NTL1 – Euclidean and Division Algorithm

Number theory is basically the study of integers.

Basic Ideas

- An odd number is of the form $2k + 1$, for some integer k.
- An even number is of the form 2m, for some integer m.
- The sum of two odd numbers is an even number.
- The sum of two even numbers is an even number.
- The sum of an odd and even number is an odd number.
- The product of two odd numbers is an odd number.
- A product of integers is even if and only if at least one of its factors is even.

Example 1. Let n be an integer greater than 1. Prove that

(a) 2^n is the sum of two odd consecutive integers.

(b) 3^n is the sum of three consecutive integers.

Theorem 1.1 (Divisibility Rules)

Let x, y, z be integers.

- $x|x.$
- $1|x \text{ and } x|0.$
- $x|y, y|z, \text{ then } x|z.$
- **If $\boldsymbol{z|x, y}$, then $\boldsymbol{z|ax + by}$ for any integers a, b** *(possibly negative).*
- **If $\boldsymbol{x|y}$, then either $\boldsymbol{y = 0}$, or $\boldsymbol{|x| \leq |y|}$.**
- *If $x|y$, and $y|x$, then $x = \pm y$, i.e., $|x| = |y|$.*
- *$x|y$ if and only if $xz|yz$ for some non-zero integer z.*
- *$x|y$ then $x|yz$ for any z.*

Note. For instance, if $n|2n + 1, then\ n|1$ which implies $n = \pm 1$. In general, in divisibility relations like these clever expressions are added/subtracted/multiplied to reduce the right side to something more manageable.

Theorem 1.2 (Two Useful Factorization Formulae)

If n is a positive integer, then

$$x^n - y^n = (x - y)(x^{n-1} + x^{n-2}y + \cdots + xy^{n-2} + y^{n-1})$$

If n is a positive odd number, then

$$x^n + y^n = (x + y)(x^{n-1} - x^{n-2}y + \cdots - xy^{n-2} + y^{n-1})$$

Well-Ordering Axiom

Every non-empty subset of the natural numbers has a least element.

Example 2. Prove that there is no integer in the interval (0, 1).

Theorem 2.1 (Division Algorithm)

For every integer pair a, b, there exists distinct integer quotient and remainders, q and r, that satisfy

$$a = bq + r, 0 \leq r < b$$

Example 3. Prove the division algorithm.

(There are two parts in the proof: existence and uniqueness.

Existence: to prove for every pair (a, b), there is a corresponding quotient & remainder

Uniqueness: to prove this quotient and remainder pair are unique.)

Theorem 2.2 (Euclid)

For natural numbers a, b, we use division algorithm to determine a quotient and remainder q, r, such that $a = bq + r$. Then $gcd(a, b) = gcd(b, r)$.

Corollary 2.1 (Euclidean Algorithm)

For two natural numbers $a, b, a > b$, to find $gcd(a, b)$, we use division algorithm repeatedly

$$a = bq_1 + r_1$$
$$b = r_1 q_2 + r_2$$
$$r_1 = r_2 q_3 + r_3$$
$$\ldots$$
$$r_{n-2} = r_{n-1} q_n + r_n$$
$$r_{n-1} = r_n q_{n+1}$$

We have $gcd(a, b) = gcd(b, r_1) = gcd(r_1, r_2) = \cdots = gcd(r_{n-1}, r_n) = r_n$

Example 4. Find gcd(110,490).

Theorem 2.3

For two polynomials, $a(x), b(x) \in \mathbb{Q}[x]$, *there exists a unique quotient and remainder polynomial,* $q(x)$ *and* $r(x)$ *such that*

$$a(x) = b(x)q(x) + r(x), deg(r) < deg(b) \text{ or } r(x) = 0.$$

Note. $\mathbb{Q}[x]$ is the set of polynomials with rational coefficients, and $\mathbb{R}[x]$ is the set of polynomials with real coefficients.

Theorem 2.4

If $a(x) = b(x)q(x) + r(x)$ *with* $deg(r(x)) < deg(b(x))$, *then*

$$gcd\big(a(x), b(x)\big) = gcd\ (b(x), r(x))$$

Note: By convention, the greatest common divisor of two polynomials is chosen to be the **monic** polynomial of highest degree that divides both polynomials. The word **monic** means that the leading coefficient is 1.

Theorem 2.5

For natural numbers, $a, m, n, gcd(a^m - 1, a^n - 1) = a^{gcd(m,n)} - 1$

Example 5. Find the greatest common divisor of $x^4 + x^3 - 4x^2 + x + 5$ and $x^3 + x^2 - 9x - 9$.

Example 6. What is the sum of all integers n such that $n^2 + 2n + 2$ divides $n^3 + 4n^2 + 4n - 14$?

Example 7. (AIME 1985) The numbers in the sequence 101, 104, 109, 116, … are of the form $a_n = 100 + n^2$, where $n = 1,2,3, \ldots$. For each n, let d_n be the greatest common divisor of a_n and a_{n+1}. Find the maximum value of d_n as n ranges through the positive integers.