4 Mon 10/5

Definition 5

$f : \mathbb{Z} \to \mathbb{Z}$ is said to be **multiplicative** if $f(mn) = f(m)f(n)$ whenever $\gcd(m, n) = 1$.

The remark above shows that φ is multiplicative.

5 Wed 10/7

A more interesting theorem about $\varphi(n)$:

Theorem 6

Let $N \geqslant 2$. We have

$$N = \sum_{d \geqslant 1 | N} \varphi(d).$$

In other words, N is the sum of $\varphi(d)$ for all divisors $d \mid N$.

Example 5.1

Take $N = 12$. We can partition $\{1, 2, \ldots, 12\}$ into sets of numbers coprime to 12, set of numbers with gcd = 2 with 12, with 3, with 4, with 6, and with 12. Then

$$\{1, 2, \ldots, 12\} = \{1, 5, 7, 11\} \sqcup \{2, 10\} \sqcup \{3, 9\} \sqcup \{4, 8\} \sqcup \{6\} \sqcup \{12\}$$

The first set has cardinality $\varphi(12)$, the second $\varphi(6)$, the third $\varphi(4)$, the other three $\varphi(3), \varphi(2), \varphi(1)$. (Think of the second set as the set of numbers of form $2n$ where $\gcd(n, 6) = 1$; 6 comes from 12/2.) Notice that we originally partitioned the set by different gcd's, and what we get are sets with cardinality $N/\gcd$.

6 Fri 10/9

Fundamental Theorem of Arithmetic, FTA

Each positive integer greater than 1 can be uniquely factorized.

Proof

First we show that each number can be prime factorized. Suppose not, then

$$S := \{x \in \mathbb{N} \mid x \geqslant 2 \text{ and } x \text{ does not have prime factors}\}$$

is not empty and thus have a least element m by the well-ordering axiom. Since m cannot be a prime, $m = ab$ for some composite numbers, but a and b can be written as product of primes. Hence m can be written as primes, contradiction. Now for the uniqueness:

2.5 The Fundamental Theorem of Arithmetic

Theorem 2.5.1 (Fundamental Theorem of Arithmetic, FTA)**.** Each positive integer greater than 1 can be uniquely factorized.

Proof. Suppose not, then there exists some positive integer x such that it can be prime factorized in at least two different ways:

$$x = \prod_{i=1}^{k} p_i \text{ and } x = \prod_{i=1}^{\ell} q_i \text{ where } p_i < p_{i+1}$$

WLOG, assume $k \leqslant \ell$. Since $p_1 \mid x$, there exists some q_m such that $p_1 \mid q_i$. However, to divide q_m, p_1 has to either equal to 1 or q_m, but any prime number is greater than 1. Therefore $p_1 = q_m$. Rearrange the indexes of the rest of q's so that they are now named $q_2, q_3, \cdots, q_j$. Similar to $p_1 = q_m$, there exists another q_n such that $p_2 = q_n$. Since $k \leqslant \ell$, each prime number in the p-prime factorization is equal to some prime number in the q-factorization. With proper rearrangement, we have shown that

$$\prod_{i=1}^{k} p_i = \prod_{i=1}^{k} q_i$$

11

Therefore,

$$\frac{x}{\prod_{i=1}^{k} p_i} = \frac{x}{\prod_{i=1}^{k} q_i} \implies 1 = \prod_{i=k+1}^{\ell} q_i$$

which is clearly impossible, given that each prime number is greater than 1. Therefore, the assumption that there exists a positive integer greater than 1 that can be prime factorized in more than one way is false, and we've proven the FTA. □

□

Example 6.1

Are there infinitely many primes 3 mod 4?. Yes. Suppose not, and suppose $\{p_1, \dots, p_n\}$ exhausts all primes 3 mod 4. Then

$$N = 2p_1p_2 \dots p_n + 1$$

is either $2 \cdot 1 + 1$ or $2 \cdot (-1) + 1$ mod 4, but both are 3. Notice that N is odd. Suppose it were the product of some primes then

$$N = q_1q_2 \dots q_n$$

and reducing both sides module 4 gives

$$3 = [q_1][q_2] \dots [q_n].$$

Notice that $[1]$ has no effect on the right hand side, so if N were a multiple of primes, there must be some q_i's that are 3 mod 4 because it's impossible to get $[3]$ out of a bunch of $[1]$'s. But we've shown that N is not a multiple of any prime of form $4k + 3$, contradiction.

Remark

There are also infinitely many primes of form $4k + 1$.

Dirichlet's Theorem

If a, b are positive coprime integers, then the sequence

$$(a, a + b, a + 2b, \dots)$$

has infinitely many primes.

Remark

By this theorem, the sequences $(3, 7, 11, \dots)$ and $(1, 5, 9, \dots)$ both contain infinitely many primes.