TJUSAMO Practice #4: Basic Number Theory

HMao

August 19th, 2006

Number theory is one of the four major topics of math olympiads. Unfortunately, most school curricula do not cover number theory at all, leaving many people clueless about the subject. In general, number theory is the study of the integers and their properties. This article will go over the theorems and concepts of number theory everyone absolutely must know to get anywhere in number theory, as well as provide some practice.

1 Modular Arithmetic

Mods should naturally spring to mind while working with number theory. Basically, "$a \pmod{b}$" is the remainder when a is divided by b. For all integers $n > 1$, we say that modulo n is a "congruence class." You don't really need to know the technicalities of the definition of a congruence class for now. Basically, we have $a \equiv a+kn \pmod{n}$ for all integers k.

Here are several warmups:

1. Evaluate $8+53+312987236982365189235638216537821582568713459713445 \pmod 5$.
2. Evaluate $(8+53)^{312987236982365189235638216537821582568713459713445} \pmod 5$.
3. Evaluate $(1+2+3+4+5+6+7+8+9+10+11+13+14+15+16+17+18+19+20)^{312987236982365189235638216537821582568713459713445^{55555}} \pmod{11}$.
4. Find all values of $\sqrt[3]{6} \pmod 7$.
5. Evaluate $4^{4^{4^4}} \pmod{10}$.

2 Five Theorems

These theorems should be second nature to you.

2.1 Euler's Theorem

For any two relatively prime integers $n > 2$ and a,

$$a^{\phi(n)} \equiv 1 \pmod{n}.$$

Note that $\phi(n)$ is defined as the number of naturals less than n and relatively prime to n.

If n is a prime, we have the subsidiary Fermat's Little Theorem, which states that

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

2.2 Wilson's Theorem

For any prime p,

$$(p-1)! \equiv -1 \pmod{p}.$$

2.3 Chinese Remainder Theorem

If an integer has a certain residue in certain prime mods, then it has a unique residue in the mod that is the product of those prime mods.

2.4 Dirichlet's Theorem

For any relatively prime naturals a and b , there are an infinite number of primes that are congruent to $a \pmod{b}$

2.5 Bertrand's Postulate

For every real $n > 1$, there is at least one prime number p such that $n < p < 2n$. This interesting result has been proven, and is more accurately named Chebyshev's Theorem. Some people mistakenly call this Bernard's Postulate.

3 Diophantine Equations

A very common type of number theory problem in many math olympiads is the diophantine equation(DE). This is any equation in which the solution set is comprised of only integers. Generally, a problem will present a system of diophantine equations and ask you to find all the solutions, and prove that you have found every one of them.

3.1 How to write the a DE solution

There are three steps to writing a solution to a DE problem:

3.1.1 Write the answers

Before writing anything else, simply state all the solutions. You can use variables to do this. For example, if you had to write solutions to the DE $x + y = 0$, you could write $(n, -n)$ for $n \in Z$.

3.1.2 Show that your answers all work

You can usually get away with saying "It is trivial to show that these answers satisfy the given equation(s)." This step could even be omitted if it is really obvious.

3.1.3 Prove that you have given all the answers

This is by far the hardest step. Here, you have to prove that there are no answers you have not found. You will have to use some number theory to do this.

3.2 Methods for solving DEs

If you are stuck, try using the techniques on this list.

1. Play around with the DE.
2. Take the equation(s) in some mod. Mod 2 is a good starting point. If you see a n-th power, try using mod n+1 or mod 2n+1. If you see squares, also try mod 4 and mod 8. If you see cubes, try mod 8, or mod 9. If you see fourth powers, try mod 16. Sometimes the key step to a problem is finding the right mod.
3. Try to factor anything, including constants and coefficients.
4. Guess and check to find solutions.
5. Impose an extra condition. For example, if the DE is symmetrical, WLOG $a \geq b \geq c$ Don't forget to state all the answers.
6. Don't forget negative numbers and 0. Often 0 is a special case.
7. Can you show that there cannot be any solutions if one of the variables approaches infinity?
8. Make a substitution, but try to keep stuff in the integers.
9. WOP and infinite descent often work together with mods to solve a problem.
10. Find an upper or lower bound for one of the variables.
11. Think about what theorems might be applicable to the problem, and try to use them.
12. Think about what would happen if one of the variables was prime.
13. Work on another problem for a while.
14. Assume the guy next to you has already solved the problem, and think about what he could have done.
15. Revisit some of the previous progress you made and try to build off of it.
16. Start over; pretend you have never seen the problem yet.

3.3 Classics

There are some diophantine equations you just have to know. Here they are for you to absorb.

3.3.1 Pythagorean Triples

The positive solutions to the DE $a^2 + b^2 = c^2$ are $(2mn, m^2 - n^2, m^2 + n^2)$ and $(m^2 - n^2, 2mn, m^2 + n^2)$ for relatively prime integers $m > n$.

3.3.2 Fermat's Last Theorem

There are no positive solutions to the DE $a^n + b^n = c^n$ for any integer $n > 2$.

3.3.3 Pell's Equation

If (m, n) is the smallest solution(minimum $m + n$) to the positive DE $a^2 - b^2c = 1$, where c is a fixed natural that is not a perfect square, then all solutions (x, y) satisfy the identity

$$x + y\sqrt{c} = (m + n\sqrt{c})^z$$

for some natural z, and every natural z generates one solution.

Some people think this is common, but I've rarely seen it used in a problem, if ever.

4 Problems

I challenge you to solve ALL of the following 15 problems by the time the advanced number theory lecture rolls around. I know you have enough time to do this, and you are welcome to ask me for help. All of the problems can be solved by things you should know. If you give up, you are a noob. If you succeed, then you will be ready for the next level...

1. {1.5} Prove Wilson's theorem.
2. {2.5} Prove Euler's theorem.
3. {1} [IMO 1959] For natural n, prove that $\frac{21n+4}{14n+3}$ is irreducible.
4. {1.5} (DE) Solve across naturals:

$$a^2 + b^2 + c^2 + 1 = (a + b + c)!$$

5. {1.5} [Leningrad 1984] Find all prime unordered pairs (a, b) such that $a^b + b^a$ is prime.
6. {1.5} [MOP '05] N is a number with has exactly 3^n digits. If these digits are all equal, prove that N is divisible by 3^n.
7. {1.5} [USAMO 1979] Solve across the nonnegative integers:

$$n_1^4 + n_2^4 + \cdots + n_{14}^4 = 1599$$

8. {2} [USAMO 1972] (In this problem, parenthesis denote GCD and brackets denote LCM) Prove that for all naturals a, b, c,

$$\frac{[a,b,c]^2}{[a,b][a,c][b,c]} = \frac{(a,b,c)^2}{(a,b)(a,c)(b,c)}$$

9. {2} [USAMO 1976] (DE) Solve:

$$a^2 + b^2 + c^2 = a^2b^2$$

10. {2} (For any natural n, the nth Fermat number is $2^{2^n} + 1$) Find all Fermat numbers that are also perfect cubes.

11. {2.5} (DE) Solve:

$$a^4 + b^4 + c^4 + d^4 + e^4 = 2^m - 7^n$$

12. {2.5} Prove that for every n, there are an infinite number of Fibonacci numbers that are divisible by n.

13. {2.5} [IMO SL 2005] Find the smallest number n such that there exist n cubes that add up to 2002^{2002}.

14. {3} [IMO 1998] Find all ordered pairs of integers (a, b) such that

$$ab^2 + b + 7 \mid a^2b + a + b$$

15. {3.5} [USAMO 2005] (DE) Prove that there are no solutions to the following system:

$$x^6 + x^3 + x^3y + y = 147^{157}$$

$$x^3 + x^3y + y^2 + y + z^9 = 157^{147}$$

5 Jacob's Final Problem

One more!

16. {4} [IMO SL 2002] Does the equation $\frac{1}{a} + \frac{1}{b} + \frac{1}{c} + \frac{1}{abc} = \frac{m}{a+b+c}$ have infinitely many solutions in positive integers a, b, c for any positive integer m?