Introduction to Number Theory

1 What is Number Theory?

Number Theory is a branch of mathematics that explores the integers and their properties. This is a much different way to approach mathematics, as previously the problems many of you have experienced deal with real numbers, a more general case. Number theory uses its own special tools in order to restrict the set of solutions within the set of integers.

2 Basic Terminology

These are all things you should be familiar with from previous mathematics courses, but in the interest of being self-contained I will review them.

- It's sort of difficult to define integers in themselves, but in this case the Wikipedia definition suffices: "An **integer** is a number that can be written without a fractional or decimal component." Some examples of integers are 5, -17, and 3628800. It is important to know that while the set of integers is closed[1] under addition, subtraction, or multiplication, it is **NOT** under division!
- An integer a is said to be a **multiple** of another integer b if there exists an integer k such that $a = kb$. The integer b here is said to be called a **factor** or a **divisor**[2] of a. Furthermore, a is said to be **divisible** by b.

  If an integer has no positive divisors other than 1 and itself, it is said to be **prime**; otherwise, it is said to be **composite** (with the exception of 1, of course.)

3 Divisibility

Some of the simplest number theory problems ask you to manipulate divisibility rules in order to solve a question. In any case, don't be afraid to churn out a little bit of basic algebra and/or casework, as there may be multiple solutions to the problem.

Example 1. *What is the value of the digit X such that the three-digit number $\overline{3X4}$ is divisible by 9?*

Solution. The divisibility rule states that the sum of the digits of any number must be divisible by 9 in order for the original number to be divisible by 9. The value of X such that $7 + X$ is divisible by 9 must be $X = \boxed{2}$. ■

Example 2. *The four-digit positive integer $3BAA$ is divisible by 12. What is the sum of all possible values of $A + B$?*

Solution. It suffices to examine the divisibility rules for 3 and 4. In order for the integer to be divisible by 4, AA must also be divisible by 4, so $A = 4$ or $A = 8$. If $A = 4$, then the sum of the digits of the number is $11 + B$, and since this sum must be divisible by 3, $B = 1, 4, 7$ all work. Similarly, if $A = 8$, then the sum of the digits of the number is $19 + B$, and the values of B that make this sum divisible by 3 are $B = 2, 5, 8$. Hence the six ordered pairs $(A, B) = (4, 1), (4, 4), (4, 7), (8, 2), (8, 5), (8, 8)$ all work, and the sum of all possible values of $A + B$ is $\boxed{63}$. ■

4 Prime Factorization

Any integer N can be written as the product of the primes it is divisible by. The **prime factorization** of N is

$$N = \prod_{p \in \mathbb{P}} p^{e_i} = 2^{e_1} \cdot 3^{e_2} \cdot 5^{e_3} \cdot \ldots,$$

where $\mathbb{P}$ is the set of positive primes and $\{e_i\}$ is a sequence of integers determining how many times the ith prime number can be divided out of N. For example, $144 = 2^2 \cdot 3^2$ and $7! = 2^4 \cdot 3^2 \cdot 5 \cdot 7$.

Often times, the crux of a number theory problem is determining how to deal with its prime factorization, albeit indirectly.

[1] A set A is said to be **closed** under an operation if said operation takes members from the set to produce a member from that same set. For example, multiplying two integers produces another integer.

[2] While both of these terms are usually interchangable, usually the latter one is more often used.

Example 3. *What is the smallest positive integer that, when multiplied by* 60*, results in a perfect cube?*

Solution. As the title of this section suggests, we look at the prime factorization of 60, $2^2 \cdot 3 \cdot 5$. Note that in order for an integer to be a perfect cube, all of the exponents in its prime factorization must be multiples of 3. Therefore, in order to do that, we need to add one factor of 2, two factors of 3, and two factors of 5. Hence the requested number is $2 \cdot 3^2 \cdot 5^2 = \boxed{450}$. ■

5 GCD and LCM

The **greatest common divisor** of a set of integers A is the largest positive integer n that divides evenly into every element in A. For example, $\gcd(15, 20) = 5$ and $\gcd(12, 18) = 6$. Similarly, the **least common multiple** of a set of integers B is the smallest positive integer N such that N is evenly divisible by every integer in B. For example, $\text{lcm}(15, 20) = 60$ and $\text{lcm}(12, 18) = 36$.

There is a general expression for the greatest common divisor and least common multiple of two integers, and its roots lay within the idea of prime factorization:

Important: Let M and N be positive integers. Consider the set of primes $p_1, p_2, \ldots, p_k$ that divide either M or N. Let

$$M = p_1^{e_1} \cdot p_2^{e_2} \cdot \ldots \cdot p_k^{e_k}, \qquad N = p_1^{f_1} \cdot p_2^{f_2} \cdot \ldots \cdot p_k^{f_k}.$$

Then

$$\gcd(M, N) = p_1^{\min\{e_1, f_1\}} \cdot p_2^{\min\{e_2, f_2\}} \cdot \ldots \cdot p_k^{\min\{e_k, f_k\}}$$

and

$$\text{lcm}(M, N) = p_1^{\max\{e_1, f_1\}} \cdot p_2^{\max\{e_2, f_2\}} \cdot \ldots \cdot p_k^{\max\{e_k, f_k\}}.$$

This is easily justified by the definition of GCD and LCM; I leave it as an exercise to the interested individual.

Example 4. *What is the greatest common divisor of* 60 *and* 150*?*

Solution. It is easy to see that $60 = 2^2 \cdot 3 \cdot 5$ and $150 = 2 \cdot 3 \cdot 5^2$. In order for an integer to divide both 60 and 150, it must have at most one factor of 2, at most one factor of 3, and at most one factor of 5.[3] Therefore the largest possible integer that divides both 60 and 150 is $2 \cdot 3 \cdot 5 = \boxed{30}$. ■

Of course, this technical definition is not always necessary. Sometimes, it is important to simply understand what the definitions of gcd and lcm actually imply.

Example 5 (Math League HS 2000-2001)**.** *With each entry I submit, I have to write a different pair of positive integers whose greatest common factor is* 1 *and whose sum is* 2000*. (Pairs differing only in the order of addition are counted as* 1 *pair,* NOT *two different pairs.) For example, I submitted the pair* $(1, 1999)$ *with my first entry. With these restrictions, at most how many entries can one person submit?*

Solution. Instead of focusing on the pairs where the greatest common divisor is 1, we instead focus on the opposite set: those pairs in which the two integers share a common factor.[4] Note that by the definition of greatest common divisor, x and y are both divisible by $\gcd(x, y)$. Therefore, the sum of these integers must be divisible by $\gcd(x, y)$ as well. Since $2000 = 2^4 \cdot 5^3$, in order for $\gcd(x, y)$ to be greater than 1, x and y must be both divisible by either 2 or 5 (or both).

We now proceed to count the number of unordered pairs of integers (x, y) that satisfy the above condition. The pairs in which x and y are both divisible by 2 are $(2, 1998), (4, 1996), \ldots, (1000, 1000)$. (By symmetry, we only need to go up to $x = 1000$, due to the condition that the pair (x, y) is identical to the pair (y, x).) Similarly, the pairs in which x and y are both divisible by 5 are $(5, 1995), (10, 1990), \ldots, (1000, 1000)$. However, if x and y are divisible by both 2 and 5, then the pair (x, y) is counted in both lists, so we need to subtract those pairs once in order to not overcount![5] These pairs are $(10, 1990), (20, 1980), \ldots, (1000, 1000)$. By simple counting arguments, we can determine that there are 500, 200, and 100 pairs in the three lists respectively, for a total of $500 + 200 - 100 = 600$ unordered pairs that satisfy the condition. Therefore, since there are 1000 possible unordered pairs, I can submit at most $1000 - 600 = \boxed{400}$ entries in total. ■

[3] Try and see why this reasoning works and how it derives the boxed formula shown above!

[4] This technique is more broadly referred to as *complementary counting*, which will be discussed more in-depth in the lecture on counting and probabilty.

[5] This technique is called the *Principle of Inclusion-Exclusion*, another idea prevalent in combinatorics.

6 Practice Problems

1. What is the largest prime factor of 143 000 000?
2. Three positive integers are each greater than 1, have a product of 27000, and are pairwise relatively prime. What is their sum?
3. Let (a, b) denote the greatest common factor of a and b, and let $[a, b]$ denote the least common multiple of a and b. Evaluate the following expressions:
   (a) $(15, 20)$
   (b) $[66, 121]$
   (c) $(12^6, 18^4)$
   ★ (d) $(2143567, 2143369)$
4. The six-digit integer $\overline{12345X}$ is divisible by 11. What is the value of the digit X?
5. When 270 is divided by the odd number x, the quotient is a positive prime (and the remainder is 0). What is the value of x?
6. What is the smallest positive integer that is neither prime nor square and that has no prime factor less than 50?
7. What is the greatest possible sum of two multiples of 12, each less than 100, whose greatest common factor is 24?
8. A standard six-sided die is rolled, and P is the product of the five numbers that are visible. What is the largest number that is certain to divide P?
9. Which of the following numbers is a perfect square?
   (A) $\frac{14!15!}{2}$ **(B)** $\frac{15!16!}{2}$ **(C)** $\frac{16!17!}{2}$ **(D)** $\frac{17!18!}{2}$ **(E)** $\frac{18!19!}{2}$
10. A store sold 72 decks of cards for $\$a67.9b$. Find $a + b$.
11. A *monoprime* is a positive even number that isn't the product of two even numbers. An *irregular number* is an integer which can be written as a product of two (possibly equal) monoprimes in more than one way. What is the smallest irregular number?
12. The product of any two of the positive integers 30, 72, and N is divisible by the third. What is the smallest possible value of N?
13. The product of two positive integers is 9984, and the greatest common factor of these integers equals the difference between them. What are the two integers?
14. Find the largest natural number n below 50 such that
$$\text{LCM}(n, n+1, \ldots, 50) = \text{LCM}(1, 2, \ldots, 50),$$
where LCM stands for least common multiple.
15. For positive integers $n \geq 2$, define $g(n)$ to be one more than the largest proper divisor of n. Hence $g(35) = 8$, since the proper divisors of 35 are 1, 5, and 7. For how many n in the range $2 \leq n \leq 100$ do we have $g(g(n)) = 2$?

★ 16. Let $[r, s]$ denote the least common multiple of positive integers r and s. Find the number of ordered triples (a, b, c) of positive integers for which $[a, b] = 1000$, $[b, c] = 2000$, and $[c, a] = 2000$.

★ 17. Let x and y be positive integers such that $7x^5 = 11y^{13}$. The minimum possible value of x has a prime factorization $a^c b^d$. What is $a + b + c + d$?

★ 18. An infinite sequence of positive integers $\{a_n\}$ is such that for any two positive integers $i \neq j$,
$$\gcd\{a_i, a_j\} = \gcd\{i, j\}.$$
Show that $a_i = i$ for all i.