would be a smaller positive element of D than c. The same argument shows that c divides b, so c satisfies property gcd-1. □

We write $c = \gcd(a, b)$. For example, $\gcd(-12, 16) = 4$. Note that $\gcd(0, 0)$ is undefined since every integer, no matter how large, divides both zeroes. Hence, the "not both zero" is a necessary assumption.

By convention, $\gcd(a, 0) = |a|$ for any $a \neq 0$. Other useful facts are:

- $\gcd(a, b) = \gcd(b, a) = \gcd(|a|, |b|)$.
- If $a' = \max(|a|, |b|)$ and $b' = \min(|a|, |b|)$, then $\gcd(a, b) = \gcd(a', b')$.
- If $a \neq 0$ and $b \neq 0$, then $\gcd(a, b) \leq \min(|a|, |b|)$.
- If a divides b, then $\gcd(a, b) = |a|$.

An efficient algorithm for computing greatest common divisors has been known for thousands of years, and was written down by Euclid around 300 BC. To start it off, first prepare the inputs by replacing $a \leftarrow \max(|a|, |b|)$ and $b \leftarrow \min(|a|, |b|)$, so as to guarantee that $a > 0$, $b \geq 0$, and $a \geq b$:

Euclid's Algorithm

```
gcd( a, b ):
[0] Let c = a
[1] Let a = b%a
[2] Let b = c
[3] If a>0, then go to [0]
[4] Print b
```

To analyze this algorithm, let a_n, b_n be the respective values of a, b after the n^{th} visit to step 2. Step 1 insures that $a > a_1 > a_2 > \cdots \geq 0$, and since each a_n is an integer, the loop must terminate after at most a steps. Steps 0 and 2 require copying the digits of a and c, step 1 is the division algorithm, step 3 requires reading the digits of a number to see if they are all 0, and step 4 requires printing the digits of a number. Hence, each step takes finitely many calculations, so the algorithm is finite.

Suppose $k \geq 1$ is the least index for which $a_k = 0$. Then a_{k-1} divides b_{k-1}, so the printed value is $b_k = a_{k-1} = \gcd(a_{k-1}, b_{k-1})$.

Note that any common divisor of both a and b also divides both $a_1 = b\%a$ and $b_1 = a$. For $n = 1, 2, \ldots, k$, the same observation reveals that any common divisor of a_n and b_n is a common divisor of both a_{n+1} and b_{n+1}. Hence, by induction on n, the set of common divisors of a and b equals the set of common divisors of a_n and b_n. In particular, these sets have the same largest element, $\gcd(a_n, b_n) = \gcd(a, b)$ for all $1 \leq n < k$, and the printed value will be $\gcd(a_{k-1}, b_{k-1}) = \gcd(a, b)$.

How many iterations through steps 0–2 will Euclid's algorithm take? Recall that for $1 \leq n < k$, $a_{n+1} < a_n$, so $a_{n+1} = a_n - d_n$ for some $0 < d_n \leq a_n$. But also, $b_{n+1} = a_n$, so for any $1 \leq n \leq k - 2$, $a_{n+2} = b_{n+1}\%a_{n+1} = a_n\%a_{n+1}$, which implies two things: $a_{n+2} < a_{n+1} = a_n - d_n$, and also $a_{n+2} = a_n\%(a_n - d_n) \leq d_n$.