



Proof. Applying the Euclidean algorithm, and using the defining relation for the Fibonacci numbers $f_j = f_{j-1} + f_{j-2}$ in each step, we see that

$$\begin{aligned} f_{n+2} &= f_{n+1} \cdot 1 + f_n, \\ f_{n+1} &= f_n \cdot 1 + f_{n-1}, \\ &\vdots \\ f_4 &= f_3 \cdot 1 + f_2, \\ f_3 &= f_2 \cdot 2. \end{aligned}$$

Hence, the Euclidean algorithm takes exactly n divisions, to show that $(f_{n+2}, f_{n+1}) = f_2 = 1$. ■

 **The Complexity of the Euclidean Algorithm** We can now prove a theorem first proved by *Gabriel Lamé*, a French mathematician of the nineteenth century, which gives an estimate for the number of divisions needed to find the greatest common divisor using the Euclidean algorithm.

 **Theorem 3.13. Lamé's Theorem.** The number of divisions needed to find the greatest common divisor of two positive integers using the Euclidean algorithm does not exceed five times the number of decimal digits in the smaller of the two integers.

Proof. When we apply the Euclidean algorithm to find the greatest common divisor of $a = r_0$ and $b = r_1$ with $a > b$, we obtain the following sequence of equations:

$$\begin{aligned} r_0 &= r_1q_1 + r_2, & 0 \leq r_2 < r_1, \\ r_1 &= r_2q_2 + r_3, & 0 \leq r_3 < r_2, \\ &\vdots \\ r_{n-2} &= r_{n-1}q_{n-1} + r_n, & 0 \leq r_n < r_{n-1}, \\ r_{n-1} &= r_nq_n. \end{aligned}$$

We have used n divisions. We note that each of the quotients $q_1, q_2, \dots, q_{n-1} \geq 1$, and $q_n \geq 2$, because $r_n < r_{n-1}$. Therefore,



GABRIEL LAMÉ (1795–1870) was a graduate of the *École Polytechnique*. A civil and railway engineer, he advanced the mathematical theory of elasticity and invented curvilinear coordinates. Although his main contributions were to mathematical physics, he made several discoveries in number theory, including the estimate of the number of steps required by the Euclidean algorithm, and the proof that Fermat's last theorem holds for $n = 7$ (see Section 13.2). It is interesting to note that Gauss considered Lamé to be the foremost French mathematician of his time.

$$\begin{aligned}
r_n &\geq 1 = f_2, \\
r_{n-1} &\geq 2r_n \geq 2f_2 = f_3, \\
r_{n-2} &\geq r_{n-1} + r_n \geq f_3 + f_2 = f_4, \\
r_{n-3} &\geq r_{n-2} + r_{n-1} \geq f_4 + f_3 = f_5, \\
&\vdots \\
r_2 &\geq r_3 + r_4 \geq f_{n-1} + f_{n-2} = f_n, \\
b = r_1 &\geq r_2 + r_3 \geq f_n + f_{n-1} = f_{n+1}.
\end{aligned}$$

Thus, for there to be n divisions used in the Euclidean algorithm, we must have $b \geq f_{n+1}$. By Example 1.28, we know that $f_{n+1} > \alpha^{n-1}$ for $n > 2$, where $\alpha = (1 + \sqrt{5})/2$. Hence, $b > \alpha^{n-1}$. Now, since $\log_{10} \alpha > 1/5$, we see that

$$\log_{10} b > (n - 1) \log_{10} \alpha > (n - 1)/5.$$

Consequently,

$$n - 1 < 5 \cdot \log_{10} b.$$

Let b have k decimal digits, so that $b < 10^k$ and $\log_{10} b < k$. Hence, we see that $n - 1 < 5k$, and because k is an integer, we can conclude that $n \leq 5k$. This establishes Lamé's theorem. ■

The following result is a consequence of Lamé's theorem. It tells us that the Euclidean algorithm is very efficient.

Corollary 3.13.1. The greatest common divisor of two positive integers a and b with $a > b$ can be found using $O((\log_2 a)^3)$ bit operations.

Proof. We know from Lamé's theorem that $O(\log_2 a)$ divisions, each taking $O((\log_2 a)^2)$ bit operations, are needed to find (a, b) . Hence, by Theorem 2.3, (a, b) may be found using a total of $O((\log_2 a)^3)$ bit operations. ■

Expressing Greatest Common Divisors—As Linear Combinations The Euclidean algorithm can be used to express the greatest common divisor of two integers as a linear combination of these integers. We illustrate this by expressing $(252, 198) = 18$ as a linear combination of 252 and 198. Referring to the steps of the Euclidean algorithm used to find $(252, 198)$, by the next to the last step we see that


$$18 = 54 - 1 \cdot 36.$$

By the preceding step, it follows that

$$36 = 198 - 3 \cdot 54,$$

which implies that

$$18 = 54 - 1 \cdot (198 - 3 \cdot 54) = 4 \cdot 54 - 1 \cdot 198.$$

 **Theorem 3.14.** Let a and b be positive integers. Then

$$(a, b) = s_n a + t_n b,$$

where s_n and t_n are the n th terms of the sequences defined recursively by

$$\begin{aligned} s_0 &= 1, & t_0 &= 0, \\ s_1 &= 0, & t_1 &= 1, \end{aligned}$$

and

$$s_j = s_{j-2} - q_{j-1} s_{j-1}, \quad t_j = t_{j-2} - q_{j-1} t_{j-1}$$

for $j = 2, 3, \dots, n$, where the q_j are the quotients in the divisions of the Euclidean algorithm when it is used to find (a, b) .

Proof. We will prove that

$$(3.2) \quad r_j = s_j a + t_j b$$

for $j = 0, 1, \dots, n$. Since $(a, b) = r_n$, once we have established (3.2), we will know that

$$(a, b) = s_n a + t_n b.$$

We prove (3.2) using the second principle of mathematical induction. For $j = 0$, we have $a = r_0 = 1 \cdot a + 0 \cdot b = s_0 a + t_0 b$. Hence, (3.2) is valid for $j = 0$. Likewise, $b = r_1 = 0 \cdot a + 1 \cdot b = s_1 a + t_1 b$, so that (3.2) is valid for $j = 1$.

Now, we assume that

$$r_j = s_j a + t_j b$$

for $j = 1, 2, \dots, k-1$. Then, from the k th step of the Euclidean algorithm, we have

$$r_k = r_{k-2} - r_{k-1} q_{k-1}.$$

Using the induction hypothesis, we find that

$$\begin{aligned} r_k &= (s_{k-2} a + t_{k-2} b) - (s_{k-1} a + t_{k-1} b) q_{k-1} \\ &= (s_{k-2} - s_{k-1} q_{k-1}) a + (t_{k-2} - t_{k-1} q_{k-1}) b \\ &= s_k a + t_k b. \end{aligned}$$

This finishes the proof. ■

The following example illustrates the use of this algorithm for expressing (a, b) as a linear combination of a and b .

Example 3.14. We summarize the steps used by the extended Euclidean algorithm to express $(252, 198)$ as a linear combination of 252 and 198 in the following table.

j	r_j	r_{j+1}	q_{j+1}	r_{j+2}	s_j	t_j
0	252	198	1	54	1	0
1	198	54	3	36	0	1
2	54	36	1	18	1	-1
3	36	18	2	0	-3	4
4					4	-5

The values of s_j and t_j , $j = 0, 1, 2, 3, 4$, are computed as follows:

$$\begin{aligned}
 s_0 &= 1, & t_0 &= 0, \\
 s_1 &= 0, & t_1 &= 1, \\
 s_2 &= s_0 - s_1q_1 = 1 - 0 \cdot 1 = 1, & t_2 &= t_0 - t_1q_1 = 0 - 1 \cdot 1 = -1, \\
 s_3 &= s_1 - s_2q_2 = 0 - 1 \cdot 3 = -3, & t_3 &= t_1 - t_2q_2 = 1 - (-1)3 = 4, \\
 s_4 &= s_2 - s_3q_3 = 1 - (-3) \cdot 1 = 4, & t_4 &= t_2 - t_3q_3 = -1 - 4 \cdot 1 = -5.
 \end{aligned}$$

Because $r_4 = 18 = (252, 198)$ and $r_4 = s_4a + t_4b$, we have

$$18 = (252, 198) = 4 \cdot 252 - 5 \cdot 198. \quad \blacktriangleleft$$

Note that the greatest common divisor of two integers may be expressed as a linear combination of these integers in an infinite number of ways. To see this, let $d = (a, b)$ and let $d = sa + tb$ be one way to write d as a linear combination of a and b , guaranteed to exist by the previous discussion. Then for all integers k ,

$$d = (s + k(b/d))a + (t - k(a/d))b.$$

Example 3.15. With $a = 252$ and $b = 198$, we have $18 = (252, 198) = (4 + 11k)252 + (-5 - 14k)198$ for any integer k . \blacktriangleleft

3.4 Exercises

- Use the Euclidean algorithm to find each of the following greatest common divisors.
 - (45, 75)
 - (102, 222)
 - (666, 1414)
 - (20785, 44350)
- Use the Euclidean algorithm to find each of the following greatest common divisors.
 - (51, 87)
 - (105, 300)
 - (981, 1234)
 - (34709, 100313)
- For each pair of integers in Exercise 1, express the greatest common divisor of the integers as a linear combination of these integers.
- For each pair of integers in Exercise 2, express the greatest common divisor of the integers as a linear combination of these integers.
- Find the greatest common divisor of each of the following sets of integers.
 - 6, 10, 15
 - 70, 98, 105
 - 280, 330, 405, 490

Example 4.10. Because $13 \equiv 3 \pmod{5}$ and $7 \equiv 2 \pmod{5}$, using Theorem 3.5 we see that $20 = 13 + 7 \equiv 3 + 2 \equiv 5 \pmod{5}$, $6 = 13 - 7 \equiv 3 - 2 \equiv 1 \pmod{5}$, and $91 = 13 \cdot 7 \equiv 3 \cdot 2 \equiv 6 \pmod{5}$. ◀

The following lemma helps us to determine whether a set of m numbers forms a complete set of residues modulo m .

Lemma 4.1. A set of m incongruent integers modulo m forms a complete set of residues modulo m .

Proof. Suppose that a set of m incongruent integers modulo m does not form a complete set of residues modulo m . This implies that at least one integer a is not congruent to any of the integers in the set. Hence, there is no integer in the set congruent modulo m to the remainder of a when it is divided by m . Hence, there can be at most $m - 1$ different remainders of the integers when they are divided by m . It follows (by the pigeonhole principle, which says that if more than n objects are distributed into n boxes, at least two objects are in the same box) that at least two integers in the set have the same remainder modulo m . This is impossible, because these integers are incongruent modulo m . Hence, any m incongruent integers modulo m form a complete system of residues modulo m . ■

Theorem 4.6. If r_1, r_2, \dots, r_m is a complete system of residues modulo m , and if a is a positive integer with $(a, m) = 1$, then

$$ar_1 + b, ar_2 + b, \dots, ar_m + b$$

is a complete system of residues modulo m for any integer b .

Proof. First, we show that no two of the integers

$$ar_1 + b, ar_2 + b, \dots, ar_m + b$$

are congruent modulo m . To see this, note that if

$$ar_j + b \equiv ar_k + b \pmod{m},$$

then, by (ii) of Theorem 4.3, we know that

$$ar_j \equiv ar_k \pmod{m}.$$

Because $(a, m) = 1$, Corollary 4.4.1 shows that

$$r_j \equiv r_k \pmod{m}.$$

Given that $r_j \not\equiv r_k \pmod{m}$ if $j \neq k$, we conclude that $j = k$.

By Lemma 4.1, because the set of integers in question consists of m incongruent integers modulo m , these integers form a complete system of residues modulo m . ■

The following theorem shows that a congruence is preserved when both sides are raised to the same positive integral power.