Math 96:
Number Theory Techniques

October 15th, 2021

Today we will discuss some techniques from number theory that may prove useful on the Putnam Exam.

1 Primes and Factorization

Number theory is concerned with the structure of the natural numbers $1, 2, 3, \ldots$ and particularly with the multiplicative structure. We say that an integer n *divides* another integer m (or that m is a *multiple* of n or $n|m$), if the ratio m/n is an integer (or equivalently if there is an integer k so that $kn = m$). One question is given an integer n, what other numbers divide it?

One way to answer many of these questions is to break down integers into primes. A *prime* number is an integer $p > 1$ so that p has no positive divisors other than 1 and p. You can think of these as the building blocks or atoms of multiplication. The Fundamental Theorem of Arithmetic states that any integer n can be written as a product of prime numbers (perhaps times -1 if n is negative), and that this product is unique up to reordering of the factors (for example 30 is both $2 \cdot 3 \cdot 5$ and $5 \cdot 2 \cdot 3$, but you can't write it as some product of different primes). This means you can sort of think of a natural number as a bag of primes that are multiplied together. To multiply two numbers, just combine the bags. One number divides another if it has fewer copies of each prime in it.

1981 A1: Let $E(n)$ denote the largest integer k so that 5^k is an integral divisor of the product $1^1 2^2 3^3 \cdots n^n$. Calculate

$$\lim_{n\to\infty} \frac{E(n)}{n^2}.$$

2 Modular Arithmetic

We say that two integers a and b are congruent *modulo* m (written $a \equiv b \pmod{m}$) if and only if $m|a - b$. Alternatively, a is congruent to b modulo m if and only if they have the same remainder when divided by m. In particular, every integer is congruent modulo m to exactly one of $0, 1, 2, \ldots, m - 1$.

Furthermore, arithmetic modulo m is well defined. This means that if $a \equiv a' \pmod{m}$ and $b \equiv b' \pmod{m}$ then $a + b \equiv a' + b' \pmod{m}$ and $ab = a'b' \pmod{m}$. This means that you can perform arithmetic on numbers modulo m while only knowing the individual numbers modulo m.

Working with numbers modulo m (for carefully chosen values of m) often allows one to vastly simplify equations, making certain kinds of computations much easier.

2001 A5: Prove that there are unique positive integers a, n such that

$$a^{n+1} - (a + 1)^n = 2001.$$

It should be noted that division in modular arithmetic is a bit more complicated. For example, there is no number n so that $2n \equiv 1 \pmod{4}$. The general result is that there is a multiplicative inverse of a modulo m (i.e. a number a' so that $aa' \equiv 1 \pmod{m}$) if and only if a and m are *relatively prime*, that is if and only if a and m share no prime factors in common.

3 Hensel's Lemma

One often wants to be able to solve equations $f(x) \equiv 0$ modulo m for various values of m. When m is a prime, often there is nothing better to do than check all possible inputs for a solution. However, when m is a product of different primes, one can use something called the Chinese Remainder Theorem to combine solutions to $f(x) = 0$ mod each prime factor of m, to get a solution modulo m.

When m has higher powers of a given prime, something called Hensel's Lemma can often by used. In particular, we have:

Lemma 1. *Let f be a polynomial and m an odd integer (usually it is taken to be a prime). Then if there is an integer x so that $f(x) \equiv 0 \pmod{m}$ and $f'(x)$ is relatively prime to m, then there exists an integer $x' \equiv x \pmod{m}$ so that $f(x') \equiv 0 \pmod{m^2}$.*

Note that by iterating this, we can find integers $x_1, x_2, \ldots, x_k, \ldots$ so that $f(x_k) \equiv 0 \pmod{m^k}$.

Hensel's Lemma can be proved by Taylor expanding f. We note that

$$f(x') = f(x) + (x' - x)f'(x) + (x' - x)^2/2f''(x) + \ldots$$

If we have $x' - x$ is a multiple of m, then all of the terms beyond the first two will be multiples of m^2 already. Thus, we just need to have $f(x) + (x' - x)f'(x) \equiv 0 \pmod{m^2}$. Since $f'(x)$ is relatively, prime to m, it has a multiplicative inverse, and we can take $x' = x - f(x)/f'(x)$. We note that m will divide $x' - x$ here because it divides $f(x)$.

1981 B3 (modified): Prove that there are infinitely many integers n with the property that if p is a prime divisor of $n^2 + 1$, then p is also a divisor of $k^2 + 1$ for some integer k with $k < n$.

4 Multiplicative Functions

A function f on the natural numbers of call *multiplicative* if $f(nm) = f(n)f(m)$ for any pair (n, m) of relatively prime integers. There are many useful functions that are multiplicative. For example:

- $d(n)$ equals the number of positive divisors of n
- n^k
- $\phi(n)$ is the number of integers between 1 and n that are relatively prime to n
- $\sigma(n)$ is the sum of the positive divisors of n

Being multiplicative is a useful property for a function to have. It means that the value of f can be determined by its values at powers of primes (since any integer n can be written as a product of prime powers). Given a function $f(n)$ one often considers the sum over divisors of this function $F(n) = \sum_{d|n} f(d)$. One important result is the following:

Lemma 2. *Given f and F above, f is multiplicative if and only if F is.*

To see one direction of this, we use prime factorization. If $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$, the divisors of n are exactly the numbers of the form $p_1^{b_1} p_2^{b_2} \cdots p_k^{b_k}$ with $b_i \leq a_i$ for each i. Thus, $F(n)$ equals

$$\sum_b F(p_1^{b_1} p_2^{b_2} \cdots p_k^{b_k}) = \sum_b F(p_1^{b_1}) F(p_2^{b_2}) \cdots F(p_k^{b_k}).$$

However, the product separates out as

$$\left(\sum_{b_1=0}^{a_1} F(p_1^{b_1}) \right) \left(\sum_{b_2=0}^{a_2} F(p_2^{b_2}) \right) \cdots \left(\sum_{b_k=0}^{a_k} F(p_k^{b_k}) \right).$$

To prove the other direction one can use the fact that

$$f(n) = \sum_{d|n} F(d)\mu(n/d)$$

where $\mu(m)$ is the so-called Mobius function, which is equal to $(-1)^k$ if m is the product of k distinct primes and 0 otherwise.

1961 A4: Define a function f over the domain of positive integers as follows: $f(1) = 1$, and for $n > 1$, $f(n) = (-1)^k$ where k is the total number of prime factors of n. For example $f(9) = (-1)^2$, $f(20) = (-1)^3$. Define $F(n) = \sum f(d)$ where the sum ranges over all positive integer divisors of n. Prove that for every positive integer n, $F(n) = 0$ or $F(n) = 1$. For which integers n is $F(n) = 1$?