

Fundamental Theorem of Arithmetic

Discrete Mathematics
Evgeny Skvortsov

Previous Lecture

- Primes
- Greatest common divisor
- Euclidean algorithm

Greatest Common Divisor

● Theorem.

If a, b are integers and d is their greatest common divisor, then there are integers u, v such that $d = au + bv$.

● Proof.

We use the Euclidean algorithm and the notation $a = r_0, b = r_1, d = r_k$

We have

$$\begin{aligned}
 d = r_k &= r_{k-2} - r_{k-1}q_{k-1} \\
 &= r_{k-2} - (r_{k-3} - r_{k-2}q_{k-2})q_{k-1} \\
 &= (r_{k-4} - r_{k-3}q_{k-3}) - (r_{k-3} - (r_{k-4} - r_{k-3}q_{k-3})q_{k-2})q_{k-1} \\
 &\quad \vdots \\
 &= r_0u + r_1v = au + bv
 \end{aligned}$$

$$\begin{aligned}
 r_0 &= r_1q_1 + r_2 \\
 &\quad \vdots \\
 r_{k-3} &= r_{k-2}q_{k-2} + r_{k-1} \\
 r_{k-2} &= r_{k-1}q_{k-1} + r_k \\
 r_{k-1} &= r_kq_k
 \end{aligned}$$

Example

- Find $d = \gcd(821, 123)$ and integers u and v such that
$$d = 821u + 123v$$

More Primes

- Prime numbers have some very special properties with respect to division

- **Lemma.**

If a, b are integers and p is prime such that $p \mid ab$ then $p \mid a$ or $p \mid b$.

- **Proof.**

If $p \mid a$ then we are done. Suppose that it is not so.

Since p is prime, we have $\gcd(p, a) = 1$.

Therefore there are u and v such that $1 = au + pv$.

Then $b = p(bu) + (ab)v$. Since $p \mid p$ and $p \mid ab$, we have $p \mid b$.

- **Lemma.**

Let a_i be an integer for $1 \leq i \leq n$, and p is prime and

then a_i for some $1 \leq i \leq n$

$$p \mid a_i$$

$$p \mid a_1 a_2 \dots a_n$$

The Fundamental Theorem of Arithmetic

● Theorem.

Every integer $n > 1$ can be represented as a product of primes uniquely, up to the order of the primes.

● Proof.

● Existence

By contradiction. Suppose that there is an $n > 1$ that cannot be represented as a product of primes, and let m be the smallest such number.

m is not prime, therefore $m = st$ for some s and t

But then s and t can be written as products of primes, because $s < m$ and $t < m$.

Therefore m is a product of primes

The Fundamental Theorem of Arithmetic (cntd)

● Uniqueness

By strong induction: $P(n)$ denotes 'n has a unique prime factorization'

Basis step: $P(2)$ is obviously true

Inductive step: Suppose $P(m)$ is true for all $m < k$

Let $k = p_1^{s_1} p_2^{s_2} \dots p_u^{s_u}$ and $k = q_1^{t_1} q_2^{t_2} \dots q_v^{t_v}$, where $p_1 < p_2 < \dots < p_u$ and $q_1 < q_2 < \dots < q_v$ are primes

Since $p_1 \mid k$, we have $p_1 \mid q_1^{t_1} q_2^{t_2} \dots q_v^{t_v}$. By one of the previous lemmas, $p_1 \mid q_j$ for some $1 \leq j \leq v$.

As p_1 and q_j are prime, we have $p_1 = q_j$.

Actually, $j=1$, because $q_1 \mid k$ and, as q_1 is prime $q_1 \mid p_e$ hence $q_1 = p_e$ for some $1 \leq e \leq u$ and $p_1 < p_e = q_1 < q_j = p_1$

Set $k' = \frac{k}{p_1} = p_1^{s_1-1} p_2^{s_2} \dots p_u^{s_u} = q_1^{t_1-1} q_2^{t_2} \dots q_v^{t_v}$

By the inductive hypothesis, $u = v$, $p_j = q_j$ and $s_j = t_j$ for $1 \leq j \leq v$

Example

- Find the prime factorization of 980,220

Least Common Multiple

- A positive integer c is called a **common multiple** of integers a and b if $a \mid c$ and $b \mid c$
- The number c is called the **least common multiple** of a and b , denoted $\text{lcm}(a,b)$ if it is a common multiple and for any common multiple d we have $c \mid d$
- **Theorem.**
For any integers a and b , the least common multiple exists.
- **Proof.** Let S be the set of all common multiples of a and b . It is nonempty, therefore S has a least element c . We show that for any $d \in S$, $c \mid d$. Indeed, $c = ma$ and $d = na$. If $c \nmid d$ is not true, then $d = qc + r$, with $0 < r < c$. We have $na = q(ma) + r$. Therefore $r = a(n - mq) > 0$, and $r < c$ is a common multiple less than c . A contradiction.

Least Common Multiple (cntd)

● Find $\text{lcm}(231, 455)$.

● **Theorem**

For any integers a and b we have $ab = \text{lcm}(a, b) \cdot \text{gcd}(a, b)$

Relatively Prime

- Numbers a and b such that $\gcd(a,b) = 1$ are called **relatively prime**
- How many relatively prime numbers are there?
- **Euler's totient function** $\varphi(n)$ is the number of numbers k such that $0 < k < n$ and n and k are relatively prime.
- If p is prime then every $k < p$ is relatively prime with n . Hence, $\varphi(p) = p - 1$.
- **Lemma.**
If a and b are relatively prime then $\varphi(ab) = \varphi(a) \cdot \varphi(b)$
- **Corollary.**
If $n = p_1^{s_1} p_2^{s_2} \dots p_u^{s_u}$ is the prime factorization of n , then

$$\varphi(n) = \left(1 - \frac{1}{p_1}\right)^{s_1} \left(1 - \frac{1}{p_2}\right)^{s_2} \dots \left(1 - \frac{1}{p_u}\right)^{s_u}$$

Homework

Exercises from the Book:

No. 1ab, 4, 5, 10, 15 (page 237)

No. 1ab, 5, 7, 9 (page 241)