Advanced Number Theory

Jacob Steinhardt

1 How To Prove That There's A Lot Of Something

How much is a lot? Well, infinity is pretty big, so let's start with that. We already know that there are a lot of primes, as if there weren't a lot, then they would make a finite set, $\{p_1, \ldots, p_n\}$. But then $p_1 p_2 \ldots p_n + 1$ would have no prime factors, which would be pretty tricky, so there are a lot of primes.

We also know that if there is more than one prime in an arithmetic progression, then there are a lot of primes. Note that more than one prime is equivalent to saying that the common difference and first term are relatively prime. This result is known as Dirichlet's Theorem because it was proven by Dirichlet. However, proving it in the general case is pretty tricky, so instead we will prove a special case – that there are infinitely many primes of the form $4k+1$. The technique is a valuable one. You find a useful property that is possessed only by numbers with divisors of the form that you are trying to show there is a lot of, then you assume that there are only finitely many primes of that form, then you find a number with that property that is not divisible by any of those primes.

In the case of $p = 4k + 1$, we know that all prime factors of $n^2 + 1$ are of the form $4k + 1$. This is because, if

$$n^2 + 1 \equiv 0 \pmod{p}$$

has a solution i, then for every quadratic residue r, $-r$ is also a quadratic residue, as $(i\sqrt{r})^2 \equiv -r \pmod{p}$. Thus, there exist distinct numbers $\sqrt{r}, -\sqrt{r}, i\sqrt{r}, -i\sqrt{r}$ among the non-zero residues of p. But this implies that $4|p-1$, so $p = 4k+1$, as stated. Now, assume that there are only finitely many primes $\{p_1, \ldots, p_n\}$ of the form $4k + 1$. Then

$$(p_1 p_2 \ldots p_k)^2 + 1$$

has no prime factors, which is a contradiction, so there are infinitely many primes of the form $4k+1$.

Another pretty cool thing is that there are arbitrarily long arithmetic progressions of primes. This theorem was proven very recently by Terence Tao. Another interesting result is that the distribution of primes goes as $\frac{1}{\ln(N)}$.

2 Generators

A *generator on p* or *primitive root of p* (denoted g) is a residue modulo p such that the equation $g^k \equiv r \pmod{p}$ has a solution for every non-zero residue r. Equivalently, it is a residue such that $\{g^1, g^2, \ldots, g^{p-1}\}$ is a permutation of $\{1, 2, \ldots, p-1\}$. It is also a residue such that the smallest positive value of k such that $p|g^k - 1$ is $p - 1$. It follows that if g is a generator, then g^k is a generator if and only if k is relatively prime to $p - 1$. Thus, if there is a single generator on p, then there are $\phi(p-1)$ such generators, where ϕ is the totient function (the number of natural numbers relatively prime to and less than a given number). Note that all of the above statements are biconditional ("if and only if" statements).

However, the existence of generators in a prime mod is far from obvious, and the proof is not enlightening at this point unless you know group theory. If you do know group theory, then the

proof has something to do with that, and is actually more general. It says that there is a single generator if and only if the mod you are working in is 2 or 4 or p^k or $2p^k$, where p is an odd prime.

3 Order

We define $ord_p(n)$, or the order of n mod p, as the smallest natural number k such that $n^k \equiv 1 \pmod{p}$. Obviously, $ord_p(g) = p-1$ iff g is a generator. Furthermore, $ord_p(r)|p-1$, and for any divisor d of $p-1$, there are $\phi(d)$ residues r such that $ord_p(r) = d$. This leads to the interesting result that

$$\sum_{d|p-1} \phi(d) = p-1$$

In fact, it does not matter that $p-1$ is one less than a prime. We can generalize this to say that

$$\sum_{d|n} \phi(d) = n$$

Keep this result in mind, as we will revisit it later.

Orders have many interesting properties that can usually be pulled out by considering numbers as powers of generators. If $ord_p(n) = k$, then $n = g^{\frac{p-1}{k}}$ for some generator g. Thus, for a fixed generator g, it must be equal to $g^{\frac{l(p-1)}{k}}$ for some l relatively prime to $p-1$. The most immediate consequence of this is that $ord_p(ab)|gcd(ord_p(a), ord_p(b))$.

4 Quadratic Reciprocity

Hopefully you already know this because Peter told you, but

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}$$

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$$

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$$

5 Some Pretty Tricky Problems

These problems are pretty tricky. In fact, they are so tricky that not even Terence Tao has solved them (at least, as of the writing of this lecture). Therefore, if you have an idea that requires you to prove (or disprove) one of these, you should probably try something else.

1. Goldbach Conjecture: Every even number greater than 2 can be written as the sum of two primes.
2. Twin Prime Conjecture: There are infinitely many numbers n for which $2n-1$ and $2n+1$ are both prime.
3. 2 is a generator in infinitely many prime mods.
4. $an^2 + bn + c$ is prime for infinitely many values of n, provided that a, b, c are relatively prime.

6 Multiplicative Functions

A function is *multiplicative* iff

$$f(p)f(q) = f(pq)$$

for all relatively prime p and q. We additionally require that $f(1) = 1$ (this only excludes the case where $f(n) = 0$ for all n).

Multiplicative functions are interesting because once a function has been proven to be multiplicative, it is easy to come up with an explicit formula in terms of the number's prime factorization. Consider, for example, τ (number of divisors of n), σ (sum of divisors of n), and ϕ (number of natural numbers relatively prime to and less than n). Once these have been shown to be multiplicative, explicit formulas in terms of the prime factorization immediately pop out, as their values are obvious in the case when the input is a power of a prime. Another interesting (and slightly surprising) result is that, for all multiplicative functions,

$$f(a)f(b) = f(gcd(a,b))f(lcm(a,b))$$

The concept of multiplicative functions allows us to define a *Dirichlet convolution* between two functions, $f * g$, read f convolve g:

$$(f * g)(n) = \sum_{d|n} f(d)g(\frac{n}{d})$$

Another slightly unexpected result is that if f and g are multiplicative, then $(f * g)$ is also multiplicative. If we define $f_c(n) = n^c$, then we are in a position to take another look at our earlier identity:

$$\sum_{d|n} \phi(d) = n$$

This is simply $\phi * f_0$! Both ϕ and f_0 are clearly multiplicative, and in the case when n is of the form p^k,

$$\sum_{d|n} \phi(d) = 1 + (p-1) + p(p-1) + p^2(p-1) + \ldots + p^{k-1}(p-1) = p^k$$

so we have proven the generalization of our identity. We can also easily show that $\tau = f_0 * f_0$ and $\sigma = f_0 * f_1$. Another unexpected result is that if f, g, and h are multiplicative, and $(f*g)(p^k) = h(p^k)$ for all primes p and natural numbers k, then $f * g = h$.

7 Moebius Inversion

Actually there should be two dots over the o instead of the e, but I don't know how to do that in LaTeX. Define the Moebius function $\mu(n)$ as follows: $\mu(n) = 0$ if a square greater than 1 divides n (equivalently, if the square of a prime divides n, or there are any exponents greater than 1 in the prime factorization of n). Otherwise, $\mu(n) = 1$ if n has an even number of distinct prime factors and $\mu(n) = -1$ if n has an odd number of distinct prime factors. $\mu(1) = 1$ as a special case, since 1 has zero prime factors. μ is multiplicative. The Moebius Inversion formula states that if

$$g = f * f_0$$

then

$$f = \mu * g$$

Note that f and g need not be multiplicative, though if f is multiplicative then g is obviously multiplicative. This is very interesting because it says that we can reverse certain Dirichlet convolutions, and it also gives us an alternate expression for ϕ:

$$\phi = f_1 * \mu$$

There are all sorts of neat relations between common arithmetic functions that can be exploited with the Moebius function.

8 Problems

The problem set will be to prove everything that I just told you. Use the definition of a primitive root as g such that $ord_p(g) = p - 1$. You may assume that such a primitive root exists:

1. g is a primitive root iff $\{g^1, g^2, \ldots, g^{p-1}\}$ is a permutation of $\{1, 2, \ldots, p-1\}$.
2. If g is a generator, then g^k is a generator iff k is relatively prime to $p - 1$.
3. There are $\phi(p-1)$ generators in mod p.
4. $ord_p(r)|p - 1$.
5. For any divisor d of $p - 1$, there are $\phi(d)$ residues r such that $ord_p(r) = d$.
6. $ord_p(n) = k$ iff $n = g^{\frac{p-1}{k}}$ for some generator g.
7. $ord_p(ab)|gcd(ord_p(a), ord_p(b))$.
8. ϕ is multiplicative.
9. If f is multiplicative, then $f(a)f(b) = f(gcd(a,b))f(lcm(a,b))$.
10. If f and g are multiplicative, then $f * g$ is multiplicative.
11. The Dirichlet convolution operation is associative and commutative.
12. If f, g, and h are multiplicative, and $(f * g)(p^k) = h(p^k)$ for all primes p and natural numbers k, then $f * g = h$.
13. μ is multiplicative.
14. $\mu * (f * f_0) = f$.
15. Let ϵ be a function such that $\epsilon(1) = 1$, $\epsilon(n) = 0$ for $n \neq 1$. Find a statement analagous to Moebius inversion for all multiplicative functions α such that there exists α^{-1} where $\alpha * \alpha^{-1} = \epsilon$.

9 More Problems

1. For any r, there are infinitely many ordered pairs (k, p), $k < p$, with p being a prime, such that $p|2^k - r$.
2. $p|1^n + 2^n + \ldots + p^n$ iff n is not a multiple of $p - 1$.
3. Let $f(n)$ denote the number of primes that divide n. Let $g(n) = 2^{f(n)}$. Find $\sum_{d|n} g(d)$ in terms of the prime factorization of d.
4. Find all functions f such that

$$\sum_{d|n} f(d) = n^2$$

   Generalize your result to

$$\sum_{d|n} f(d) = n^k$$

   and

$$\sum_{d|n} f(d) = \phi(n)$$

5. If g is a multiplicative function and

$$\sum_{d|n} f(d) = g(n)$$

   then prove that f is multiplicative and unique and characterize f in terms of its prime factorization and the values of g at powers of primes.
6. There are infinitely many primes of the form $4k - 1$.
7. Find, and prove the uniqueness of, the function f such that

$$\int_1^x f\left(\frac{x}{y}\right) g\left(y\right) dy = \frac{d}{dx} g\left(x\right)$$

   for all smooth functions g. (Hint: it may be necessary to express your answer as the limit of a class of functions.)