the set

$$\{\,0,\ \frac{a}{d},\ \frac{2a}{d},\ \cdots,\ \frac{(d-1)a}{d},\ a\,\}.$$

So the number of lattice points on the line segment AB is equal to $d+1$.

Therefore, the number of lattice points inside $\triangle ADB$ or on its legs is equal to $s-(d+1)$.

Thus, the total number of lattice points on or inside the rectangle $OADB$ is equal to

$$s+[s-(d+1)]=2s-(d+1).$$

However, the total number of lattice points on or inside the rectangle $OADB$ is $(a+1)(b+1)$, and therefore

$$2s-(d+1)=(a+1)(b+1),$$

so that

$$d=2s-(a+1)(b+1)-1=2\sum_{k=1}^{a-1}\left\lfloor k\frac{b}{a}\right\rfloor+a+b-ab.$$

□

Example. If $a=4$ and $b=18$, then

$$\begin{aligned}(4,18)&=2\left\{\left\lfloor\frac{18}{4}\right\rfloor+\left\lfloor\frac{2\cdot 18}{4}\right\rfloor+\left\lfloor\frac{3\cdot 18}{4}\right\rfloor\right\}+4+18-4\cdot 18\\&=2\,(4+9+13)+4+18-72\\&=52+22-72\\&=2.\end{aligned}$$