TJUSAMO - Number Theory 1

Sohail Farhangi, Victoria Xia

October 22nd, 2012

The goal of these number theory lectures is to make sure you have all the basic tools you'll likely need to tackle number theory questions, and then from there it's just practice and exposure to lots of different techniques and problems.

1 Common Tricks to Get You Started

- You should already be comfortable with manipulating moduli, the division algorithm, Fermat's Little Theorem, Euler's Totient (Phi) Function, and GCDs and LCMs.
- Express everything you know algebraically. If you conclude a number is odd, write it as $2m + 1$.
- Factor, factor, factor. I don't know why, but difference of squares is impossibly overused.
- If some equality holds, then the equality must hold in any modulus you pick. This is particularly useful for diophantine equations.

  Example 1: Find all integer solutions (a, b) to the equation $3^a - 2^b = 1$.
- Integers are cool. Fractions... sometimes are, but often aren't. Clear them if they're annoying you.
- If you know an integer x is greater than the integer m, then $x \geq m + 1$.
- Primes are your friends. Take advantage of their properties whenever you can. Remember that all positive integers, with the exception of 1, have at least one prime factor.

  Example 2: Let a, b, c be positive integers. Prove that if the numbers $\frac{a^2}{a+b}, \frac{b^2}{b+c}, \frac{c^2}{c+a}$ are all integers and primes, then $a = b = c$.
- Consider specific primes or prime-factorizations.

  Example 3: Show that the sum $\frac{1}{m} + \frac{1}{m+1} + \cdots + \frac{1}{m+n}$ is not an integer for any given positive integers m and n.
- Primes are infinite, so you can always find one as large as you'd like. (See problem 6.)
- When you can't get primes, relatively prime is the next best thing. Often times you can divide out the gcd of two numbers to make the remainder relatively prime.
- The Euclidean Algorithm: If $n = mq + r$, then $\gcd(n, m) = \gcd(m, r)$.

  Example 4: Two players take turns playing a game. They start with two distinct positive integers written on a board. At each turn, the player may take the positive difference of any two integers on the board and write that difference on the board, as long as it is not already there. If the winner is the last player who can legally move, which player has a winning strategy?

- Bezout's Identity: There exist integers x and y such that $ax + by = \gcd(a, b)$ for any integers a and b.
- Induction is often helpful to extend results to multiple variables. (For example, show that there exist integers $x_1, x_2, ...x_k$ such that $a_1x_1+a_2x_2+\cdots+a_kx_k = \gcd(a_1, a_2, ..., a_k)$ for any integers $a_1, a_2, ..., a_k$.)

2 Practice Problems

2.1 Not-So-Difficult Ones

1. Find all pairs of positive integers (x, y) for which $x^2 - y! = 2001$.
2. Determine all nonnegative integer solutions to $x_1^4 + x_2^4 + \cdots + x_{14}^4 = 1599$.
3. Let $x_1, x_2, x_3, ...$ be a sequence defined by $x_1 = 4$ and $x_{n+1} = x_1x_2x_3\cdots x_n + 5$ for $n \geq 1$. Find all pairs of positive integers $\{a, b\}$ such that x_ax_b is a perfect square.
4. Find all pairs of positive integers (m, n) such that $\phi(mn) = \phi(m) + \phi(n)$.
5. The primes p and q satisfy $\frac{p}{p+1} + \frac{q+1}{q} = \frac{2n}{n+2}$ for some positive integer n. Find all possible values of $p - q$.

2.2 Somewhere In Between

6. For any positive integers n and k, let $L(n, k)$ be the least common multiple of the k consecutive integers $n, n+1, ..., n+k-1$. Show that for any integer b, there exist integers n and k such that $L(n, k) > bL(n+1, k)$.
7. Do there exist positive integers m, n such that $m^{20} + 11^n$ is a perfect square?
8. Let $n_1, ..., n_k$ be positive integers, and let $d_1 = 1$ and $d_i = \frac{\gcd(n_1,...,n_{i-1})}{\gcd(n_1,...,n_i)}$ for $2 \leq i < k$. Prove that all the sums $\sum_{i=1}^{k} a_in_i$, with $a_i \in \{1, 2, ..., d_i\}$ are mutually distinct modulo n_1.

2.3 Not-So-Easy Ones

9. Find all pairs of prime numbers p, q such that $p^2 - p - 1 = q^3$.
10. Find all functions $f : \mathbb{N} \to \mathbb{N}$ such that $f(m) - n$ divides $m^2 - f(n^2)$ for any positive integers m, n as long as $f(m) \neq n$.
11. Determine which rational numbers can be expressed in the form $\frac{a^p+b^q}{c^r+d^t}$ for given pairwise relatively prime positive integers p, q, r, t and any integers a, b, c, d.