Iowa City Math Circle Handouts

Ananth Shyamal, Divya Shyamal, and Reece Yang

August 12, 2018

3 Prime Numbers and Factorizations

3.1 Definitions and Basic Theorems

Let a and b be two natural numbers. If for some natural number k, $a = kb$, then we say that b divides a, or $b|a$, and that b is a *divisor* of a.

A *prime number* is a number that is only divisible by 1 and itself. 2, the only even prime, 3, 5, 7, and 11 are the first 5 prime numbers. The following propositions illustrate how useful primes can be in number theory.

Proposition 3.1: There are infinitely many primes.
Proof: The following proof was first proposed by Euclid.
First, let's assume that there exist only n primes for the sake of contradiction. Denote the primes by $p_1, p_2, \ldots, p_n$. Now consider the number $p_1 p_2 \cdot \cdots \cdot p_n + 1$. This number is not divisible by any of the existing primes, because when divided by them, there will always be a remainder of 1. Thus, $p_1 p_2 \cdots p_n + 1$ must be prime, which contradicts our assumption. Therefore there are an infinite number of primes.

Proposition 3.2: (Fundamental Theorem of Arithmetic) Every positive integer can be *uniquely* written as a product of nonnegative powers of primes. This decomposition of a number is called the number's *prime factorization.*

Proposition 3.3: Let n be a positive integer with factorization

$$n = p_1^{a_1} \cdot p_2^{a_2} \cdot \cdots \cdot p_k^{a_k}$$

Let d be a positive integer with prime factorization

$$d = p_1^{b_1} \cdot p_2^{b_2} \cdot \cdots \cdot p_j^{b_j}$$

Then $d|n$ iff $j \leq k$ and $b_i \leq a_i$ for all $1 \leq i \leq j$

Proposition 3.4: Let n be a positive integer with prime factorization

$$n = p_1^{e_1} \cdot p_2^{e_2} \cdot \cdots \cdot p_k^{e_k},$$

where the p_i's are distinct prime numbers and the e_i's are nonnegative integers. Then

1. The number of divisors of n is

$$(e_1 + 1)(e_2 + 1) \cdots (e_k + 1).$$

2. The sum of all the positive divisors of n is

$$\left(1 + p_1 + p_1^2 + \cdots + p_1^{e_1}\right)\left(1 + p_2 + p_2^2 + \cdots + p_2^{e_2}\right) \cdots \left(1 + p_k + p_k^2 + \cdots + p_k^{e_k}\right).$$

   We can simplify each multiplicand of this expression using the formula for the sum of a geometric sequence.

Example 3.1: Consider the number 315. Find its prime factorization, its number of divisors, and the sum of its divisors.
Solution: Notice that

$$315 = 5 \cdot 63 = 5 \cdot 7 \cdot 9 = 3^2 \cdot 5 \cdot 7,$$

so the prime factorization of 315 is $3^2 \cdot 5 \cdot 7$.
By the formula above, the number of divisors is

$$(2+1)(1+1)(1+1) = 12$$

and the sum of divisors is

$$\left(1+3+3^2\right)(1+5)(1+7) = 13 \cdot 6 \cdot 8 = 624.$$

The above proposition gives us a rather simple but useful fact: the number of divisors of a positive integer is odd if and only if the number is a perfect square.

All integers greater than 1 that are not prime are called *composite*. Moreover, a composite number is any positive integer with at least one divisor other than itself and 1. Notice that the number 1 is neither prime nor composite.
Two positive integers are said to be *relatively prime* (or *coprime*) if they share no common divisors other than 1. For example, the numbers 12 and 35 are coprime.

3.2 GCD and LCM

We use the notation $\gcd(a, b)$ to denote the greatest common divisor of a and b. Also, let $\text{lcm}(a, b)$ denote the least common multiple of a and b. Note that if a and b are relatively prime, then $\gcd(a, b) = 1$ and $\text{lcm}(a, b) = ab$. Additionally, if $b|a$ then $\text{lcm}(a, b) = a$.

Now, given the prime factorization of two numbers, how can we find their lcm and gcd? This next proposition answers this question.

Proposition 3.5: Let m and n be positive integers with prime factorizations

$$m = p_1^{a_1} \cdot p_2^{a_2} \cdot \cdots \cdot p_i^{a_i}$$

and

$$n = p_1^{b_1} \cdot p_2^{b_2} \cdot \cdots \cdot p_j^{b_j},$$

where p_k is the kth prime number, the a_k's and b_k's are nonnegative integers, and p_i and p_j are the largest prime divisors of m and n, respectively. Without loss of generality, let $i \geq j$. For all $k \in \{j+1, j+2, \ldots i\}$, let $b_k = 0$. Then

$$\text{lcm}(m, n) = p_1^{\max(a_1,b_1)} \cdot p_2^{\max(a_2,b_2)} \cdot \cdots \cdot p_i^{\max(a_i,b_i)}$$

and

$$\gcd(m, n) = p_1^{\min(a_1,b_1)} \cdot p_2^{\min(a_2,b_2)} \cdot \cdots \cdot p_j^{\min(a_j,b_j)}.$$

Example 3.2: Find $\gcd(630, 1500)$ and $\text{lcm}(630, 1500)$.
Solution: We first compute the prime factorizations of 630 and 1500 as

$$630 = 2 \cdot 3^2 \cdot 5 \cdot 7$$

and

$$1500 = 2^2 \cdot 3 \cdot 5^3.$$

Using these, we get

$$\begin{aligned} \text{lcm}(630, 1500) &= 2^{\max(1,2)} \cdot 3^{\max(2,1)} \cdot 5^{\max(1,3)} \cdot 7^{\max(1,0)} \\ &= 2^2 \cdot 3^2 \cdot 5^3 \cdot 7 \\ &= 31500 \end{aligned}$$

and

$$\begin{aligned} \gcd(630, 1500) &= 2^{\min(1,2)} \cdot 3^{\min(2,1)} \cdot 5^{\min(1,3)} \\ &= 2 \cdot 3 \cdot 5 \\ &= 30. \end{aligned}$$

The previous proposition gives rise to the following proposition, which can be very useful in number theory problems.

Proposition 3.6: For positive integers m and n,

$$m \cdot n = \gcd(m, n) \cdot \text{lcm}(m, n).$$

3.3 Euclidean Division Algorithm

We start of with a result that is behind the Euclidean division algorithm.

Proposition 3.7: Let m and n be positive integers with $m > n$ and let r be the remainder when m is divided by n. Then

$$\gcd(m, n) = \gcd(m - n, n) = \gcd(r, n).$$

The Euclidean algorithm repeatedly simplifies the expression $\gcd(m, n)$ using the above result. We use the following example to show the steps of the algorithm.

Example 3.3: Find $\gcd(1374, 141)$.
Solution: Applying *Proposition 3.7* multiple times, we get

$$\begin{aligned}
\gcd(1374, 141) &= \gcd(1374 \pmod{141}, 141) \\
&= \gcd(105, 141) \\
&= \gcd(36, 105) \\
&= \gcd(105 \pmod{36}, 36) \\
&= \gcd(33, 36) \\
&= \gcd(3, 33) \\
&= 3.
\end{aligned}$$

We will now demonstrate the Euclidean Division Algorithm more generally. Let a and b be integers with $a > b$. Then we may write:

$$\begin{aligned}
a &= bq_1 + r_1 \\
b &= r_1 q_2 + r_2 \\
r_1 &= r_2 q_3 + r_3 \\
&\vdots \\
r_{k-2} &= r_{k-1} q_k + r_k \\
r_{k-1} &= r_k q_{k+1} + r_{k+1}.
\end{aligned}$$

Since all r_n are nonnegative and $r_1 > r_2 > \cdots > r_{k+1}$, there must be some i such that $r_{i+1} = 0$. For this i, $\gcd(a, b) = r_i$.

3.4 Chicken McNugget Theorem

Let's start off with an example.

Example 3.4: Chicken McNuggets can be purchased in boxes of 5 and 12. Find the largest number of McNuggets that cannot be purchased?
Solution: To solve this problem, we need the help of the following theorem.

Proposition 3.8: (Chicken McNugget Theorem) Let m and n be *relatively prime* positive integers greater than one. Then

1. The greatest positive integer that cannot be written as a linear combination of m and n (i.e. a number of the form $p \cdot m + q \cdot n$, where p and q are nonnegative integers) is $mn - (m + n)$.

2. The number of positive integers that cannot be written as a linear combination of m and n is $\frac{(m-1)(n-1)}{2}$.

Thus, the answer to the above example is $5 \cdot 12 - (5 + 12) = 43$.

3.5 Exercises

Problem 1: (2013 AMC 8 Problem 10) What is the ratio of the least common multiple of 180 and 594 to the greatest common factor of 180 and 594?
(A) 110 **(B)** 165 **(C)** 330 **(D)** 625 **(E)** 660

Problem 2: (1959 IMO Problem 1) Prove that the fraction $\frac{21n+4}{14n+3}$ is irreducible for every natural number n.

Problem 3: (MathCounts) What is the smallest whole number that can be multiplied by 200 such that the product is a perfect cube?

Problem 4: (MathCounts) What is the sum of the three positive integers less than 1000 that have exactly five positive integer divisors.

Problem 5: (2005 AIME 1 Problem 3) How many positive integers have exactly three proper divisors (positive integral divisors excluding itself), each of which is less than 50?

Problem 6: (2016 AMC 10A Problem 22) For some positive integer n, the number $110n^3$ has 110 positive integer divisors, including 1 and the number $110n^3$. How many positive integer divisors does the number $81n^4$ have?
(A) 110 **(B)** 191 **(C)** 261 **(D)** 325 **(E)** 425

Problem 7: (1996 AHSME Problem 29) If n is a positive integer such that $2n$ has 28 positive divisors and $3n$ has 30 positive divisors, then how many positive divisors does $6n$ have?
(A) 32 **(B)** 34 **(C)** 35 **(D)** 36 **(E)** 38

Problem 8: (2004 AIME 2 Problem 8) How many positive integer divisors of 2004^{2004} are divisible by exactly 2004 positive integers?

Problem 9: (1983 AIME Problem 8) What is the largest 2-digit prime factor of the integer $\binom{200}{100}$?

Problem 10: (2018 AMC 10B Problem 23) How many ordered pairs (a, b) of positive integers satisfy the equation

$$a \cdot b + 63 = 20 \cdot \text{lcm}(a, b) + 12 \cdot \gcd(a, b).$$

(A) 0 **(B)** 2 **(C)** 4 **(D)** 6 **(E)** 8

Problem 11: (2016 AMC 10A Problem 25) How many ordered triples (x, y, z) of positive integers satisfy $\text{lcm}(x, y) = 72, \text{lcm}(x, z) = 600$ and $\text{lcm}(y, z) = 900$?
(A) 15 **(B)** 16 **(C)** 24 **(D)** 27 **(E)** 64

Problem 12: (1985 AIME Problem 13) The numbers in the sequence 101, 104, 109, 116,... are of the form $a_n = 100 + n^2$, where $n = 1, 2, 3, \ldots$ For each n, let d_n be the greatest common divisor of a_n and a_{n+1}. Find the maximum value of d_n as n ranges through the positive integers.