NTL2 – Bezout's Identity, Fundamental Theorem of Arithmetic

Theorem 3.1 (Bezout's Identity)

For natural numbers a, b, there exist $x, y \in \mathbb{Z}$ such that $ax + by = gcd\ (a, b)$.

Proof: Run the Euclidean Theorem backwards.

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

Example 1.

(a) Express 5 as a linear combination of 45 and 65.

(b) Express 10 as a linear combination of 110 and 380.

Example 2. Suppose you have a 5-liter jug and a 7-liter jug. We can perform any of the following moves:

Fill a jug completely with water

Transfer water from one jug to another, stopping if the other jug is filled.

Empty a jug of water.

The goal is to end up with one jug having exactly 1 liter of water. How do we do this?

Theorem 3.2 (General Bezout's Identity)

For integers $a_1, a_2, \ldots, a_n$, there exist $x_1, x_2, \ldots, x_n \in \mathbb{Z}$ such that

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n = \sum_{i=1}^{n} a_ix_i = gcd\ (a_1, a_2, \ldots, a_n)$$

Proof: Using Induction, moving from 2 to 3 variables.

Note. Bezout's Identity for polynomials works the same exact way as it does for integers.

Assume $f(x), g(x) \in \mathbb{Z}[x]$, then using Euclid's Algorithm, we can find $u(x), v(x) \in \mathbb{Q}[x]$ such that

$$f(x)u(x) + g(x)v(x) = \gcd\big(f(x), g(x)\big).$$

Example 3. Find polynomials $u, v \in \mathbb{Q}[x]$ such that

$$(x^4 - 1)u(x) + (x^7 - 1)v(x) = x - 1.$$

Theorem 3.3 (Euclid's Lemma)

If $a|bc$ and $gcd(a,b) = 1$, then $a|c$.

Theorem 4.1 (Fundamental Theorem of Arithmetic)

Every integer $n \geq 2$ has a unique prime factorization.

$$n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$$

where $p_1, \dots, p_k$ are distinct primes and $\alpha_1, \dots, \alpha_k$ are positive integers.

Proof: There are two parts, existence and uniqueness and both parts can be proved by induction.

Existence: to prove every integer $n \geq 2$ has a prime factorization.

Theorem 4.2 (GCD and LCM)

Let the prime factorizations of two integers a, b be

$$a = p_1^{e_1} p_2^{e_2} \dots p_k^{e_k} = \prod_{i=1}^{k} p_i^{e_i} = \prod p_k^{e_k}$$

$$b = p_1^{f_1} p_2^{f_2} \dots p_k^{f_k} = \prod_{i=1}^{k} p_i^{f_i} = \prod p_k^{f_k}$$

The exponents above can be zero and the $p_i's$ are distinct. Then,

$$gcd(a,b) = p_1^{min\,(e_1,f_1)} p_2^{min\,(e_2,f_2)} \dots p_k^{\min(e_k,f_k)}$$

$$lcm[a,b] = p_1^{max\,(e_1,f_1)} p_2^{max(e_2,f_2)} \dots p_k^{max\,(e_k,f_k)}$$

Corollary 4.1

For $a, b \in \mathbb{Z}^+, gcd(a,b)\, lcm[a,b] = ab$.

Example 4. (Canada 1970) Given the polynomial

$$f(x) = x^n + a_1 x^{n-1} + a_2 x^{n-2} + \cdots + a_{n-1} x + a_n$$

With integer coefficients $a_1, a_2, \dots, a_n$ and given also that there exist four distinct integers a, b, c and d such that

$$f(a) = f(b) = f(c) = f(d) = 5,$$

Show that there is no integer k such that $f(k) = 8$.

Example 5. Let a, b, c be positive integers. If $\gcd(a,b,c)\, lcm[a,b,c] = abc$, prove that $\gcd(a,b) = \gcd(b,c) = \gcd(c,a) = 1$.

Theorem 4.3 (Four Number Lemma)

Let a, b, c and d be positive integers such that $ab = cd$. There exist positive integers p, q, r, s such that

$$a = pq, b = rs, c = ps, d = qr.$$

Example 6. Prove that if $ab = cd$, then $a + b + c + d$ is not a prime number.

Example 7. (USAMO 1972) Let a, b and c be integers. Prove that

$$\frac{(lcm[a,b,c])^2}{lcm[a,b] \cdot lcm[b,c] \cdot lcm[c,a]} = \frac{(\gcd(a,b,c))^2}{\gcd(a,b) \cdot \gcd(b,c) \cdot \gcd(c,a)}$$