1. Recall: Euclidean algorithm for computing $\gcd(a,b)$ of two nonnegative integers with $a \geq b$.

   Let $r_0 = a$, and $r_1 = b$, then by successively apply the division algorithm, we obtain

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

   Consequently, we have

$$\gcd(a,b) = \gcd(r_0, r_1) = \gcd(r_1, r_2) = \cdots = \gcd(r_n, 0) = r_n.$$

   The number of divisions used by the Euclidean algorithm is n.

2. The Euclidean algorithm can be simply expressed by the following recursive form:

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

   with the condition $\gcd(c,0) = c$ when $c > 0$.

3. Pseudocode for $\gcd(a,b)$ with $a \geq b$.

```
procedure gcd(a,b)
if b = 0 then
   gcd(a,b) = a
else
   gcd(a,b) := gcd( b, a mod b)
endif
```

4. Complexity of the Euclidean algorithm

   Lamé's theorem: The number of divisions used by the Euclidean algorithm to find $\gcd(a,b)$ is less than or equal to 5 times the number of decimal digits in b, i.e.,

$$n \leq 5k,$$

   where $k = \lfloor \log_{10} b \rfloor + 1$.[1]

5. Before we prove Lamé's theorem, let us prove the following result.

   Lemma. Let f_n be the Fibonacci sequence, namely $f_n = f_{n-1} + f_{n-2}$ for $n \geq 2$ and $f_0 = 0$ and $f_1 = 1$. Then $f_n > \alpha^{n-2}$ for $n \geq 3$, where $\alpha = \frac{1}{2}(1+\sqrt{5})$ is the root of $\alpha^2 - \alpha - 1 = 0$.

   Proof. We use (strong) mathematical induction. Let $P(n)$ be the statement $f_n > \alpha^{n-2}$. We want to show that $P(n)$ is true whenever $n \geq 3$.

[1] If b has k decimal digits, then $b < 10^k$ and $\log_{10} b < k$. Precisely, the number k of the decimal digits in b is $k = \lfloor \log_{10} b \rfloor + 1$, which is less than or equal to $\log_{10} b + 1$.

Basis step: First note that

$$\alpha < 2 = f_3, \quad \alpha^2 = (3+\sqrt{5})/2 < 3 = f_4,$$

So $P(3)$ and $P(4)$ are true.

Inductive step: Assume that $P(j)$ is true, namely, $f_j > \alpha^{j-2}$ for all integers j with $3 \leq j \leq k$ for some $k \geq 4$.

We now show that $P(k+1)$ is true, that is $f_{k+1} > \alpha^{k+1-2} = \alpha^{k-1}$. In fact,

$$\begin{aligned} f_{k+1} &= f_k + f_{k-1} \\ &> \alpha^{k-2} + \alpha^{k-3} && \text{(by the inductive hypothesis)} \\ &= (\alpha+1)\alpha^{k-3} && \text{(since } \alpha \text{ is a root of } x^2 - x - 1 = 0\text{)} \\ &= \alpha^2 \cdot \alpha^{k-3} = \alpha^{k-1}. \end{aligned}$$

It follows that $P(k+1)$ is true. This completes the proof. □

6. Proof of Lamé's theorem

   By the Euclidean algorithm, we know

   - $r_0 > r_1 > r_2 > \cdots > r_{n-1} > r_n > 0$.
   - $q_1, q_2, \ldots, q_{n-1} \geq 1$.
   - $q_n \geq 2$ since $r_{n-1} > r_n > 0$.

   By these facts, we have

$$\begin{aligned} r_n &\geq 1 = f_2 \\ r_{n-1} = r_n q_n &\geq 2r_n \geq 2f_2 = f_3 \\ r_{n-2} = r_{n-1}q_{n-1} + r_n &\geq r_{n-1} + r_n \geq f_3 + f_2 = f_4 \\ &\vdots \\ r_2 = r_3 q_3 + r_4 &\geq r_3 + r_4 \geq f_{n-1} + f_{n-2} = f_n \\ b = r_1 = r_2 q_2 + r_3 &\geq r_2 + r_3 \geq f_n + f_{n-1} = f_{n+1} \end{aligned}$$

   Now by the last inequality and Lemma in item 5, we have

$$b \geq f_{n+1} \geq \alpha^{n-1}.$$

   Therefore

$$\log_{10} b \geq \log_{10} \alpha^{n-1} = (n-1)\log_{10}\alpha > (n-1)\cdot\frac{1}{5},$$

   where we the fact that $\log_{10}\alpha \approx 0.209 > \frac{1}{5}$. Consequently. we have

$$n \leq 5k,$$

   where k is the number of decimal digits in b.

7. As an example of applying Lamé's theorem. If b has 3 dicimal digits (whatever the size of a), Lemé's theorem tells us that the Eculidean algorithm will take less than or equal to $5\cdot(3+1) = 20$ divisions to find $\gcd(a,b)$.