MATH6222 week 6 lecture 17

Rui Qiu

2017-03-31

Definition: An integer $n > 2$ is **prime** if $d|n \implies d = 1$ or $d = n$. We say an integer is **composite** if not prime. Equivalently, n is composite if $\exists$ divisor $d|n$ with $1 < d < n$.

Lemma: Any integer $n > 1$ is a product of primes, i.e.

$$n = p_1 p_2 \cdots p_k$$

for some prime $p_1, p_2, \ldots, p_k$.

Proof: Prove this by strong induction on n.

Base Case $n = 2$. (2 is a product of 2, which is prime itself.)

Inductive Step: Given integer n, either n is prime or n is composite.

If n is prime, nothing to prove.

If n is composite, can write $n = n_1 n_2$ where $1 < n_1 < n, 1 < n_2 < n$.

By the induction hypothesis,

- $n_1 = p_1 p_2 \cdots p_k,\ p_i$ prime.
- $n_2 = q_1 q_2 \cdots q_l,\ q_j$ prime.

So $n = n_1 n_2 = p_1 \cdots p_k q_1 \cdots q_l$.

Fundamental Theorem of Arithmetic: Any integer $n > 2$ can be written uniquely as a product of primes.

Suppose $n = p_1 p_2 \cdots p_k$, and $n = q_1 q_2 \cdots q_l$. Then must have $k = l$, after reordering we have $p_1 = q_1, p_2 = q_2, \ldots$

Imagine a world with only even numbers. Define the "new prime" as numbers non-divisible by smaller even numbers, in this case 6 and 10 are primes, etc.

- Determine which numbers ≤ 40 are prime.
  $2, 6, 10, 14, 18, 22, 26, 30, 34, 38.$

- Determine prime factorizations for all integers ≤ 40.
  $2 = 2, 4 = 2 \times 2, 6 = 6, 8 = 2 \times 2 \times 2, 10 = 10, 12 = 2 \times 6, 14 = 14, 16 = 2 \times 2 \times 2 \times 2, 18 = 18, 20 = 2 \times 10, 22 = 22, 24 = 2 \times 2 \times 6, 26 = 26, 28 = 2 \times 14, 30 = 30, 32 = 2 \times 2 \times 2 \times 2 \times 2, 34 = 34, 36 = 2 \times 18 = 6 \times 6, 40 = 2 \times 2 \times 10.$

Then a problem emerges, 36 **has two "prime" factorizations!**

$$36 = 6 \times 6 = 2 \times 18$$

Two integers a and b are relatively prime if $\gcd(a, b) = 1$. (Example: $a = 6, b = 25, \gcd(a, b) = 1$.) Equivalently, $\exists\, m, n \in \mathbb{Z}$ such that $ma + nb = 1$.
(What is the relationship between this and prime factorization?)

Lemma: Let p be prime, let a be any integer, either $p|a$ or p and a are relatively prime.

Proof: Consider $\gcd(a, p)$. Must have

- $\gcd(a, p) = 1 \implies a$ and p are relatively prime.
- $\gcd(a, p) = p \implies p|a$.

Proposition (Key Property of Primes): p prime, a, b integers. If $p|ab$ then $p|a$ or $p|b$.

Proof: If $p|a$, nothing to prove. So assume $p \not| a$. So p and a are relatively prime.
By the Euclidean algorithm, $\exists\, m, n \in \mathbb{Z}$ such that $ma + np = 1$.
Let's multiple this by b:

$$mab + npb = b$$

p divides mab, and p divides npb automatically, so p divides b.

Corollary: If $p|(a_1 \cdots a_k)$, then $p|a_i$ for some i.
Proof by induction on k. $k = 2$ done. .... (skipped)

Proof of Fundamental Theorem of Arithmetic: By strong induction on $n = 2$. Suppose we have two prime factorizations of n:

- $n = p_1 p_2 \cdots p_k,\ p_i$ prime.
- $n = q_1 q_2 \cdots q_l,\ q_j$ prime.

So

$$p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_l$$

$p_1 | (q_1 \cdots q_l) \implies p_1 | q_i$ for some $i = 1, \ldots, l$.
Since q_i is prime, $p_1 = q_i$. After reordering, assume $p_1 = q_1$.
Now we have

$$p_2 \cdots p_k = q_2 \cdots q_l$$

Now by the induction hypothesis, after reordering, we have $p_2 = q_2, p_3 = q_3, \ldots p_k = q_l$

Corollary:

1. An integer $d|n \iff$ every prime factor d is a prime factor of n.
2. $\gcd(a, b)$ is just product of all primes occurring in both a and in b.

Proof: Suppose $d|n$, then $n = dk$, then $d = p_1 p_2 \cdots p_i, k = q_1 q_2 \cdots q_j$. ....