CIT 596: ALGORITHMS & COMPUTATION

Extended GCD

Getting More from Euclid's Algorithm

- Euclid's algorithm computes the greatest common divisor of two integers a and b.

```
EUCLID(a, b)
    if b == 0
        return a
    else
        EUCLID(b, a % b)
```


- Along the way, we can also find two integers x and y (one positive, one negative) such that

$$\gcd(a, b) = ax + by.$$

- Expressing $\gcd(a, b)$ as a linear combination of a and b is very useful for cryptography!

Example: $\mathbf{gcd(74, 26)}$

$$74 \% 26 = 74 \cdot 1 + 26 \cdot (-2) = 22$$
$$26 \% 22 = 26 \cdot 1 + 22 \cdot (-1) = 4$$
$$22 \% 4 = 22 \cdot 1 + 4 \cdot (-5) = 2$$
$$4 \% 2 = 4 \cdot 1 + 2 \cdot (-2) = 0$$

$$\begin{aligned} 2 &= 22 \cdot 1 + 4 \cdot (-5) \\ &= 22 \cdot 1 + \big(26 \cdot 1 + 22 \cdot (-1)\big) \cdot (-5) \\ &= 26 \cdot (-5) + 22 \cdot 6 \\ &= 26 \cdot (-5) + \big(74 \cdot 1 + 26 \cdot (-2)\big) \cdot 6 \\ &= 74 \cdot 6 + 26 \cdot (-17) \end{aligned}$$

The Extended GCD Algorithm

Input: Integers $a \geq 1$ and $b \geq 0$ with $a \geq b$

Output: Integers x, y, d such that $ax + by = d = \gcd(a, b)$

$\textsc{ExtendedGCD}(a, b)$

    if $b == 0$

        return $(1, 0, a)$

    else

        $(u, v, d) = \textsc{ExtendedGCD}(b, a \mathbin{\%} b)$

        return $(v, u - v \cdot \lfloor a/b \rfloor, d)$

Proof of Correctness

Base case: When $b = 0$, the algorithm returns $(1, 0, a)$, which is correct since $1 \cdot a + 0 \cdot b = a = \gcd(a, 0)$.

Inductive step: Fix $k \geq 1$ and assume the algorithm is correct for all $b < k$ (IH). We now show that the algorithm is also correct for $b = k$.

Since $a \% b < b$, the IH tells us that

$$bu + (a \% b)v = d = \gcd(b, a \% b).$$

We know that $\gcd(b, a \% b) = \gcd(a, b)$, so it suffices to show that

$$av + b \cdot (u - v \cdot \lfloor a/b \rfloor) = bu + (a \% b)v.$$

Subtracting bu from both sides and dividing both sides by v yields

$$a \% b = a - b \cdot \lfloor a/b \rfloor,$$

which is the definition of $a \% b$. $\square$