MATH1081 – Discrete Mathematics

Topic 2 – Number theory and relations
Lecture 2.02 – The Euclidean algorithm

Lecturer: Dr Sean Gardiner – sean.gardiner@unsw.edu.au

The Division Theorem

Theorem. (Division Theorem)
For any integers a and b with $b \neq 0$, there exist unique integers q and r such that both

$$a = qb + r \quad \text{and} \quad 0 \leq r < |b|.$$

We call q the quotient and r the remainder when a is divided by b.

Proof. See Angell: Slide 3.37 (or Gardiner: Lecture 3.04, Example 4).

Example. What is the quotient and remainder when...

- 30 is divided by 7?
- 30 is divided by 6?
- 30 is divided by -4?
- -30 is divided by 4?

The Euclidean algorithm

The Euclidean algorithm is a process that, given two integers a and $b \neq 0$ as inputs, efficiently finds $\gcd(a, b)$. The algorithm makes use of the Division Theorem, finding quotients and remainders iteratively in the following way:

$$\begin{aligned}
a &= q_0 \times b + r_0 && \text{where } q_0, r_0 \in \mathbb{Z} \text{ and } |b| > r_0 \geq 0,\\
b &= q_1 \times r_0 + r_1 && \text{where } q_1, r_1 \in \mathbb{Z} \text{ and } r_0 > r_1 \geq 0,\\
r_0 &= q_2 \times r_1 + r_2 && \text{where } q_2, r_2 \in \mathbb{Z} \text{ and } r_1 > r_2 \geq 0,\\
r_1 &= q_3 \times r_2 + r_3 && \text{where } q_3, r_3 \in \mathbb{Z} \text{ and } r_2 > r_3 \geq 0,\\
&\vdots && \vdots\\
r_{n-2} &= q_n \times r_{n-1} + r_n && \text{where } q_n, r_n \in \mathbb{Z} \text{ and } r_{n-1} > r_n \geq 0,\\
r_{n-1} &= q_{n+1} \times r_n + 0 && \text{where } q_{n+1} \in \mathbb{Z} \text{ and } r_n > 0.
\end{aligned}$$

The process terminates immediately after the nth step, when the remainder is first found to be zero. The remainder at the nth step is then the GCD of a and b. That is,

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

Example – Euclidean algorithm

Example. Use the Euclidean algorithm to find $\gcd(403, 286)$.

Solution.

Example. Use the Euclidean algorithm to find $\gcd(283, 193)$.

Solution.

The Euclidean algorithm – proof

Theorem. For any integer inputs a and $b \neq 0$, the Euclidean algorithm always outputs $\gcd(a, b)$.

Proof.

Euclidean algorithm in reverse

Recall the Euclidean algorithm applied to 286 and 403 as follows:

$$\begin{aligned} 403 &= 1 \times 286 + 117, && ① \\ 286 &= 2 \times 117 + 52, && ② \\ 117 &= 2 \times 52 + 13, && ③ \\ 52 &= 4 \times 13 + 0. \end{aligned}$$

Notice that working backwards from the penultimate line, it should be possible to make careful substitutions so that we can eventually express $\gcd(403, 286)$ as an integer linear combination of 403 and 286:

$$\begin{aligned} 13 &= 117 - 2 \times 52 && \text{(from ③)} \\ &= 117 - 2 \times (286 - 2 \times 117) && \text{(substituting from ②)} \\ &= 5 \times 117 - 2 \times 286 && \text{(collecting terms)} \\ &= 5 \times (403 - 286) - 2 \times 286 && \text{(substituting from ①)} \\ &= 5 \times 403 - 7 \times 286 && \text{(collecting terms).} \end{aligned}$$

So we can write $\gcd(403, 286)$ in the form $403x + 286y$ for integers x and y, where specifically $x = 5$ and $y = -7$.

Bézout's identity

The method we just saw can be generalised for any pair of integers.

Theorem. (Bézout's identity)
Given any integers a and b, there exist integers x and y such that

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

Values for x and y can be found by applying the Euclidean algorithm to a and b and then working backwards, like in the previous example.

Note that the solution pair (x, y) is not unique. For example, we saw $\gcd(403, 286) = 13 = 5 \times 403 + (-7) \times 286$, but it is also true that $\gcd(403, 286) = 13 = (-17) \times 403 + 24 \times 286$.

Notice that Bézout's identity cannot be used in reverse. However, the following weaker statement is true.

Theorem. Given $d = ax + by$ for some integers a, b, x, y, we have that

$$\gcd(a, b) \mid d.$$

Proof.

Example – Bézout's identity

Example. Find integers x and y such that $\gcd(283, 193) = 283x + 193y$.

Solution.

Solving linear equations for integers

Theorem. Given integers a, b, and c, there exist integers x and y such that $ax + by = c$ if and only if $\gcd(a, b) \mid c$.

Proof. First suppose $ax + by = c$ for some integers x and y. Since $\gcd(a, b)$ is a divisor of both a and b, we must have that $\gcd(a, b) \mid (ax + by)$ for all integers x, y. So $\gcd(a, b) \mid c$.

Next suppose $\gcd(a, b) \mid c$. Then $c = \gcd(a, b)k$ for some integer k. By Bézout's identity, we know there exist integers x' and y' such that $\gcd(a, b) = ax' + by'$. Multiplying through by k then gives $c = a(kx') + b(ky')$ where $x = kx'$ and $y = ky'$ are integers.

Corollary. Suppose we are given integers a, b, and c, and wish to solve $ax + by = c$ for integers x and y.

- If $\gcd(a, b) \nmid c$, then there are no integer solutions.
- If $\gcd(a, b) \mid c$, then we can find integer solutions as follows:
  - Find integers x' and y' satisfying $ax' + by' = \gcd(a, b)$ by applying the Euclidean algorithm to a and b and working backwards.
  - Writing $d = \gcd(a, b)$, we have that $x = \frac{c}{d}x'$ and $y = \frac{c}{d}y'$ are integer solutions to $ax + by = c$.

Example – Solving linear equations for integers

Example. Find integers x and y such that $289x + 119y = 13$.

Solution.

Solution.

Using Bézout's identity in proofs

When proving statements involving GCDs, it can often be useful to use Bézout's identity. That is, if we are given that $\gcd(a, b) = c$, then we can use the fact that $c = ax + by$ for some $x, y \in \mathbb{Z}$.

For example, consider the following applications:

Theorem. Suppose a, b, and c are integers with $a \mid bc$ and $\gcd(a, b) = 1$. Then $a \mid c$.

Proof.

Exercise. Suppose a and b are integers and p is a prime number. Prove that if $p \mid ab$, then $p \mid a$ or $p \mid b$.

Proof. (See Problem Set 3, Question 28.)

This property of prime numbers is actually the way prime elements are generally defined.