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:

$$\begin{aligned} r_0 &= r_1 q_1 + r_2, && 0 \le r_2 < r_1, \\ r_1 &= r_2 q_2 + r_3, && 0 \le r_3 < r_2, \\ &\vdots \\ r_{n-2} &= r_{n-1} q_{n-1} + r_n, && 0 \le r_n < r_{n-1}, \\ r_{n-1} &= r_n q_n. \end{aligned}$$

We have used n divisions. We note that each of the quotients $q_1, q_2, \ldots, q_{n-1} \ge 1$, and $q_n \ge 2$, 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

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