Euclidean Algorithm

You may or may not have heard about the Euclidean Algorithm. Usually, it is introduced as a systematic method to find $\mathrm{GCD}(a, b)$ of two positive integers a and b. The Euclidean Algorithm relies on a simple result:

> *Theorem. For two positive integers $a > b$, if $a \bmod b = c$, then $\mathrm{GCD}(a, b) = \mathrm{GCD}(b, c)$.*

Proof. We only need to prove that the set of (positive) common divisors of a and b is identical to the set of (positive) common divisors of b and c.

- Suppose p is a (positive) common divisor of a and b. Then $a = mp$ and $b = np$ for some positive integers $m > n$. Since $a \bmod b = c$, we know $a = kb + c$ for some positive integer k. Therefore, we have $c = a - kb = mp - knp = (m - kn)p$, which implies p divides c.
- Suppose p is a (positive) common divisor of b and c. Then $b = xp$ and $c = yp$ for some positive integers $x > y$. (We know $x > y$ because $b > c$.) Therefore, we have $a = kb + c = kxp + yp = (kx + y)p$, which implies p divides a.

For a concrete example, suppose we were to find the greatest common divisor of 230 and 2024:

$2024 = 230 \times 8 + 184$ **// therefore GCD(230,2024) = GCD(230,184)**
$230 = 184 \times 1 + 46$ **// therefore GCD(230,184) = GCD(46,184)**
$184 = 46 \times 4$ **// therefore GCD(46,184) = 46**

Therefore, we have $\mathrm{GCD}(230, 2024) = 46$ (note that the comments on the right make a chain-of-equivalence).

What is less obvious is the Euclidean Algorithm can also help find the multiplicative inverse in modulo arithmetic (if one exists). More specifically, if $\mathrm{GCD}(a, b) = 1$, then the process of Euclidean Algorithm actually reveals the mystery number z such that $a \times z \equiv 1 \pmod{b}$. Look at this concrete example where we find the greatest common divisor of 230 and 7, although we know in advance that it is 1 (because 7 is a prime and 230 is not a multiple of 7):

$230 = 7 \times 32 + 6$ **// in other words,** $6 = 230 - 7 \times 32$
$7 = 6 \times 1 + 1$ **// in other words,** $1 = 7 - 6 \times 1$
$6 = 1 \times 6$

Now let's look at the notes on the right-hand side and combine the information there:

$$
\begin{aligned}
1 &= 7 - 6 \times 1 \\
&= 7 - (230 - 7 \times 32) \times 1 \\
&= 7 \times 33 - 230 \\
&= 7 \times 33 + 230 \times (-1).
\end{aligned}
$$

This implies $1 \equiv 230 \times (-1) \pmod{7}$. If we don't want the mystery number to be negative, we can also conclude that $1 \equiv 230 \times 6 \pmod{7}$, since $6 \equiv (-1) \pmod{7}$.

Although in the example above 7 is a prime, the algorithm works for any two coprime integers a and b. Therefore, it is more powerful (strictly speaking about finding multiplicative inverses) than Fermat's Little Theorem, because the latter only works when b is a prime.

Practice the Euclidean Algorithm in the next practice quiz.