Euclidean Algorithm and Bézout's Identity

Pranav Konda

September 13, 2020

§1 Euclidean Algorithm

Recall that the **division algorithm** states that for every pair of integers a and b, there exists a distinct integer quotient and remainder, q and r, such that

$$a = bq + r \text{ for } 0 \leq r < b.$$

Using this, we can arrive at the main subject of this handout, the **Euclidean Algorithm**.

Theorem 1.1 (Euclid)
For natural numbers a and b, and their quotient and remainder q and r (obtained from the division algorithm) such that $a = bq + r$, we have $\gcd(a, b) = \gcd(b, r)$.

Proof. We claim that the set of common divisors between a and b is the same as those between b and r.

Let d be a common divisor of a and b. Since d divides both a and b, it must also divide all linear combinations of a and b, so $d|a - bq = r$. Thus d is also a common divisor of b and r.

Now assume d is a common divisor of b and r. Then d must divide all linear combinations of b and r, and it follows that $d|bq + r = a$. Thus d is a common divisor of a and b as well.

Since the sets of common divisors of a and b are equivalent, their greatest elements must be equivalent as well, so $\gcd(a, b) = \gcd(b, r)$. □

An immediate corollary of Theorem 1.1 is the Euclidean Algorithm, which provides a quick way to calculate the greatest common divisor of 2 numbers.

Corollary (Euclidean Algorithm)
For two natural numbers a and b, where $a > b$, repeated use of the division algorithm yields

$$\begin{aligned} a &= bq_1 + r \\ b &= r_1 q_2 + r_2 \\ r_1 &= r_2 q_3 + r_3 \\ &\cdots \\ r_{n-2} &= r_{n-1} q_n + r_n \\ r_{n-1} &= r_n q_{n+1}. \end{aligned}$$

Then it follows that $\gcd(a, b) = \gcd(b, r_1) = \cdots = \gcd(r_{n-1}, r_n) = r_n$.

The division algorithm, and by extension the euclidean algorithm also hold for the set of all polynomials with rational coefficients, where a, b, q, and r would be polynomials.

Example 1.2 (1986 AIME/5): What is the largest positive integer n such that $n^3 + 100$ is divisible ny $n + 10$?

Answer. Note that $n^3 + 100$ can be expressed as $(n+10)(n^2 + an + b) + c = n^3 + (10+a)n^2 + (10a + b)n + 10b + c$ for $a, b, c \in \mathbb{R}$. Equating the coefficients yields the following system:

$$\begin{cases} 0 = a + 10 \\ 0 = 10a + b \\ 100 = 10b + c \end{cases}$$

which yields $a = -10$, $b = 100$, and $c = -900$. By the Euclidean Algorithm we have

$$\gcd(n^3 + 100, n + 10) = \gcd(-900, n + 10) = \gcd(900, n + 10),$$

which has a maxiumum value for n when $\boxed{n = 890}$.

Let's look at another example, this time from the first IMO.

Example 1.3 (1959 IMO/1): Prove that the fraction $\dfrac{21n+4}{14n+3}$ is irreducible for every natural number n.

Proof. We can apply the Euclidean Algorithm as follows:

$$\gcd(21n + 4, 14n + 3) = \gcd(7n + 1, 14n + 3) = \gcd(7n + 1, 1) = 1.$$

Since the greatest common divisor of $21n + 4$ and $14n + 3$ is 1 for all n, it follows that $\dfrac{21n+4}{14n+3}$ is irreducible. □

§2 Bézout's Identity

One application of the Euclidean Algorithm is **Bézout's Identity**.

Theorem 2.1 (Bézout's Identity)
For any natural numbers a and b, there exist $x, y \in \mathbb{Z}$ such that $ax + by = \gcd(a, b)$.

Proof. We can apply the Euclidean Algorithm backwards:

$$\begin{aligned} \gcd(a, b) &= r_{n-2} - r_{n-1}q_n \\ &= r_{n_2} - (r_{n-3} - r_{n-2}q_{n-1})q_n = r_{n-2}(1 + q_n q_{n-1}) - r_{n-3}q_n \\ &= \cdots \\ &= ax + by. \end{aligned}$$

□

Example 2.2: Find x, y such that $110x + 380y = 3$.

Answer. Applying the Euclidean Algorithm, we obtain

$$\begin{aligned} 380 &= 110 \times 3 + 50 \\ 110 &= 50 \times 2 + 10 \\ 50 &= 10 \times 5. \end{aligned}$$

Now, we do it backwards, to obtain

$$\begin{aligned}10 &= 110 - 50 \times 2 \\ &= 110 - (380 - 110 \times 3) \times 2 \\ &= 7 \times 110 - 2 \times 380.\end{aligned}$$

Then we have $(x, y) = (7, -2)$.

Let's prove **Euclid's Lemma** using Bézout's Identity.

Example 2.3 (Euclid's Lemma): Prove that if $a|bc$ and $\gcd(a, b) = 1$, then $a|c$.

Proof. By Bézout's Identity, there exist some x and y such that

$$ax + by = 1.$$

Mutiplying this by c yields $c(ax) + c(by) = c$, and since $a|ac$ and $b|bc$, we have $a|c(ax) + c(by) = c$. □

Let's look at another example.

Example 2.4 (Putnam 2000): Prove that the expression

$$\frac{\gcd(m, n)}{n}\binom{n}{m}$$

is an integer for all (n, m) such that $n \geq m \geq 1$.

Proof. By Bézout's Identity, we have a and b such that $\gcd(m, n) = am + bn$. Substitution into the expression yields

$$\frac{am + bn}{n}\binom{n}{m} = \frac{am}{n}\binom{n}{m} + b\binom{n}{m}.$$

Note that

$$\frac{am}{n}\binom{n}{m} = \frac{am}{n}\left(\frac{n!}{m!(n-m)!}\right) = a\left(\frac{(n-1)!}{(m-1)!(n-m)!}\right) = a\binom{n-1}{m-1}.$$

Thus

$$\gcd(m, n)n\binom{m}{n} = a\binom{m-1}{n-1} + b\binom{m}{n}$$

is an integer for all integral $n \geq m \geq 1$. □

We can also extend Bézout's Identity to any number of variables.

Theorem 2.5 (General Form of Bézout's Identity)
For any integers $a_1, a_2, \cdots, a_n$, there exist integers $x_1, x_2, \cdots, x_n$ such that

$$\sum_{i=1}^{n} a_i x_i = \gcd(a_1, a_2, \cdots, a_n).$$

Just like before, Bézout's Identity works in the set of all polynomials with rational coefficients as well.

§3 Sources

1. AoPS (https://artofproblemsolving.com)
2. Justin Steven's Olympiad Number Theory Through Challenging Problems (https://s3.amazonaws.com/aops-cdn.artofproblemsolving.com/resources/articles/olympiad-number-theory.pdf)