

TJUSAMO Lecture 11- Number Theory

Pdiao06

January 28, 2006

In my opinion, number theory is an extremely fascinating subject. There is much crazy number theory out there (ever heard of the Riemann Hypothesis?). Fortunately, the stuff in contest math is much simpler than that. It is mostly ignored in high school curriculum, we seem to like to do a lot of algebra and calculus. However, do not let this fool you, number theory is not nearly as “advanced” as those subjects. At the core, number theory is very simple. In fact, most of the time, the problems can be stated in very simple terms and at the same time, the tools we have are much more limited than in other subjects. This is good news and bad news. Good news is it doesn't take long to learn the tools. Bad news is it requires much trickiness.

Now that the little introductory blurb is done. Let us go over some common notation.

1 Notation

1. $\mathbb{N}, \mathbb{Z}, \mathbb{Z}_p, \mathbb{Z}/p\mathbb{Z}, \mathbb{Q}, \mathbb{Q}', \mathbb{R}$, and \mathbb{C} We will take these to be the natural numbers, integers, p -adic integers, integers in mod p , rational numbers, irrational numbers, reals, and complex numbers respectively. Don't worry about the p -adic numbers if you don't know what those are, that was just thrown in to warn some people of the real standard notations.
2. The above things are all systems or playgrounds. They are where we are working. Most of the time, in math class without even knowing it, we make the assumption we are working in the reals. Sometimes, we venture into the complex numbers. For example, what if I asked two simple questions:
 - Solve for $x: x^2 = 1$ Well the answer is, it depends. What if I told you that 3 is a solution? What if I told you, that indeed there are 4 solutions: $x = 1, 3, 5, 7$? You would think I was crazy until you realized that I was working in mod 8.
 - Solve for $x: x^2 = -1$ What is the answer? You might be more suspicious now. In the reals there are no solutions! In fact, this is essentially the only polynomial equation that has no solutions in the reals. As soon as we add i to the reals, we can solve this equation. We also happen to now be able to solve all such

equations. We have created the complex numbers! But I claim that in fact the solutions could be $x = 2, 3$ You are probably on to me now. I'm talking about mod 5! But maybe crazier than that, $x = i, j, k$, are also solutions. Working with quaternions (this is where those vectors and cross products and stuff come from), we have these solutions. Our ARML shirt was blatantly wrong last year, since $i * j = k$ which is certainly not real.

I hope you are all sufficiently confused now. Apparently, an innocent polynomial equation could have more than the degree number of solutions, no solutions, or not even make any sense at all. Fortunately, all you have to avoid all this craziness is make sure you specify the system you are working in. In that spirit, let us learn some more ways to specify the system you are in. If we put a little floating plus to the right of any of these symbols we get the positive numbers. Most of the time, we put a little cross floating to the right of these signs we get the same system with zero removed. For example \mathbb{N} is essentially the same as \mathbb{Z}^+ . Also, sometimes you might see things that look like $\mathbb{R}[x]$. What this means, is we add x as an element to the reals and see what kind of system we get. In this case, we get polynomials. Another example is that $\mathbb{R}[i]$ is essentially the same as \mathbb{C} . As you can tell all of these systems can be related to each other. It is extremely important to understand the relationships between them. In fact, I believe all of these systems can be based directly back to the integers, so if ever there is some sort of contradiction in math and the whole thing collapses, we must have gotten the integers wrong. All these systems have rules and we start calling them groups, rings, fields, etc. As you learn more math, I'm sure you will study them if you haven't already. Maybe one day you'll finally understand Druker's shirt. \mathbb{Z}_1 ring to rule them all: $\{0\}$.

3. In general, variable names in math are actually quite standard. For example, for some reason w, x, y, z are useful as variables. Maybe the numbers at the beginning of the alphabet are used for constants most often. Often times, s, t, u, v are most useful as some sort of parameters. p is almost always a prime and in the case when we need two primes, we either use subscripts or sometimes venture to use q . m, n are often generic integers, with m frequently used for mods and n for numbers. i, j, k are most useful as indices, but sometimes k gets used in division. q, r are obviously related and commonly related to division as quotient and remainder. These are not strict rules, but I have seen an instructor change all the ps in an equation to ms just because we pointed out it didn't necessarily have to be prime.

Other notation and terminology will be explained as they come up. As a note about the general style of the lecture, it is bad. But beyond that, I am going to omit most proofs so as to not turn this into a textbook. If you have any questions, you can always talk to me personally.

2 Divisibility and Primes

2.1 Preliminary Notions

Most of us know what it means for something to divide something else. However, for our purposes, it is important to define exactly what it means. For $a, b \in \mathbb{Z}$ and $a \neq 0$, we say that a divides b iff $\exists k \in \mathbb{Z}$ s.t. $b = ka$. We write $a|b$ to indicate that a divides b . a is called a divisor of b and b is called a multiple of a . A prime p is prime iff it has exactly two distinct positive divisors. Any other integer is composite except 1 and -1 .

Here are two more concepts that most everybody is already familiar with. The *greatest common divisor* of two integers a, b (not both 0) is $k = \gcd(a, b) = (a, b)$ where $\forall d \in \mathbb{Z}$ s.t. $d|a, d|b, k \geq d$. Two integers a and b are *relatively prime* or *coprime*, if $(a, b) = 1$. The *least common multiple* of integers a and b is defined as the smallest positive integral multiple of both a and b . We write it as $\text{lcm}[a, b] = [a, b]$.

Work out for yourself this gcd and lcm junk for those crazy numbers 0 and 1. Also, note that these definitions can be generalized in many different ways. One way is by defining gcd and lcm for n numbers and the other is to generalize to different systems, not the integers.

2.2 Fundamental Theorem of Arithmetic

There are several fundamental theorems that lead up to the Fundamental Theorem of Arithmetic. We will briefly cover them and omit the proofs.

1. **Division Algorithm** Most of you probably know how to divide, but probably never thought of it in this way. Thankfully given any two integers a and b with $b \neq 0$, you can divide a by b . In more precise terms: Given $a, b \in \mathbb{Z}$, $\exists q, r \in \mathbb{Z}$ s.t. $a = bq + r, 0 \leq r < |b|$. We call a, b, q , and r the dividend, divisor, quotient, and remainder respectively. This is known as the division algorithm for unknown reasons.
2. **Bezout's Identity** Using the division algorithm we can solve an extremely interesting question. Given two integers a and b , the equation $ax + by = 1$ has integer solutions iff $(a, b) = 1$. This is an extremely important idea that was on the AMC 12A as a problem this year. Notice that this also implies that $ax + by = d$ has solutions for all integer d . What d can you solve for if $(a, b) \neq 1$?
3. **Euclid's Lemma** This can be easily proven with Bezout's Identity. It states that if $a|bc$ and $(a, b) = 1$, then $a|c$. This is an interesting and intuitive fact to know. However it is most useful in proving the final result.
4. **Fundamental Theorem of Arithmetic** This is also known as unique factorization. It states that given any integer n , it can be uniquely expressed as the product of distinct prime powers with a sign in front. Everybody's been prime factoring since 4th grade, but now you know for sure that no matter how you do it, you'll get the same answer.

Using the fundamental theorem of arithmetic it is very easy to see exactly some things about gcds lcms. The gcd of two numbers will simply be the product of the highest prime powers that will divide both of the numbers. Just imagine lookin at the prime factorizations one prime at a time and just taking the minimum of the two prime powers in each factorization. The lcm of two numbers would simply be the max of the prime powers. Taking these two results it is easy to conclude that $(a, b) * [a, b] = ab$

2.3 Euclidean Algorithm

This algorithm comes from one important fact. That fact is actually much important than the algorithm, because that one fact has widespread connotations. It is actually a very simple fact: If $d|a$ and $d|b$, then $d|(ax + by)$, where x and y are integers. In particular: $d|a, b \Rightarrow d|(a - b)$. We can apply this fact in many clever ways. One thing to do is to find the gcd. Clearly $(a, b)|a$ and $(a, b)|b$. Well at each step we have two numbers, starting with a and b . We want to subtract the smaller number from the larger number and keep the two smallest numbers of the three. Notice that the gcd still divides both of these numbers since $(a, b)|(a - b)$. We continue this process until we get to the fact that the gcd divides zero and some other number. Notice however that euclid's algorithm works backward too. That is to say, anything that divides both of these numbers will also divide the original two numbers. Thus, the gcd of the pair of numbers never changes. The gcd of zero and the last number must therefore be the last number. That last number is the gcd of a and b . This is known as Euclid's algorithm and even though it is slower than the prime factorization method in a lot of small cases, often times it is much harder to factor large numbers.

2.4 Prime Stuff

Here are some quick facts that sometimes come up.

1. **Infinitely many Primes** Exactly as it sounds like. There are a bajillion proofs of this out there. However, the classic one is still assuming there is a finite set of them a_1, a_2, \dots, a_n . Now consider the number $(a_1)(a_2) \dots (a_n) + 1$. What prime divides this number?
2. **Bertrand's Postulate** These things have such funny names. This has been proven already, it is no longer a postulate. It basically states that there is always a prime between n and $2n$.
3. **Dirichlet's Theorem** Not only are there infinitely many primes, but there are infinitely primes in any reasonable arithmetic sequence of integers. (No, there aren't infinitely many primes in the sequence $2, 4, 6, \dots$.) I guess I should specify that reasonable means $(a, d) = 1$, where a is the first term and d is the common difference). Most of the time, this is useful just to ensure there is one such prime.

4. **Prime Number Theorem** This is actually probably never going to be applicable, but it is a triumph of number theory and has to do with primes. There are quite a few open conjectures having to do with primes out there: twin primes conjecture, riemann hypothesis, etc. However, this is one we've actually proven! What it says is that the number of primes less than or equal to x approaches $\frac{x}{\ln x}$ as x goes to infinity.

Primes become more special when we learn about mods and are special all over the place such as in group theory and other things.

2.5 Some other systems

2.5.1 Gaussian Integers - $\mathbb{Z}[i]$

The Gaussian Integers are interesting because they have division too! The statement is almost exactly the same: Given $a, b \in \mathbb{Z}[i]$, $\exists q, r \in \mathbb{Z}[i]$ s.t. $a = bq + r$ and $|r| < |b|$. You'll notice that division can always be stated in this way, as long as we have some way of comparing the sizes of r and b . In this case, we use the norm in the complex sense $|a + bi| = \sqrt{a^2 + b^2}$. We can do all of the stuff we did in the integers with the Gaussian integers now! This includes the fundamental theorem of arithmetic, with primes being defined as any numbers whose only factors are units and unit multiples of itself and who are not units themselves. A unit is any number with a multiplicative inverse, namely $1, -1, i, -i$. Gaussian integers allow us to prove a couple of quick things about integers.

1. The sums of two squares is multiplicative: $(a^2 + b^2)(c^2 + d^2) = (ac - bd)^2 + (ad + bc)^2$
This is easily proven just by showing that norms are multiplicative in the Gaussian integers. In this way we realize that we can always rewrite the product of two sums of squares as one sum of squares.
2. Using other Gaussian integer trickery, we get a result due to Fermat. Let p be an odd prime, p can be expressed as a sum of squares iff $p \equiv 1 \pmod{4}$.
3. Combining the last two things and the fact that $2 = 1^2 + 1^2$, we can figure exactly which positive integers can be expressed as the sum of two squares. To check if a positive integer n can be expressed as the sum of two squares, we divide out all powers of two and prime factors congruent to one mod four. What we have left must be a perfect square.

2.5.2 Quaternions

I just wanted to mention them. They are essentially numbers of the form $a + bi + cj + dk$ where a, b, c, d are all real numbers. Also, addition is component wise but multiplication is no longer quite commutative. We have that $i^2 = j^2 = k^2 = ijk = -1$. From this we can derive the usual stuff. In fact quaternions are quite important for 3-d graphics. Where do you think the the i, j, k unit vectors come from? By imposing restrictions on a, b, c, d (I don't remember if they have to be integers or something else, but it is chosen so that

division and therefore the fundamental theorem still hold). We can use the same ideas as we used to prove the two squares stuff with the Gaussian integers and prove the Legendre's four squares theorem. This theorem states that all positive integers can be expressed as the sum of four squares. I will also quickly mention a theorem due to Gauss, even though I don't know where it comes from: $n = a^2 + b^2 + c^2$ iff $n \neq (8k + 7)4^m$.

2.5.3 Polynomials

3 Modular Arithmetic

4 Special Functions

5 Diophantine Equations

6 Tricks of the Trade

These were taken word for word from Melanie Wood's MOSP lecture.

1. Plug in simple cases.
2. Check in modulo m , where m is carefully chosen.
3. Consecutive numbers are relatively prime.
4. If $p|a$ and $p|b$, $p|a + b$ and $p|a - b$
5. Divide into multiple cases.
6. Consider the order of k modulo m .
7. Go back and forth between writing $a \equiv b \pmod{n}$ and $n|a - b$.
8. Don't be afraid to use the quadratic formula.
9. Infinite Descent
10. Factoring
11. Build large numbers with the properties you want.
 - Chinese Remainder Theorem (CRT)
 - Always large enough primes (even in reasonable arithmetic progressions)
12. A rational is an integer if

- every prime power that divides the denominator divides the numerator.
- it is rational and the root of a monic polynomial with integer coefficients.
- it is the answer to a counting problem
- it is a term in a recursive sequence with integer initial values and integer coefficients

7 Acknowledgements and Other Reading

All of this is compiled from two summers at the Ross math program and MOSP lectures. If you want to learn more, Naoki Sato has a much more comprehensive lecture online at www.artofproblemsolving.com in the resources and articles section.

8 Unsolved Problems

If you are working on a problem and your proof relies on one of these, you should probably reconsider it.

9 Practice