Lecture 3.7: The Euclidean algorithm

Matthew Macauley

Department of Mathematical Sciences
Clemson University
http://www.math.clemson.edu/~macaule/

Math 4190, Discrete Mathematical Structures

Greatest common divisor

Definition

Let $a, b \in \mathbb{Z}$, not both zero. The greatest common divisor of a and b, denoted $\gcd(a, b)$, is the positive integer d satisfying:

(i) d is a common divisor of a and b, i.e.,

$$d \mid a \quad \text{and} \quad d \mid b.$$

(ii) If c also divides a and b, then $c \leq d$. In other words,

$$\forall c \in \mathbb{N}, \quad \text{if } c \mid a \text{ and } c \mid b, \text{ then } c \leq d.$$

Examples

Compute the following:

1. $\gcd(72, 63) =$
2. $\gcd(10^{12}, 6^{18}) =$
3. $\gcd(5, 0) =$
4. $\gcd(0, 0) =$

Greatest common divisor

Lemma

If $a, b \in \mathbb{Z}$ are not both zero, and $q, r \in \mathbb{Z}$ satisfy $a = bq + r$, then

$$\gcd(a, b) = \gcd(b, r).$$

Proof

We'll show:

1. $\gcd(a, b) \leq \gcd(b, r)$.

2. $\gcd(b, r) \leq \gcd(a, b)$.

The Euclidean algorithm

Around 300 B.C., Euclid wrote his famous book, *The Elements*, in which he described what is now known as the Euclidean algorithm:

Proposition VII.2 (Euclid's *Elements*)

Given two numbers not prime to one another, to find their greatest common measure.

The algorithm works due to two key observations:

- If $a \mid b$, then $\gcd(a, b) = a$;
- If $a = bq + r$, then $\gcd(a, b) = \gcd(b, r)$.

This is best seen by an example: Let $a = 654$ and $b = 360$.

$$
\begin{array}{ll}
654 = 360 \cdot 1 + 294 & \qquad \gcd(654, 360) = \gcd(360, 294) \\
360 = 294 \cdot 1 + 66 & \qquad \gcd(360, 294) = \gcd(294, 66) \\
294 = 66 \cdot 4 + 30 & \qquad \gcd(294, 66) = \gcd(66, 30) \\
66 = 30 \cdot 2 + 6 & \qquad \gcd(66, 30) = \gcd(30, 6) \\
30 = 6 \cdot 5 & \qquad \gcd(30, 6) = 6.
\end{array}
$$

We conclude that $\gcd(654, 360) = 6$.

The Euclidean algorithm (modernized)

Input: Integers $A, B \in \mathbb{Z}$ with $A > B \geq 0$.

Initalize. $a := A$, $b := B$, $r := B$.

while $(b \neq 0)$

  $r := a \bmod b$

  $a := b$

  $b := r$

end while

gcd $:= a$

return gcd;

Writing the gcd as a linear combination

Proposition

Let $a, b \in \mathbb{Z}$, not both zero. Then $d = \gcd(a, b)$ is the smallest positive integer that can be written as

$$d = ax + by, \qquad \text{for some } \; x, y \in \mathbb{Z}.$$

Proof

Define the set

$$S = \{u \mid u \in \mathbb{Z}^+, \; u = ax + by \text{ for some } x, y \in \mathbb{Z}\}.$$

Let $c = \min S$. Our goal is to show that $d = c$. We'll show:

1. $c \geq d$.

2. $c \leq d$.

The extended Euclidean algorithm

It can be useful to keep track of extra information when doing the Euclidean algorithm.

The following is an example of the extended Euclidean algorithm, for $a = 654$ and $b = 360$.

		654	360
	$654 = 1 \cdot 654 + 0 \cdot 360$	1	0
	$360 = 0 \cdot 654 + 1 \cdot 360$	0	1
$654 = 360 \cdot 1 + 294$	$294 = 1 \cdot 654 - 1 \cdot 360$	1	-1
$360 = 294 \cdot 1 + 66$	$66 = 1 \cdot 360 - 1 \cdot 294$	-1	2
$294 = 66 \cdot 4 + 30$	$30 = 1 \cdot 294 - 4 \cdot 66$	5	-9
$66 = 30 \cdot 2 + 6$	$6 = 1 \cdot 66 - 2 \cdot 30$	-11	20
$30 = 6 \cdot 5$			

We conclude that:

$$\gcd(654, 360) = 6 = 654(-11) + 360(20).$$

This allows us to solve equations of the form

$$654x \equiv 6 \mod 360 \qquad \Longrightarrow \qquad x = -11 \equiv 349 \pmod{360}$$

and

$$360x \equiv 6 \mod 654 \qquad \Longrightarrow \qquad x = 20 \pmod{654},$$

which we'll need when we study cryptography.