NASSAU COUNTY INTERSCHOLASTIC MATHEMATICS LEAGUE
ALL-STAR PROGRAM

$\forall^*$

Practice #2: Number Theory, Part I: Primes and Divisibility

The field of **number theory** is the area of mathematics concerned with the nature and properties of the integers.

Some terms and symbols used in number theory:

- $\mathbb{Z}$ represents the set of integers. Unless otherwise specified, for this paper, all variables will represent integers.
- We will use the symbol $\mathbb{Z}^+$ to stand for the set of positive integers, $\mathbb{Z}^-$ for the negatives.
- The term **nonnegative integer** refers to an element of the set $\mathbb{Z}^+ \cup \{0\}$. The term **nonpositive integer** is used similarly for an element of the set $\mathbb{Z}^- \cup \{0\}$.
- We say that:
  - b is a **multiple** of a,
  - a is a **divisor** of b,
  - a is a **factor** of b, or
  - a **divides** b $(a \mid b)$ if there exists an integer k such that $ak = b$.
- Note that 0 is a multiple of every integer, since for any integer a, $a \cdot 0 = 0$.
- A **prime** number is a number greater than or equal to 2 that has exactly two positive divisors, 1 and the number itself.
- A **composite** number is a number greater than or equal to 2 that has more than two positive divisors.
- The number 1 is called a **unit**, and is neither prime nor composite.
- The **greatest common factor** (or **greatest common divisor**) of a set of numbers is defined as follows: $gcf(a_1, a_2, ..., a_n)$ is the greatest positive integer g such that $g \mid a_k$ for all $k = 1, 2, ..., n$.
- The **least common multiple** is defined as: $lcm(a_1, a_2, ..., a_n)$ is the least positive integer m such that $a_k \mid m$ for all $k = 1, 2, ..., n$.
- Two numbers a and b are **relatively prime** if $gcf(a, b) = 1$. Note that 1 is relatively prime to all integers.

The **Euclidean Algorithm** can be used to find the GCF of two integers. For example, to find the GCF of 391 and 1139:

$$1139 = 391 \cdot 2 + 357$$
$$391 = 357 \cdot 1 + 34$$
$$357 = 34 \cdot 10 + 17$$
$$34 = 17 \cdot 2 + 0$$

The algorithm starts by dividing the larger number by the smaller and expressing the result with a remainder, as in the first line above. Then, repeat the process using the divisor and remainder of the first line as the dividend and divisor. Continue until you obtain a zero remainder. The final nonzero remainder (here, 17) is the GCF.

1. Prove that the final remainder in the Euclidean algorithm is a factor of both of the two original numbers.
2. Prove that any number which divides the two original numbers also divides the final remainder. This proves that the final remainder is the <u>greatest</u> common factor.

Now, given any two integers a and b, we can construct a **linear combination** $ax + by$ of those two numbers.

3. Show that any linear combination of a and b is also divisible by $gcf(a, b)$.

So, given that any linear combination of two numbers must be a multiple of their GCF, we know that the smallest possible positive value of $ax+by$ is $gcf(a,b)$ itself. However, there is still the question of whether or not that value can *always* be obtained, given any two numbers a and b. Well, it turns out that it can, and we're going to prove that by using a method which can also be used to determine *which* values of x and y are necessary to do so.

For this example, let's use the previous two values, $a=1139$ and $b=391$. Thus, the first line of the Euclidean algorithm for 1139 and 391 now reads

$$a=2b+357.$$

Solving this for 357 gives us

$$357=a-2b.$$

Plugging this in for the 357 in the next line of the Euclidean algorithm yields

$$b=1(a-2b)+34$$

$$34=3b-a$$

Now, the second equation solved for its remainder, we can plug in for both 357 and 34 in line 3:

$$a-2b=10(3b-a)+17$$

$$a-2b=30b-10a+17$$

$$11a-32b=17$$

which is the linear combination desired. We can check by plugging in the values of a and b:

$$11(1139)-32(391)=12529-12512=17.$$

Since this method can be used no matter what the values of a and b, we have now proven:

- For any integers a and b, there exists integers x and y such that $ax+by=gcf(a,b)$, and there is no smaller positive integer of the form $ax+by$.

A special case of this theorem is of some use, as both an existence theorem and an alternate definition of relatively prime:

- Integers a and b are relatively prime if and only if $ax+by=1$ for some integers x and y.

4. Find a general method, given solution (11, -32) to the Diophantine equation $1139x+391y=17$, of finding all other solutions.

The **Fundamental Theorem of Arithmetic** states that every positive integer greater than 1 has a unique factorization into prime numbers, that is, given any k, there exists a *unique* prime factorization $k=p_1p_2...p_n$ (here we will use the letter p exclusively to represent prime numbers.) Note that in this factorization there may be repetition among the list of prime factors given.

This fact, while important and intuitive to many mathematicians (and many math students,) is neither trivial nor is it trivial to prove. We're going to tackle this problem, as a group, in 3 parts. If you're reading this on your own, you'll have to try these yourself:

I. Prove that if $p\mid ab$, then $p\mid a$ or $p\mid b$. (Use the special case of the linear combination theorem above.)

II. Prove that any number $k\geq 2$ can be factored into a product of prime numbers. (Use strong induction.)

III. Prove that said prime factorization is unique. (Assume two factorizations and show they must be the same.)

5. Use prime factorization of integers to determine a general method for finding the GCF and LCM of a set of integers.

6. Prove that $gcf(a,b)\cdot lcm(a,b)=ab$. Does this work with 3 or more integers? Why or why not?

7. Prove another way of defining relatively prime: $lcm(a,b)=ab$ if and only if a and b are relatively prime.

Warm-up problems:

1. Determine the number of distinct positive divisors of 720,000.

2. Determine the sum of the positive factors of 1080.

3. Compute the number of lattice points in the first quadrant that lie on the graph of the line $14x + 35y = 2009$.

4. Three (not necessarily distinct) positive integers a, b, and c have a greatest common factor of 20 and a least common multiple of 800. Let m and M be the smallest and largest possible values of abc, respectively. Compute M/m.

5. Show that for all prime numbers $p > 3$, 24 divides $p^2 - 1$ evenly. [AHSME 1973]

6. What is the largest integer which must evenly divide all integers of the form $n^5 - 5n^3 + 4n$, where n is an integer greater than 2? [AMC]

7. Find the positive integer m such that the polynomial $p^3 + 2p + m$ divides $p^{12} - p^{11} + 3p^{10} + 11p^3 - p^2 + 23p + 30$. [AOPS]

The following practice problems are not necessarily directly related to the preceding material, but are at least tangentially related:

1. A “Primitive Pythagorean Triangle” is a right triangle with side-lengths that are three positive integers such that no two side-lengths have a common factor other than 1. In how many non-congruent Primitive Pythagorean Triangles is the difference between the length of the hypotenuse and the length of one of the legs equal to a prime p with p < 2008? [NYSML 2008 I6]

2. Compute the number of non-congruent rectangles whose length and width are positive integers and whose area is 2007. [NYSML 2007 I1]

3. Call a k-digit integer $d_1 d_2 \ldots d_k$ “Two-Prime-Linked” or TPL for short, if (a) all the digits are different and (b) each pair of adjacent digits forms a two-digit prime. For example, 417 is a 3-digit TPL integer since 4, 1, 7 are all different and 41 and 17 are two-digit primes. Compute the largest TPL integer. [NYSML 2007 I5]

4. Call a positive integer pooq if it is a four-digit integer of the form p00q where p and q are distinct one-digit primes, the middle two digits are zeroes, and the integer p00q is divisible by exactly one of the two primes, p or q. Thus, the year 2005 is pooq since 2 and 5 are different one-digit primes and 2005 is divisible by 5 and not by 2. Compute the number of pooq positive integers.[NYSML 2005 I5]

5. Let x be the number of even two-digit positive integers divisible by 4, and let y be the number of even two-digit positive integers that are not divisible by 4. Compute y – x. [NYSML 2003 I1]

6. How many positive integers less than 123 have an odd number of positive integer factors? [NYSML 2003 I3]

7. Let n be the smallest positive integer with the same number of distinct prime factors as the number 2002. Compute $\frac{n}{2002}$. [NYSML 2002 I1]