Number theory in the year 2014

January 4, 2014

1 Introduction

Number Theory is one of the oldest subjects in math, long before math olympiads were around! This set of notes aims to introduce you to some tools and tricks to get you oriented when you're working on a number theory problem. Remember, the best way to get better is to develop your intuition by doing lots and lots of examples!

If you're looking to strengthen your knowledge of the basic theorems and their not-so-basic corollaries, Naoki Sato has an excellent set of notes online:

http://www.artofproblemsolving.com/Resources/Papers/SatoNT.pdf

2 Primes are the building blocks of Number Theory!

Fundamental theorem of arithmetic: Every positive integer n can be uniquely written as a product of prime powers $n = \prod_{i=1}^{m} p_i^{e_i}$.

Ok, so we all probably know this theorem (though I bet it's harder to prove than most of you think!) The great thing about it is that this is really a theorem to be used: given a problem about an integer n, you should always consider looking at its prime factorization! For instance, a positive integer n is equal to 1 if and only if its not divisible by any prime! Also, many functions have nice representations in terms of the prime factorization. Here are some examples:

- The Euler phi function $\phi(n)$ is defined to be the number of positive integers less than n which are relatively prime to n.
- The divisor function $d(n)$ is defined to be the number of positive integers that divide n.
- The sum-of-divisors function $\sigma(n)$ is defined to be the sum of all positive divisors of n: $\sigma(n) = \sum_{m|n} d(m)$.

For $f(n)$ any of the functions above, one has the relation $f(mn) = f(m)f(n)$ whenever $(m, n) = 1$ **(Excercise:Prove this!)** This relation is called being *weakly multiplicative*. This means that to compute $f(n)$ we just need to compute $f(p^k)$

for prime numbers p and integers k. It follows that for $n = \prod_{i=1}^{m} p_i^{e_i}$ we have the relations

$$\phi(n) = \prod_{i=1}^{m}(p_i^{e_i} - p_i^{e_i-1}), d(n) = \prod_{i=1}^{m}(e_i + 1), \sigma(n) = \prod_{i=1}^{m} \frac{p_i^{e_i+1} - 1}{p_i - 1}$$

For some practise with weakly multiplicative functions, try the following exercises:

Exercise 1.

1. *For a positive integer n, let $f(n) = \sum_{d|n} d^2$ denote the sum of the squares of all the divisors of n. Find a formula for $f(n)$.*
2. *For a positive integer n, let $f(n) = \sum_{d|n} \phi(d)$ denote the sum of the phi function evaluated at all divisors of n. Find a formula for $f(n)$.*

Factoring into primes can also frequently turn multiplicative problems into additive ones, as in the following example:

Example 1. *Let a, b be positive integers with*

$$a|b^2, b^2|a^3, a^3|b^4, \ldots$$

Prove that $a = b$.

3 Modular arithmetic: some basic facts

Given a positive integer n,we say two integers a, b are equal (or congruent) *modulo* n if $a - b$ is divisible by n. We write this as $a \equiv b \mod n$.

Modular arithmetic is just like ordinary arithmetic except we only care about equality modulo some number n. Every integer is congruent to one of $\{0, 1, \ldots, n-1\}$ modulo n so we have a finite set of numbers which we can add and multiply! We call $\{0, 1, \ldots, n-1\}$ the *residue classes* modulo n. We can even divide by certain numbers: e

- If $(a, n) = 1$, then there is a unique residue class b modulo n such that $ab \equiv 1 \mod n$. We refer to b as a^{-1}.

The following is perhaps the most useful tool in all of number theory:

Theorem 3.1. ***Fermat's little theorem***
For p a prime number and n a positive integer not divisible by p, we have

$$n^{p-1} \equiv 1 \mod p.$$

It is also useful to note that $n^p \equiv n \mod p$ for ALL n, and this can sometimes be a more convenient form.

Proof. Consider the product

$$A \equiv 1 \cdot 2 \cdots (p-1) \mod n.$$

Then

$$n^{p-1}A \equiv n \cdot (2a) \cdots ((p-1)n) \mod p.$$

But as we're working modulo n, the sets $\{1, 2, \ldots, n\}$ and $\{n, 2n, \ldots, (p-1)n\}$ are permutations of each other(why?) hence

$$n^{p-1}A \equiv A \mod p$$

and the conclusion follows.

□

The trick in the proof works very frequently: Since there are only finitely many numbers in modular arithmetic, it often helps to group them all together!

Fermat's little theorem has a very natural generalization, proved in the same way:

Theorem 3.2. ***Euler's theorem***
Let m, n be positive integers with $(m, n) = 1$. Then

$$m^{\phi(n)} \equiv 1 \mod n.$$

This has the following very nice corollary: we say that an integer m is a *quadratic residue* modulo n if there exists an integer k with $k^2 \equiv m \mod n$.

Theorem 3.3. *Let p be an odd prime. Then if -1 is a quadratic residue modulo p, $p \equiv 1 \mod 4$.*

Proof. Suppose $k^2 \equiv -1 \mod p$. Then $p|k^4 - 1$, so by Fermat's little theorem

$$p|(k^4 - 1, k^{p-1} - 1) \to p|(k^{(p-1,4)} - 1).$$

Now, assume $p \equiv 3 \mod 4$. Then we get that $p|k^2 - 1$ and so $2 \equiv 0 \mod p$, a contradiction.

□

This is one of the most used facts throughout number theory. In fact, the 'if' in the theorem is really an 'if and only if'. Prove this by doing the following 2 exercises:

Exercise 2.

- ***Wilson's theorem*** *Let p be an odd prime. Show that $(p-1)! \equiv -1 \mod p$.*
- *Let $p \equiv 1 \mod 4$ be a prime number. Consider $x = \left(\frac{p-1}{2}\right)!$. Prove that $x^2 \equiv -1 \mod p$, and hence -1 is a quadratic residue.*

3.1 Supplements: Primitive roots

This section contains material that is a bit more advanced, but is definitely good to keep in mind as the way arithmetic modulo primes works!

for positive integers m, n with $(m, n) = 1$, we say that k is the *order* of m modulo n if k is the smallest positive integer with $m^k \equiv 1 \mod n$. It is not hard to show that if $m^s \equiv 1 \mod n$, then $k|s$. Thus the order of m always divides $\phi(n)$.

For a positive integer n, m is called a *primitive root* modulo n if $(m, n) = 1$ and the order of m is exactly $\phi(n)$. This implies that the sequence $1, m, m^2, \ldots, m^{\phi(n)-1}$ contains every residue class modulo n that is relatively prime to n.

Theorem 3.4. *If $n = p^k$ or $n = 2p^k$ where p is an odd prime, then there exists a primitive root modulo n.*

Exercise 3. *Prove this using the following steps:*

- *Assume $n = p$ is a prime. For $d|p-1$, Show that the number of residue classes x with order d is at most $\phi(d)$.*
- *For $n = p^k$ with $k \geq 2$, show that if x is a primitive root modulo p^{k-1}, then either x or $x + p$ is a primitive root modulo p^k.*

The existence of a primitive root makes a lot of tricky looking stuff really simple. For example, it can be used to give a really quick proof of the fact that -1 is a quadratic residue modulo a prime p if and only if $p = 2$ or $p \equiv 1 \mod 4$. Try the following exercises using primitive roots:

Exercise 4.

- *Prove that for a prime p and positive integers d, m with $p \not| m$, the equation*
$$x^d = m$$
has either $(m, p-1)$ or 0 solutions.
- *For an odd prime p, Determine the positive integers m for which*
$$1^m + 2^m + \cdots + (p-1)^m$$
is divisible by p.

4 Modular arithmetic: Some basic tricks

A typical problem in number theory asks to find all solutions in positive integers to some polynomial equation, and a typical trick for these problems is to try and use modular arithmetic! Here is an example:

Example 2. *Prove there are no integer solutions m, n to $m^5 + 7 = y^2$.*

Proof. Working modulo 11, $m^5 + 7$ must equal one of $\{6, 7, 8\}$ and y^2 must equal one of $\{0, 1, 3, 4, 5, 9\}$. Thus there are no solution.

□

If you're used to doing number theory, the above solution probably looked familiar. How did we know to look modulo 11? Well, we wanted to work modulo some number n such that there are few residues that are $5'th$ powers. This amounts to $5|\phi(n)$, so the prime 11 seemed natural. In general, you want to pick a prime p (or a prime power sometimes) such that $p-1$ shares many factors with the exponents. It can also be helpful to work modulo 8, as it has only 1 odd quadratic residue! Try using the same philosophy to solve the following problem:

Example 3. *Find all integer solutions to* $x_1^9 + x_2^9 + ... + x_8^9 = 2005$.

This basic idea usually can't solve most problems by itself, but if you can combine it with other observations and keep pushing you can get really far! Here is a good example from the Russian Olympiad in 2006:

Example 4. *If an integer* $a > 1$ *is such that* $(a-1)^3 + a^3 + (a+1)^3$ *is the cube of an integer, then show that* $4|a$.

Proof. The sum of cubes looks pretty, but useless for working with! Expand to get $3a(a^2+2) = k^3$ for some k. Now, since $-2a \cdot (3a) + 3 \cdot (a^2+2) = 6$, we have $(3a, a^2+2) = 1, 2, 3$ or 6. If a is even, then $a^2 + 2 \equiv 2 \mod 4$. Now,

$$2|k^3 \Rightarrow 2|k \Rightarrow 8|k^3$$

so if a is even then $4|a$, as desired. Else, we must have $(3a, a^2+2) = 1$ or 3.

If $(3a, a^2+2) = 1$, then $3a = s^3$ and $a^2 + 2 = t^3$ for some integers s, t. Since $3a = s^3$ we must have a be divisible by 3, and thus $t^3 \equiv 2 \mod 9$, which is easily checked to be impossible. Thus this case cannot happen.

If $(3a, a^2+2) = 3$, then $a^2 + 2 \equiv 0 \mod 3$, so 3 doesn't divide a and thus $a = s^3$ for some integer s. Hence we have

$$\left(\frac{k}{s}\right)^3 = 3(a^2+2) = 3(s^6+2)$$

which implies that $s^6 \equiv 7 \mod 9$, which is also impossible. Thus this case cannot happen either and we're done again.

□

While the above proof is quite long, there wasn't a single complicated step! All we did was go through the cases for greatest common divisors, work mod 4 and work mod 9. You'd be surprised how often this kind of tenacity pays off!

Some other supplements to this technique are as follows:

- For positive integers m, n we have $(m, n) < |m - n|$
- If m, n are relatively prime positive integers and mn is a k'th power, than m and n are k'th powers also
- For some polynomial equations $P(x, y, z) = 0$, if you can show each variable is divisible by n, you can divide everything by n to get a smaller solution!
- Factor polynomial expressions as often as possible, especially if on the other side lies a perfect power!

5 Quadratic reciprocity

If p is an odd prime and a is relatively prime to p, set $\left(\frac{a}{p}\right)$ to be 1 if a is a quadratic residue modulo p, and -1 otherwise. the following theorem displays a remarkable and deep symmetry:

Theorem 5.1. ***Quadratic reciprocity*** *If p, q are distinct odd primes, then*

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

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

6 Olympiad Problems

Try the following problems for practise (Careful: They're not designed to be easy!)

1. Prove that for positive integers m, n, the number $m^3 + mn^3 + n^2 + 3$ cannot divide $m^2 + n^3 + 3n - 1$.
2. For each positive integer a, let $M(a)$ denote the number of positive integers b for which $a+b$ divides ab. Find the maximum value of $M(a)$ for $1 \leq a \leq 2013$.
3. Find all primes p, q such that q divides $30p - 1$ and p divides $30q - 1$.
4. Show that if an infinite arithmetic progression of positive integers contains a square and a fifth power, it must contain a tenth power.
5. (Indonesia, 2013) An integer n is called "elephantine" if there exists a positive integer x such that $x^{nx} + 1$ is divisible by 2^n.
   - Prove 2015 is Elephantine.
   - Find the smallest x such that $x^{nx} + 1$ is divisible by 2^n for $n = 2015$.
6. Find all solutions of the following equation in integers $x, y : x^4 + y = x^3 + y^2$
7. a, b are integers with $a \neq 0$ such that $a + 3 + b^2$ is divisible by $6a$. Prove that $a < 0$.
8. Prove that for all positive integers n there is a power of 10 with n digits in base 2 or base 5 but not in both.
9. Prove that every positive integer can be written as $x^2+y^2-5z^2$ for appropriate integers x, y, z.
10. The function $f : \mathbb{Z} \to \mathbb{Z}$ has the property that for all m, n we have

    $$f(m) + f(n) + f(f(m^2 + n^2)) = 1.$$

    It is given that there exist integers a, b with $f(a) - f(b) = 3$. Prove that there exist integers c, d with $f(c) - f(d) = 1$.

11. 100 distinct natural numbers $a_1, a_2, \ldots, a_{100}$ are given. Set b_i to be a_i plus the gcda of the remaining 99 numbers. What is the maximal possible number of distinct integers among the b_i?

12. Consider a positive integer number n and the function $f : \mathbb{N} \to \mathbb{N}$ by

$$f(x) = \begin{cases} \frac{x}{2} & \text{if } x \text{ is even} \\ \frac{x-1}{2} + 2^{n-1} & \text{if } x \text{ is odd} \end{cases}.$$

Determine the set:

$$A = \{x \in \mathbb{N} \mid \underbrace{(f \circ f \circ .... \circ f)}_{n \ f\text{'s}}(x) = x\}.$$

13. Find all positive integer triples (a, n, k) such that $n > 1$, and $a^n + 1$ is the product of the first k odd primes.

14. Find all positive integer triples (m, p, q) such that p, q are prime and

$$2^m p^2 + 1 = q^5.$$

15. Find all pairs of positive integers (m, n) such that

$$2^n + (n - \phi(n) - 1)! = n^m + 1.$$

16. Alice and Bob play a game. They Start with an empty set S. First, Alice picks a positive integer m to add to S. Then Bob must pick a positive integer which is not a multiple of m, and adds it to S. On each subsequent turn, a positive integer k has to be picked which cannot be obtained by adding together elements already in S, possibly with repetition, and then k gets added to S. So for example, if $S = \{5, 7\}$ at some point in the game, then Alice **can't** pick {5,7,10,12,14,15...}. The loser is the player that picks the number 1. Determine which player has a winning strategy.