Math 96:
Number Theory Techniques

October 18th, 2019

Number theory is the study of the integers and in particular of their multiplicative and additive structures and how these relate to each other.

1 Prime Numbers

The most fundamental concept in number theory is that of prime numbers. These are integers $p > 1$ so that p cannot be written as $a \cdot b$ for any integers $1 < a, b < p$. Perhaps the biggest result in number theory is the fundamental theorem of arithmetic

Theorem (Fundamental Theorem of Arithmetic)**.** *Any positive integer n can be written as a product of prime numbers. Furthermore, this representation is unique up to the ordering of the terms.*

This means that we can treat numbers as sorts of bags of primes. For example, we say that d *divides* n (or $d|n$) if there is an integer a so that $n = d \cdot a$. Note that multiplying by a exactly, adds more primes to d. Therefore, d divides n if and only if each prime that divides d also divides n at least as many times.

Also note that given two numbers a and b in order for n to be both a multiple of a and a multiple of b, it must have at least as many copies of each prime p as the maximum number of copies among a and b. If it has exactly, this many copies for each p it is the *least common divisor* or a and b (denoted $\text{lcm}(a, b)$). Note that if $a|n$ and $b|n$ for any n, then $\text{lcm}(a, b)|n$. Similarly, we have a *greatest common divisor*, $\gcd(a, b)$. We also say that a pair of integers are *relatively prime* if their greatest common divisor is 1.

1999 B6: Let S be a set of integers greater than 1. Suppose that for each integer n there is some $s \in S$ such that $\gcd(s, n) = 1$ or $\gcd(s, n) = s$. Show that there exist $s, t \in S$ so that $\gcd(s, t)$ is prime.

2 Modular Arithmetic

We say that two integers a and b are congruent modulo some other integer m (written $a \equiv b \pmod{m}$) if m divides $a - b$. It is not hard to show, that this is an equivalence relation, meaning that you can think about the numbers modulo m as classes rather than needing to specify which number. Also note that any a is equivalent to exactly one number in $\{0, 1, 2, \ldots, m-1\}$. Finally, arithmetic modulo m is well defined in that you can determine $a+b \pmod{m}$ or $a \cdot b \pmod{m}$ only knowing $a \pmod{m}$ and $b \pmod{m}$. Finally, you cannot always divide modulo m, but if a and m are relatively prime, there is always an a' so that $aa' \equiv 1 \pmod{m}$.

This makes modular arithmetic a convenient tool, as often problems are simplified by considering everything modulo m for some carefully chosen m (usually a prime or a power of a prime).

1949 B4: Show that the coefficients $a_1, a_2, a_3, \ldots$ in the expansion $\frac{1}{4}[1+x-(1-6x+x^2)^{1/2}] = a_1x + a_2x^2 + a_3x^3 + \ldots$ are positive integers.

3 Chinese Remainder Theorem

If m and n are relatively prime, then k is divisible by the product mn if and only if it is divisible by m and n individually. This relates the value of k modulo n with the value of k modulo m. It turns out that much more is true:

Theorem (Chinese Remainder Theorem)**.** *Let $n_1, n_2, \ldots, n_k$ be pairwise relatively prime integers with $n = n_1 n_2 \cdots n_k$. Notice that if we are given the value of an integer x modulo n, this determines its value modulo each of the n_i. Conversely, if we are given integers $x_1, x_2, \ldots, x_k$, there is a unique congruence class x modulo n so that $x \equiv x_i \pmod{n_i}$ for all i.*

This says that if we want to understand x modulo n, it is enough to understand it modulo each n_k. Since any n can be broken down as a product of powers of primes, usually this means that when considering modular information it suffices to consider each prime separately. We also note that these numbers can be constructed. You can first produce numbers a_i which is a multiple of all of the n_j for $j \neq i$ so that $a_i \equiv x_i \pmod{n_i}$ and $a_i \equiv 0 \pmod{n_j}$. Then you can take x as the sum of the a_i.

USAMO 2008 #1: Prove that there are n pairwise relatively prime integer $k_1, k_2, \ldots, k_n$ greater than 1, such that $k_1 k_2 \cdots k_n - 1$ is a product of two consecutive integers.

4 Modular Arithmetic Modulo Primes

Modular arithmetic is especially interesting modulo primes. For one thing, all non-zero elements have inverses. In particular if $a \not\equiv 0 \pmod{p}$ for a prime number p, then there exists a b so that $ab \equiv 1 \pmod{p}$. This gives the numbers mod p the structure of a *field.* Being able to divide is often quite useful. Another important property of arithmetic modulo p has to do with exponentiation. In particular, we have the following:

Theorem (Fermat's Little Theorem)**.** *For any integer a and any prime p*

$$a^p \equiv a \pmod{p}.$$

Additionally, if you consider how these number behave under multiplication, there is always a primitive generator g so that the non-zero integers modulo p are exactly $1, g, g^2, g^3, \ldots, g^{p-2}$.

1994 B6: For any integer a set

$$n_a = 101a - 100 \cdot 2^a.$$

Show that for $0 \leq a, b, c, d \leq 99$ that $n_a + n_b \equiv n_c + n_d \pmod{10100}$ implies $\{a, b\} = \{c, d\}$.