The (Extended) Euclidean Algorithm - RECAP

Euclid of Alexandria $\sim$ *300 BC.*

Greatest Common Divisor / Euclidean Algorithm

Greatest Common Divisor

For integers a, b the **greatest common divisor** (GCD) of a and b is the largest positive integer d that divides both a and b.

Question: How to find the GCD of two numbers?

Euclidean Algorithm

Input: Integers a, b with $a \geq b \geq 0$.
Output: Integer d that is the greatest common divisor of a and b.

Recipe:
Find $q_1, r_1 \in \{0, 1, 2, \ldots\}$ such that:
$a = q_1 b + r_1$ **and** $r_1 < b$.
Find $q_2, r_2 \in \{0, 1, 2, \ldots\}$ such that:
$b = q_2 r_1 + r_2$ and $r_2 < r_1$.

Continue: Find $q_i, r_i \in \{0, 1, 2, \ldots\}$ s.t.:
$r_{i-2} = q_i r_{i-1} + r_i$ and $r_i < r_{i-1}$
until $r_i = 0$.
Then: $d = r_{i-1}$ (the second-last remainder) is the GCD between a and b.

Modular Inverse / Extended Euclidean Algorithm

Inverses $\mod p$

Let x be an integer and p be a prime. The inverse of $x \mod p$ is defined as the number $y \mod p$ such that $x \cdot y = 1 \mod p$. Usually y is denoted as $y = x^{-1}$.

Question: How to find the inverse of x modulus p?

Extended Euclidean Algorithm

Input: Integer x and prime number p.
Output: Integer $y \mod p$ such that $x \cdot y = 1 \mod p$.

Recipe:

1. Compute the Euclidean Algorithm between x and p
2. Find an equation of the form $1 = r_{i-2} - q_i r_{i-1}$.
3. Read the equation 'reversely' and write each remainder as a combination of the previous reminders, until you reach an equation of the form $1 = x \cdot y + p \cdot m$.
4. The equation above modulus p reads: $x \cdot y = 1 \mod p$, thus y is the modular inverse of x modulus p

watchout: the EEA works also when p is not prime! You can use it to find the inverse of any $x \mod n$ (for general n) everytime x and n are coprime, i.e. $GCD(x, n) = 1$.