Number Theory

Tristan Pollner, Eshaan Nichani

August 7, 2014

1 Introduction

Number theory deals with the properties of integers. Number Theory problems are not as common as problems of the other subjects, and most solutions involve ideas from both Combinatorics and Algebra. In this class we will go over some basic strategies and theorems in number theory.

2 Concepts and Theorems

2.1 Basics

If a = nb for integers a, n, b, we say that a is a multiple of b, and b is a factor (or divisor) of a. A number p is *prime* if its only factors are 1 and itself. We can write a number n as the product of its prime factors as follows: $n = p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$

2.2 GCD and LCM

For two positive integers a and b, gcd(a,b) (greatest common divisor) is the largest integer that divides both a and b, and lcm(a,b) (least common multiple) is the smallest positive integer that is a multiple of a and b. If $a = p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$ and $b = p_1^{f_1} p_2^{f_2} \dots p_k^{f_k}$ (where some of the es and fs may be 0), then

$$gcd(a,b) = p_1^{min(e_1,f_1)} p_2^{min(e_2,f_2)} \dots p_k^{min(e_k,f_k)}$$

and

$$lcm(a,b) = p_1^{max(e_1,f_1)} p_2^{max(e_2,f_2)} \dots p_k^{max(e_k,f_k)}$$

Also, note that $gcd(a,b) \cdot lcm(a,b) = ab$.

One way to find the gcd of two numbers is by using the Euclidean algorithm. This uses the fact that $gcd(a,b) = gcd(a - nb, b)$ for any integer n. Then, using this repeatedly we can reduce our numbers down to two smaller ones, which we know the gcd of. For example, let's find the gcd of 105 and 28. We get that

$$gcd(105,28) = gcd(105-3\cdot 28, 28) = gcd(21,28) = gcd(21, 28-21) = gcd(21,7) = gcd(21-2\cdot 7, 7) = gcd(7,7) = 7$$

2.3 Modular Arithmetic

Mods are a way to look at the remainder of integers when divided by other integers. We say that $a \equiv b$ (mod m) if a and b give the same remainder upon division by m. For example, $25 \equiv 1$(mod 12). Addition and multiplication work the same in modular arithmetic as they do in regular arithmetic. For example $138 \cdot 13 \equiv 6 \cdot 2 \equiv 12$ (mod 13). Division, however is trickier. When using mods, we can look at what are called *inverses*. We let the inverse of a(mod m) be the unique positive integer $b < m$ such that $ab \equiv 1$(mod m). We see that a has an inverse if and only if $gcd(a,m) = 1$.

2.4 Divisors

Let $n = p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$. Then the number of divisors of n is

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

Note that for any divisor, the exponent of the prime must be less than the exponent in n. The sum of the divisors is

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

This is because upon expanding we get every possible combination of products of prime powers. Finally, the number of positive integers less than n and relatively prime to n is

$$\phi(n) = (p_1^{e_1} - p_1^{e_1-1})(p_2^{e_2} - p_2^{e_2-1}) \dots (p_k^{e_k} - p_k^{e_k-1}) = n(1 - \frac{1}{p_1})(1 - \frac{1}{p_2}) \dots (1 - \frac{1}{p_k}).$$

Note that after expanding, this is just PIE.

2.5 Some Advanced Theorems

If a is relatively prime to n, then

$$a^{\phi(n)} \equiv 1(\text{mod n}),$$

where $\phi(n)$ is Euler's totient function (in the previous section). If n is prime, then $\phi(n) = n - 1$. This gives Fermat's Little Theorem, which states that if p is a prime, and p doesn't divide a,

$$a^{p-1} \equiv 1(\text{mod p}).$$

Wilson's Theorem states that for a prime p

$$(p-1)! \equiv -1(\text{mod p}).$$

The Chinese Remainder Theorem states that if you have a congruence mod m and mod n, where m and n are relatively prime, then there exists exactly 1 solution mod mn that satisfies both the congruences. For example, consider the congruences $x \equiv 1(\text{mod } 3)$ and $x \equiv 3 \ (\text{mod } 4)$. This must have exactly 1 solution mod 12, and through guessing and checking we get that $x \equiv 7(\text{mod } 12)$.

3 Tips

1. **Look at primes.** Often times problems involving divisibility can be simplified by looking at divisibility of primes or powers of primes.

2. **Use techniques from Algebra.** Remember your factorization skills, these can come in handy when solving Diophantine equations. Try to exploit symmetry. Also replace variables using what you know about them. If you know an integer is odd, replace it with 2k+1 for some positive integer k. Also remember Simon's Favorite Factoring Trick.

3. **Look at small cases/Find trivial solutions.** Looking at small cases or trivial solutions can help you generalize and determine the solution to the original problem.

4. **Know powers mod certain numbers.** For example, perfect squares must equal 0 or 1 mod 3 and 4, and perfect cubes are -1, 0, or 1 mod 9.

5. **Guess and Check** Don't be afraid to guess and check. You should not start blindly guessing, however. First try to reduce the possibilities, and afterwards try each of these choices.

4 Problems

1. For $k > 0$, let $I_k = 10\dots064$, where there are k zeros between the 1 and the 6. Let $N(k)$ be the number of factors of 2 in the prime factorization of I_k. What is the maximum value of $N(k)$?

2. How many of the integers between 1 and 1000, inclusive, can be expressed as the difference of the squares of two nonnegative integers?

3. Find the number of rational numbers r, $0 < r < 1$, such that when r is written as a fraction in lowest terms, the numerator and denominator have a sum of 1000.

4. How many pairs of positive integers (a, b) are there such that $\gcd(a, b) = 1$ and

$$\frac{a}{b} + \frac{14b}{9a}$$

is an integer?

5. There exist r unique nonnegative integers $n_1 > n_2 > \cdots > n_r$ and r unique integers a_k $(1 \le k \le r)$ with each a_k either 1 or -1 such that

$$a_1 3^{n_1} + a_2 3^{n_2} + \cdots + a_r 3^{n_r} = 2008.$$

Find $n_1 + n_2 + \cdots + n_r$.

6. Let $n = 2^{31}3^{19}$. How many positive integer divisors of n^2 are less than n but do not divide n?

7. It is known that, for all positive integers k,

$$1^2 + 2^2 + 3^2 + \cdots + k^2 = \frac{k(k+1)(2k+1)}{6}.$$

Find the smallest positive integer k such that $1^2 + 2^2 + 3^2 + \cdots + k^2$ is a multiple of 200.

8. The sum of the first m positive odd integers is 212 more than the sum of the first n positive even integers. What is the sum of all possible values of n?

9. Ms. Math's kindergarten class has 16 registered students. The classroom has a very large number, N, of play blocks which satisfies the conditions:

(a) If 16, 15, or 14 students are present, then in each case all the blocks can be distributed in equal numbers to each student, and
(b) There are three integers $0 < x < y < z < 14$ such that when x, y, or z students are present and the blocks are distributed in equal numbers to each student, there are exactly three blocks left over.

Find the sum of the distinct prime divisors of the least possible value of N satisfying the above conditions.

10. In a rectangular array of points, with 5 rows and N columns, the points are numbered consecutively from left to right beginning with the top row. Thus the top row is numbered 1 through N, the second row is numbered $N + 1$ through $2N$, and so forth. Five points, P_1, P_2, P_3, P_4, and P_5, are selected so that each P_i is in row i. Let x_i be the number associated with P_i. Now renumber the array consecutively from top to bottom, beginning with the first column. Let y_i be the number associated with P_i after the renumbering. It is found that $x_1 = y_2$, $x_2 = y_1$, $x_3 = y_4$, $x_4 = y_5$, and $x_5 = y_3$. Find the smallest possible value of N.

11. (hard) Find the largest integer n satisfying the following conditions:
(i) n^2 can be expressed as the difference of two consecutive cubes;
(ii) $2n + 79$ is a perfect square.
(iii) $n < 1000$