Chapter 4

Number Theory

Reference Book:

- Concrete Mathematics – Graham, Knuth, Patashnik

Topics:

- Divisibility
- Primes
- Prime Examples
- Factorial Factors
- Relative Primality
- ‘mod’: The Congruence Relation

Number Theory

What is Number Theory?

Number theory is the branch of mathematics that explores the integers and their properties.

Learning Outcome: Students will be able to:

- effectively express the concepts and results of Number Theory.
- construct mathematical proofs of statements and find counterexamples to false statements in Number Theory.
- collect and use numerical data to form conjectures about the integers.
- understand the logic and methods behind the major proofs in Number Theory.
- work effectively as part of a group to solve challenging problems in Number Theory.

Divisibility

❖We say that m divides n (or n is divisible by m) if $m > 0$ and the ratio n/m is an integer. This property underlies all of number theory, so it's convenient to have a special notation for it. We therefore write

$$m \backslash n \iff m > 0 \text{ and } n = mk \text{ for some integer } k.$$

❖(The notation `m|n' is actually much more common than `m\n' in current mathematics literature. But vertical lines are over used | for absolute values, set delimiters, conditional probabilities, etc. and backward slashes are underused. Moreover, `m\n' gives an impression that m is the denominator of an implied ratio. So we shall boldly let our divisibility symbol lean leftward.)

If m does not divide n we write '$m \not\backslash n$'

GCD & LCM

The *greatest common divisor* of two integers m and n is the largest integer that divides them both:

$$\gcd(m,n) = \max\{ k \mid k\backslash m \quad \text{and} \quad k\backslash n \}$$

For example, $\gcd(12,18) = 6$.

Euclid's algorithm uses the recurrence

$$\gcd(0,n) = n ;$$

$$\gcd(m,n) = \gcd(n \bmod m,\ m)\,, \qquad \text{for } m > 0.$$

$$m'm + n'n = \gcd(m,n)$$

Another familiar notion is the *least common multiple*,

$$\operatorname{lcm}(m,n) = \min\{ k \mid k > 0, \quad m\backslash k \quad \text{and} \quad n\backslash k \}$$

Proof 1

$$k \backslash m \quad \text{and} \quad k \backslash n \qquad \iff \qquad k \backslash \gcd(m,n)\,.$$

(Proof: If k divides both m and n, it divides $m'm + n'n$, so it divides $\gcd(m,n)$. Conversely, if k divides $\gcd(m,n)$, it divides a divisor of m and a divisor of n, so it divides both m and n.)

❖Detail:

k\m means m=ka, where a is an integer
k\n means n=kb, where b is an integer

Now, gcd(m,n) = m'm+n'n (according to Euclid's) algorithm
= m' (ka) + n' (kb)
= k (m'a + n'b)
i.e. k \ gcd(m,n)

[Proved]

Primes

- A positive integer p is called prime if it has just two divisors, namely 1 and p.
- 1 isn't prime, so the sequence of primes starts out like this:

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, \ldots.$$

Proof 2

❖**Prove that, Any positive integer n can be written as a product of primes and it is unique.**

$$n = p_1 \ldots p_m = \prod_{k=1}^{m} p_k, \qquad p_1 \leqslant \cdots \leqslant p_m$$

❖**Part-I:: Product of Prime:**

❖ Basis: If m=0 then n=1 (because we consider this to be an empty product)

❖Induction: Such a factorization is always possible because if $n > 1$ is not prime it has a divisor n1 such that $1 < n1 < n$; thus we can write $n = n1 \cdot n2$. We know that by induction, n1 and n2 can be written as products of primes.

❖ Otherwise *n* is a prime number

Proof 2 (Contd)

❖ **Prove that, Any positive integer n can be written as a product of primes and it is unique.**

$$n = p_1 \dots p_m = \prod_{k=1}^{m} p_k , \qquad p_1 \leqslant \cdots \leqslant p_m$$

❖ **Part-II:: Product of Prime is unique**

❖ i.e. we shall prove there's only one way to write *n* as a product of primes in nondecreasing order.

❖ There is certainly only one possibility when n = 1, since the product must be empty in that case;

❖ so let's suppose that n > 1 and that all smaller numbers factor uniquely.

❖ Suppose we have two factorization — where the p's and q's are all prime.

❖ Nov $n = p_1 \dots p_m = q_1 \dots q_k , \qquad p_1 \leqslant \cdots \leqslant p_m \quad \text{and} \quad q_1 \leqslant \cdots \leqslant q_k ,$

❖ If not, we can assume that p1 < q1, making p1 smaller than all the q's.

❖ Then gcd (p1, q1) =1 and hence, ap1 + bq1 =1

❖ a.p1. (q2. q3. ... qk) + b.q1. (q2. q3. ... qk) = 1. (q2. q3. ... qk)

❖ a.p1. (q2. q3. ... qk) + b.n = 1. (q2. q3. ... qk)

❖ p1 divides L.H.S. , so it should also divide R.H.S. But (q2. q3. ... qk) < n

❖ But q2 ... qk < n, so it has a unique factorization (by induction). This contradiction shows that p1 must be equal to q1 after all. Therefore we can divide both of n's factorizations by p1, obtaining p2 ... pm = q2 ... qk < n. The other factors must likewise be equal (by induction), so our proof of uniqueness is complete.

Factorial Factors

See pdf given in your google classroom