More Results About Prime Numbers
Class activity, Week 4

You saw the Sieve of Eratosthenes in the pre-class work. From the way the sieve works, the following proposition immediately follows:

Theorem 1: Every integer $n \geq 2$ is either a prime or can be written as a product of primes.

proof: We will use a proof by strong induction to prove this result.

(Show the first statement in induction is true.)

2 is prime

Now we assume the statement is true for all integers $\ell \geq 2$ up to k, i.e. that every ℓ is either a prime or a product of primes. We will show that $k+1$ is also a prime or a product of primes. If $k+1$ is prime, we are done. Suppose not, then $k+1$ has more than 2 distinct positive factors. Thus there exists 2 numbers $2 \leq a, b < k+1$ such that $ab = k+1$. By our assumption, a & b are either prime or can be written as a product of primes.

Hence, $k+1$ is a product of primes, and the statement is true for $k+1$.

This proves that every $n \geq 2$ is either a prime or a product of primes. □

The next natural question is whether the prime factorization is unique or not. This question was considered throughout history possibly starting with Euclid. The question was later investigated by Kamal al-Din al-Farisi, Jean Prestet, Euler, and Legendre. They used the prime factorization to find all the factors of an integer and stated the uniqueness of prime factorization without a proof. The proof had to wait until 1801 when Gauss published his proof in *Disquisitiones Arithmeticae.*

Theorem 2: (Fundamental Theorem of Arithmetic) Every integer $n \geq 2$ is either a prime or a product of primes, and the product is unique except for rearrangement of the factors.

proof: We proved existence in Theorem 1. To prove uniqueness, we use strong induction again.

For $n = 2$, uniqueness of prime factorization is clear.

Suppose uniqueness is true for all $\ell \leq k$ and we will show the uniqueness holds for $k+1$. Suppose

$$k+1 = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_t$$

are two prime factorizations of $k+1$. We will show that $r = t$ and that the primes q_j's are just a rearrangement of p_i's. Since the two prime factorizations are equal, we know that $p_1 | q_1 q_2 \cdots q_t$. By Euclid's Lemma, $p_1 | q_k$ for some k. But q_k is a prime, therefore, $p_1 = q_k$. Since we are not concerned with the order of the primes, we can reorder the q_j's if needed. Hence assume that $p_1 = q_1$.

Consider now $\ell = (k+1)/p_1 = (k+1)/q_1$. If $\ell = 1$, we are done. The two prime factorizations of $k+1$ are shown to be equal since $p_1 = q_1$. Otherwise, consider the two prime factorizations of ℓ:

$$\ell = p_2 p_3 \cdots p_r = q_2 q_3 \cdots q_t.$$

Since $\ell \leq (k+1)/2 < k$, we can apply the inductive assumption to conclude that $r = t$ and that the q_j's are just a rearrangement of p_i's.

Hence, by strong induction, the theorem is true for all $n \geq 2$. □

There is a very useful result that follows from the Fundamental Theorem of Arithmetic:

Theorem 3: Let $a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ with $\alpha_i > 0$ be the unique prime factorization of a and $b > 0$. Then $b|a$ if and only if $b = p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k}$ with $0 \leq \beta_i \leq \alpha_i$ for every i.

In other words, we know the form of a divisor of a given number once we know the prime factorization of that number.

GCD and LCM using prime factorization: Suppose a and b are two integers with $p_1, p_2, \ldots, p_k$ primes dividing either a or b. Then we can write a and b in terms of p_i's as follows:

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} \text{ and } b = p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k}$$

In this case, $\gcd(a, b)$ is the product of $p_i^{\min(\alpha_i, \beta_i)}$'s and $\text{lcm}(a, b)$ is the product of $p_i^{\max(\alpha_i, \beta_i)}$'s.

Even though prime factorization is not a computationally efficient process, for small numbers, finding the gcd and lcm using prime factorization works.

1. Justify these GCD and LCM formulas. (Hint: Use Theorem 3.)

$\gcd(a,b) = \prod p_i^{e_i} \mid a$ iff $0 \leq e_i \leq \alpha_i$ for every i. Similarly for b. Thus $e_i \leq \min(\alpha_i, \beta_i)$ for all i. If $e_i < \min(\alpha_i, \beta_i)$ for some i then swapping e_i for e_i+1 would create a larger product which divides both a & b. Thus $e_i \geq \min(\alpha_i, \beta_i)$ for all i. Thus $e_i = \min(\alpha_i, \beta_i)$ for all i.

$a \mid \text{lcm}(a,b) = \prod p_i^{e_i}$ iff $0 \leq \alpha_i \leq e_i$ for every i. similarly for b. By a similar argument $\max(\alpha_i, \beta_i) \leq e_i$ and $\max(\alpha_i, \beta_i) \geq e_i$. Thus $\max(\alpha_i, \beta_i) = e_i$ for all i.

Another result you considered in the pre-class work was the proof of infinitude of prime numbers. The proof we saw can be modified to prove that there are indeed infinitely many prime numbers of the form $4k + 3$.

2. We will use a proof by contradiction. Assume there are finitely many primes $p_1, p_2, \ldots, p_r$ of the form $4k + 3$, i.e. congruent to 3 mod 4. Consider now $n = 4p_1 p_2 \cdots p_r - 1$.

a. What is n congruent to mod 4? 3

b. Explain why none of p_i divides n.

$n \equiv -1 \equiv p_i - 1 \not\equiv 0 \mod p_i$

c. Explain why neither 2 nor 3 divides n.

n is odd

$p_1 = 3$

d. Explain why parts b and c then mean that all the prime factors of n are primes congruent to 1 mod 4, and why that leads to a contradiction.

No prime is $\equiv 0 \bmod 4$.
2 is the only prime $\equiv 2 \bmod 4$.
No primes $\equiv 3 \bmod 4$ divide n.
→ all prime factors of n are $\equiv 1 \bmod 4$

The product of #'s $\equiv 1 \bmod 4$ is $\equiv 1 \bmod 4$
but $n \equiv 3 \bmod 4$

One last result we should mention, which is an extremely useful tool in many calculations, is the Prime number Theorem, which tells us about how many primes do we expect less than a given number.

Theorem: (Prime Number Theorem) If $\pi(x)$ represents the number of primes less than x, then

$$\lim_{x \to \infty} \frac{\pi(x)}{x/\log(x)} = 1$$

In other words, the fraction of prime numbers less than x is about $\frac{1}{\log(x)}$[1]. There is an even more precise way to represent the ratio of $\pi(x)$ to x, with a specific error function. This theorem implies that even though there are infinitely many primes, they get less dense as numbers grow. We can see why this is the case from the way the Sieve of Eratosthenes operates and from Proposition 2 in the pre-class. But still primes are not too rare. Check out the `https://en.wikipedia.org/wiki/Prime_number_theorem` for more information.

[1] We use log in place of ln in most upper-level math writing.