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?

  Here $q = 4$ and $r = 2$, since $30 = 4 \times 7 + 2$ and $0 \leq 2 < 7$.

- 30 is divided by 6?

  Here $q = 5$ and $r = 0$, since $30 = 5 \times 6 + 0$ and $0 \leq 0 < 6$.

- 30 is divided by -4?

  Here $q = -7$ and $r = 2$, since $30 = (-7) \times (-4) + 2$ and $0 \leq 2 < |-4|$.

- -30 is divided by 4?

  Here $q = -8$ and $r = 2$, since $-30 = (-8) \times 4 + 2$ and $0 \leq 2 < 4$.

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:

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

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. We have

$$403 = 1 \times 286 + 117,$$
$$286 = 2 \times 117 + 52,$$
$$117 = 2 \times 52 + 13,$$
$$52 = 4 \times 13 + 0.$$

So $\gcd(403, 286) = 13$.

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

Solution. We have

$$283 = 1 \times 193 + 90,$$
$$193 = 2 \times 90 + 13,$$
$$90 = 6 \times 13 + 12,$$
$$13 = 1 \times 12 + 1,$$
$$12 = 12 \times 1 + 0.$$

So $\gcd(283, 193) = 1$. (That is, 283 and 193 are coprime.)

The Euclidean algorithm – proof

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

Proof. To prove this is true, we need to show that the process always terminates, and always returns the GCD.

As a reminder, the first few steps of the Euclidean algorithm for a and b are:

$$a = q_0 \times b + r_0 \qquad \text{where } q_0, r_0 \in \mathbb{N} \text{ and } |b| > r_0 \geq 0,$$
$$b = q_1 \times r_0 + r_1 \qquad \text{where } q_1, r_1 \in \mathbb{N} \text{ and } r_0 > r_1 \geq 0,$$
$$r_0 = q_2 \times r_1 + r_2 \qquad \text{where } q_2, r_2 \in \mathbb{N} \text{ and } r_1 > r_2 \geq 0 \dots$$

Notice that the process must eventually terminate, since we have $|b| > r_0 > r_1 > \cdots \geq 0$, so the remainders are strictly decreasing, and must eventually reach zero after at most $|b|$ steps.

Notice also that $\gcd(a, b) = \gcd(b, r_0)$, by Property 6 from Lecture 2.01. Similarly, $\gcd(b, r_0) = \gcd(r_0, r_1)$, and so on. So in particular, if the algorithm terminates after n steps (so the remainder $r_{n+1} = 0$), we have that $\gcd(a, b) = \gcd(b, r_0) = \gcd(r_0, r_1) = \cdots = \gcd(r_{n-1}, r_n) = \gcd(r_n, 0)$. Recall also that $\gcd(r_n, 0) = r_n$, so the output of the Euclidean algorithm really is $\gcd(a, b)$.

Euclidean algorithm in reverse

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

$$403 = 1 \times 286 + 117, \qquad \text{①}$$
$$286 = 2 \times 117 + 52, \qquad \text{②}$$
$$117 = 2 \times 52 + 13, \qquad \text{③}$$
$$52 = 4 \times 13 + 0.$$

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. By definition, $\gcd(a, b) \mid a$ and $\gcd(a, b) \mid b$. So $\gcd(a, b)$ must be a divisor of any integer linear combination of a and b, by a previous result about divisibility.

Example – Bézout's identity

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

Solution. The Euclidean algorithm applied to 283 and 193 gives:

$$283 = 1 \times 193 + 90,$$
$$193 = 2 \times 90 + 13,$$
$$90 = 6 \times 13 + 12,$$
$$13 = 1 \times 12 + 1,$$
$$12 = 12 \times 1 + 0.$$

Working backwards from the penultimate line, we get:

$$1 = 13 - 12$$
$$= 13 - (90 - 6 \times 13)$$
$$= 7 \times 13 - 90$$
$$= 7 \times (193 - 2 \times 90) - 90$$
$$= 7 \times 193 - 15 \times 90$$
$$= 7 \times 193 - 15 \times (283 - 193)$$
$$= 22 \times 193 - 15 \times 283.$$

So $\gcd(283, 193) = 1 = 22 \times 193 - 15 \times 283$, that is, $x = -15$ and $y = 22$.

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. The Euclidean algorithm applied to 289 and 119 gives:

$$289 = 2 \times 119 + 51,$$
$$119 = 2 \times 51 + 17,$$
$$51 = 3 \times 17 + 0.$$

So $\gcd(289, 119) = 17$, which does not divide 13. Thus there are no integer solutions to $289x + 119y = 13$.

Example. Find integers x and y such that $289x + 119y = 34$.

Solution. In this case, $\gcd(289, 119) = 17$ is a divisor of 34, so there do exist integer solutions.

Working backwards from the penultimate line of the Euclidean algorithm:

$$17 = 119 - 2 \times 51$$
$$= 119 - 2(289 - 2 \times 119)$$
$$= 5 \times 119 - 2 \times 289.$$

So an integer solution to $17 = 289x' + 119y'$ is $x' = -2$ and $y' = 5$.

Thus an integer solution to $34 = 289x + 119y$ is $x = -4$ and $y = 10$.

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. Since $a \mid bc$, we may write $bc = ak$ for some integer k.
Since $\gcd(a, b) = 1$, by Bézout's identity there exist integers x and y such that $1 = ax + by$. Multiplying this through by c gives

$$c = acx + bcy = acx + aky = a(cx + ky).$$

Since $ck + ky$ is an integer, we can conclude that $a \mid c$.

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.