MATH453 Elementary Number Theory

Lecture 6: LCM and Dirichlet's Theorem

Lecturer: Bruce Berndt *Scribe: Kevin Gao*

6.1 Least Common Multiple

Definition 6.1 (Least Common Multiple)**.** Let $a, b \neq 0$. The ***least common multiple*** of a and b, denoted by $[a, b]$ or $\operatorname{lcm}(a, b)$, is the least $m > 0$ such that $a \mid m$ and $b \mid m$.

Example. What is $\operatorname{lcm}(2^3 3^2 7^5, 2 \cdot 3^5 7 \cdot 11^2)$?
We take the least common multiple of each factor, so we have $2^3 3^5 7^5 11^2$

If $\gcd(a, b) = 1$, $\operatorname{lcm}(a, b) = ab$. In general, we have the following theorem

Theorem 6.1. $\gcd(a, b) \cdot \operatorname{lcm}(a, b) = ab$

Proof. Assume $a, b > 1$. If either a or b is equal to 1, then the proof is trivial. Let

$$a = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n} \qquad b = p_1^{b_1} p_2^{b_2} \cdots p_n^{b_n}$$

so that $p_1, \ldots, p_n$ are the primes in common to a and b. Since $\gcd(a, b)$ is the greatest common **divisor**,

$$\gcd(a, b) = p_1^{\min(a_1, b_1)} p_2^{\min(a_2, b_2)} \cdots p_n^{\min(a_n, b_n)}$$

Also,

$$\operatorname{lcm}(a, b) = p_1^{\max(a_1, b_1)} p_2^{\max(a_2, b_2)} \cdots p_n^{\max(a_n, b_n)}$$

Multiply the two together and we get

$$\gcd(a, b) \cdot \operatorname{lcm}(a, b) = p_1^{a_1 + b_1} \cdots p_n^{a_n + b_n} = (p_1^{a_1} \cdots p_n^{a_n}) \cdot (p_1^{b_1} \cdots p_n^{b_n}) = ab$$

∎

In practice, we can use theorem to find the least common multiple once we find the greatest common divisor using the Euclidean algorithm.

6.2 Arithmetic Progression and Dirichlet's Theorem

Arithmetic progression is another name for the arithmetic sequence, a sequence of integers in which the difference between two consecutive numbers is constant. In general, the nth term in an arithmetic sequence/progression is given by

$$a_n = a_1 + (n - 1)d$$

How many primes are there in an infinite arithmetic progression? The theorem of Dirichlet tells us that indeed there are infinitely many primes in an infinite arithmetic progression.

Theorem 6.2 (Dirichlet's Theorem on Primes in Arithmetic Progression)**.** If $\gcd(a,b) = 1$ (a and b are **relatively prime**), then the set

$$\{an + b \mid n \in \mathbb{Z},\, n \geq 0\}$$

has **infinitely** many primes.

The proof of Dirichlet's theorem is beyond the scope of this course but will be covered in a course on analytic number theory. We can, however, prove some special cases of Dirichlet's theorem.

6.2.1 Special Cases of Dirichlet's Theorem

Lemma 6.3. Let $a, b \in \mathbb{Z}^+$. Suppose $a, b \in \{4n+1 \mid n \in \mathbb{Z},\, n \geq 0\}$. Then, $ab \in \{4n+1 \mid n \in \mathbb{Z},\, n \geq 0\}$.

Proof. Let $a = 4n_1 + 1$ and $b = 4n_2 + 1$. Then,

$$ab = (4n_1 + 1)(4n_2 + 1) = 16n_1n_2 + 4(n_1 + n_2) + 1$$

which can be factored as $4(4n_1n_2 + n_1 + n_2) + 1$. Take $n = (4n_1n_2 + n_1 + n_2)$ which is clearly a non-negative integer. Then, $n = ab \in \{4n + 1 \mid n \in \mathbb{Z},\, n \geq 0\}$. ∎

Using this simple fact, we can show that there are infinitely many primes of the form $4n + 1$.

Proposition 6.1. There exist infinitely many primes in $\{4n + 3 \mid n \in \mathbb{Z},\, n \geq 0\}$.

Proof. By contradiction.

Suppose for contradiction that there exist only finitely many primes in $\{4n + 3 \mid n \in \mathbb{Z},\, n \geq 0\}$. Say there exist only $r + 1$ such primes. Clearly, $p_0 = 3$, and we have $p_0, p_1, \ldots, p_r$ from the set that are primes.

Take $N = 4p_1p_2 \cdots p_r + 3$. By the Fundamental Theorem of Arithmetic, N has some prime divisor. We claim that N has some prime divisor $q_j \in \{4n + 3 \mid n \in \mathbb{Z},\, n \geq 0\}$. Further, we claim that if not, all prime divisors of N is of the form $4n + 1$. This is because we assumed that q_j is a prime divisor and the prime numbers ≥ 3 not of the form $4n + 3$ can be written as $4n + 1$ for some n. And if all prime divisors of N are of the form $4n + 1$, then N must also be of the form $4n + 1$ by Lemma 6.3, which is not true. Then, q_j is either 3 or one of $p_1, \ldots, p_r$.

If $q_j = 3$, $q_j \mid 3$ and $q_j \mid N$. It follows that $q_j \mid (N - 3)$ so $q_j \mid 4p_1 \cdots p_r$. This is a contradiction because $p_1, \ldots, p_r$ are primes not including 3. Hence, $q_j \neq 3$.

If $q_j \in \{p_1, \ldots, p_r\}$, then $q_j \mid 4p_1 \ldots p_r$. And by choice of q_j, $q_j \mid N$. It follows that $q_j \mid N - 4p_1 \cdots p_r$. This implies $q_j \mid 3$, which is a contradiction as well becuase $3 \notin \{p_1, \ldots, p_r\}$.

In both cases, we have a contradiction so the assumption that there are finitely many primes of the form $4n + 3$ must be false. ∎

Note that this proof will not work for the general case of Dirichlet's theorem because Lemma 6.3 does not hold in the general case.

Let's look another example of a similar special-case proof.

Lemma 6.4. Let $a, b \in \mathbb{Z}^+$. Suppose $a, b \in \{3n+1 \mid n \in \mathbb{Z},\, n \geq 0\}$. Then, $ab \in \{3n+1 \mid n \in \mathbb{Z},\, n \geq 0\}$.

Proof. Similar to the proof for Lemma 6.3. ■

> **Theorem 6.5.** There exist infinitely many primes of the form $3n + 2$ for $n \geq 0$.

Proof. Suppose for contradiction that there exist only finitely many primes of the form $3n + 2$. Say there are $r + 1$ such primes, namely, $2, p_1, \ldots, p_r$.

Similar to the proof for the previous theorem, we let

$$N = 3p_1 \cdots p_r + 2$$

We claim that there exsits a prime divisor of N of the form $3n + 2$. To see why this claim holds, assume that N has no such divisors. Then, there are two possibilities for the prime divisors of N. First, we have $3 \mid N$. This is also not possible because $3 \nmid 2$. This implies that $3n$ is not a prime divisor for N. The only remaining possiblity is that all prime divisors of N are of the form $3n + 1$.

However, by the previous lemma, we know that if all prime divisors of N are of the form $3n + 1$, then N itself must also be of the form $3n + 1$, which is not true. Hence, N must have some prime divisor of the form $3n + 2$. Now, consider the following two cases regarding the prime divisor q of N:

Case 1: $q = 2$. we have $2 \mid N$ and clearly $2 \mid 2$. It follows thata $2 \mid N - 2$, but this is a contradiction because $3p_1 \cdots p_r$ does not contain 2 as a factor. Therefore, $q = 2$ is not possible.

Case 2: $q \in \{p_1, \ldots, p_r\}$. $q \mid N$ and $q \mid 3p_1 \cdots p_r$. It follows that $q \mid 2$. But again, this is not possible becuase q and 2 are both primes.

In both cases, we have a contradiction. This implies that N itself is a prime that is not in $\{2, p_1, \ldots, p_r\}$. Hence, our initial assumption that there are finitely many primes of the form $3n + 2$ must be false, so the theorem holds. ■