Classical Number Theory

Reid Barton

Black Lecture, July 1, 2004

Tools & Ideas

Inequalities

In order to prove that a number doesn't belong to some set S, prove that it lies between two consecutive elements of S. Divisibility relations imply order relations (but watch out for signs and zero).

Root-flipping

Let $P(x, y)$ be a quadratic polynomial in two variables, and suppose we have a pair of integers (a, b) such that $P(a, b) = 0$. Then we can find new pairs (a', b) and (a, b') by using sum-of-roots or product-of-roots formulas on the quadratics $P(x, b)$ and $P(a, y)$ with the known roots a and b respectively. This can be useful either in a descent proof or as a construction of infinitely many solutions to an equation. The sequences of pairs (a_n, b_n) generated by this approach usually satisfy some kind of linear recurrence.

Pell Equations

An equation of the form $x^2 - Dy^2 = \pm 1$, with D not a square, is called a Pell equation. The best way to think about this is to view $x^2 - Dy^2$ as the norm of the element $x + \sqrt{D}y$ of $\mathbb{Z}(\sqrt{D})$. Since the norm is multiplicative, given two solutions (x_1, y_1) and (x_2, y_2), we can find a new solution (x_3, y_3) by

$$x_3 + \sqrt{D}y_3 = (x_1 + \sqrt{D}y_1)(x_2 + \sqrt{D}y_2).$$

So once we find a single nontrivial solution, we can find infinitely many by raising it to powers. The corresponding pairs (x_i, y_i) satisfy a linear recurrence. This is the most common use for Pell equations on olympiad problems. On a more theoretical level, it can be useful to know that the equation $x^2 - Dy^2 = 1$ always has a nontrivial solution (assuming D is not a square). However, for some values of D, $x^2 - Dy^2 = -1$ has no nontrivial solutions. Warning: It is not necessarily the case that all solutions are generated by powers of a single fundamental solution!

Modular Arithmetic

When faced with a Diophantine equation, one good first step is to consider the possible values of the variables modulo some small number. Try 8, 9, and any m such that $d \mid \varphi(m)$ if the problem involves dth powers. Sometimes you need a variable modulus, but this starts to get into the next category.

Congruential Number Theory

The main tool in solving problems involving congruencies is an understanding of the structure of the ring $\mathbb{Z}/m\mathbb{Z}$, which we denote by $\mathbb{Z}_m$ for convenience. We use $\mathbb{Z}_m^*$ for the group of units in $\mathbb{Z}_m$ (residues relatively prime to m).

- By the Chinese Remainder Theorem, the ring $\mathbb{Z}_m$ is the direct sum of the rings $\mathbb{Z}_{p^k}$ over prime powers p^k appearing in the prime factorization of m.
- Primitive roots exist in $\mathbb{Z}_{p^k}$ for p an odd prime, so the group $\mathbb{Z}_{p^k}^*$ is isomorphic to the group $\mathbb{Z}_{\varphi(p^k)}$.
- Let a be a unit in $\mathbb{Z}_{p^k}$ and let d be its order modulo p^k. Then $a^t \equiv 1 \pmod{p^k}$ iff d divides t. In particular, d divides $\varphi(p^k) = p^{k-1}(p-1)$.
- Let p an odd prime and $k \geq 1$. For integers a, $b \perp p$, $a \equiv b \pmod{p^k}$ iff $a^p \equiv b^p \pmod{p^{k+1}}$.

Quadratic Residues

The Legendre symbol $\left(\frac{a}{p}\right)$ is defined when p is an odd prime as

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{if } p \mid a \\ 1 & \text{if } p \nmid a \text{ and } a \text{ is a square modulo } p \\ -1 & \text{if } p \nmid a \text{ and } a \text{ is not a square modulo } p. \end{cases}$$

It satisfies the identites

$$\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}, \quad \left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right),$$

$$\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2} = \begin{cases} 1 & \text{if } p \equiv 1 \pmod 4 \\ -1 & \text{if } p \equiv 3 \pmod 4 \end{cases}, \quad \left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8} = \begin{cases} 1 & \text{if } p \equiv 1 \text{ or } 7 \pmod 8 \\ -1 & \text{if } p \equiv 3 \text{ or } 5 \pmod 8 \end{cases},$$

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

the last of which is known as quadratic reciprocity.

Pythagorean Triples

If a, b, c are relatively prime positive integers with $a^2 + b^2 = c^2$, then without loss of generality a is odd and b is even, and there exist positive integers u and v such that $a = u^2 - v^2$, $b = 2uv$, and $c = u^2 + v^2$. You can also solve the equation $a^2 + b^2 = 2c^2$ by substituting $a = x + y$, $b = x - y$.

Infinite Descent

The classic example of infinite descent is the proof that $x^4 + y^4 = z^4$ has no solutions in nonzero integers, but infinite descent can also come up in problems involving modular arithmetic (e.g., show all variables are even and then divide by 2) or root-flipping.

Unique Factorization

Some rings of algebraic integers besides $\mathbb{Z}$ have the unique factorization property, the most useful being the Gaussian integers $\mathbb{Z}[i]$ and the ring $\mathbb{Z}[\omega]$ where $\omega = e^{2\pi i/3} = \frac{-1+\sqrt{3}i}{2}$. You need to be careful, though, because

- many similar rings do not have unique factorization ($\mathbb{Z}[\sqrt{5}i]$, for example);
- factorization is only unique up to units, and there are a lot of units (± 1 and $\pm i$ in $\mathbb{Z}[i]$, and ± 1, $\pm\omega$, $\pm(\omega + 1)$ in $\mathbb{Z}[\omega]$);
- it can be tricky to check that two elements of $\mathbb{Z}[i]$ or $\mathbb{Z}[\omega]$ are relatively prime;
- primes in $\mathbb{Z}$ are not necessarily prime in $\mathbb{Z}[i]$ or $\mathbb{Z}[\omega]$. In fact, the primes in $\mathbb{Z}$ that remain prime in $\mathbb{Z}[i]$ are exactly the primes of the form $4k + 3$.

Random Facts

- Dirichlet's Theorem: Any arithmetic progression of positive integers contains infinitely many primes, unless all of its terms have a common factor.
- Lucas's Theorem: $\binom{a}{b} \equiv \binom{a_k}{b_k} \cdots \binom{a_0}{b_0} \pmod p$ where $a_k \cdots a_0$ and $b_k \cdots b_0$ are the base-p representations of a and b.
- Wilson's Theorem: $(p-1)! \equiv -1 \pmod p$ for any prime p.
- Wolstenholme's Theorem: $\binom{2p}{p} \equiv 2 \pmod{p^3}$ for any prime $p \geq 5$.

Problems

All of these problems are from 1998–2003 IMO short lists, so you should already know how to solve them.

1. What is the smallest positive integer t such that there exist integers x_1, x_2, $\ldots$, x_t with
$$x_1^3 + x_2^3 + \cdots + x_t^3 = 2002^{2002}?$$

2. Let b be an integer greater than 5. For each positive integer n, consider the number
$$x_n = \underbrace{11\ldots1}_{n-1}\underbrace{22\ldots2}_{n}5,$$
written in base b. Prove that the following condition holds if and only if $b = 10$:

   There exists a positive integer M such that for any integer n greater than M, the number x_n is a perfect square.

3. Determine all pairs of positive integers (a, b) such that $ab^2 + b + 7$ divides $a^2b + a + b$.

4. Determine all pairs of positive integers (a, b) such that
$$\frac{a^2}{2ab^2 - b^2 + 1}$$
is a positive integer.

5. Is there a positive integer n such that the equation
$$\frac{1}{a} + \frac{1}{b} + \frac{1}{c} + \frac{1}{abc} = \frac{m}{a + b + c}$$
has infinitely many solutions in positive integers a, b, c?

6. Prove that there are infinitely many positive integers n such that $p = nr$, where p and r are respectively the semiperimeter and the inradius of some triangle with integer side lengths.

7. Find all pairs (n, p) of positive integers such that p is prime, $n \leq 2p$, and n^{p-1} divides $(p-1)^n + 1$.

8. Let p_1, p_2, $\ldots$, p_n be distinct primes greater than 3. Show that $2^{p_1p_2\cdots p_n} + 1$ has at least 4^n divisors.

9. Determine if there exists a positive integer n such that n has exactly 2000 prime divisors and $2^n + 1$ is divisible by n.

10. Let p be a prime number. Prove that there exists a prime number q such that for every integer n, the integer $n^p - p$ is not divisible by q.

11. Let $p \geq 5$ be a prime number. Prove that there exists an integer a with $1 \leq a \leq p-2$ such that neither $a^{p-1} - 1$ nor $(a+1)^{p-1} - 1$ is divisible by p^2.

12. For a positive integer n, let $d(n)$ be the number of all positive divisors of n. Find all positive integers n such that $d(n)^3 = 4n$.

13. Consider the system
$$\begin{aligned} x + y &= z + u \\ 2xy &= zu. \end{aligned}$$
Find the greatest value of the real constant M such that $m \leq x/y$ for any positive integer solution (x, y, z, u) of the system, with $x \geq y$.

14. Determine all triples of positive integers (a, m, n) such that $a^m + 1$ divides $(a+1)^n$.

15. Let $a > b > c > d$ be positive integers and suppose $a^2 - ac + c^2 = b^2 + bd + d^2$. Prove that $ab + cd$ is not prime.

Homework

1. Let n be an integer greater than 1, and let

$$p(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + 1$$

be a polynomial with nonnegative integer coefficients such that $a_j = a_{n-j}$ for $1 \leq j \leq n-1$. Prove that there exist infinitely many pairs of positive integers (a, b) such that $a \mid p(b)$ and $b \mid p(a)$.

2. (MOP 00) Find the number of zeros at the end of the number

$$4^{5^6} + 6^{5^4}.$$

3. (Putnam 97/B5) Define $a_1 = 2$, $a_n = 2^{a_{n-1}}$ for $n \geq 2$. Prove that $a_{n-1} \equiv a_n \pmod{n}$.

4. (Putnam 99/A6) Define the sequence $\{a_i\}_{i \geq 1}$ by

$$a_1 = 1, \quad a_2 = 2, \quad a_3 = 24, \quad a_n = \frac{6a_{n-1}^2 a_{n-3} - 8a_{n-1}a_{n-2}^2}{a_{n-2}a_{n-3}}.$$

Show that a_n is divisible by n for each n.

5. (APMO 97/2) Find an integer n, $100 \leq n \leq 1997$, such that n divides $2^n + 2$.

6. (IMO 90/3) Find all positive integers n such that n^2 divides $2^n + 1$.

7. (Putnam 94/B6) For each nonnegative integer i define $n_i = 101i + 100 \cdot 2^i$. If $0 \leq a, b, c, d \leq 99$ and $n_a + n_b \equiv n_c + n_d \pmod{10100}$, show that $\{a, b\} = \{c, d\}$.

8. (MOP 95?) If a positive integer n is a square mod p for every prime p, must n be a square number?

9. (Bulgaria 96) Find all pairs of primes (p, q) such that $pq \mid (5^p - 2^p)(5^q - 2^q)$.

10. (Romania 96) Find all pairs of primes (p, q) such that $\alpha^{3pq} \equiv \alpha \pmod{3pq}$ for any integer α.

11. (Russia 96) Suppose that p is a odd prime, $n > 1$ is an odd number, and x, y, k are positive integers such that $x^n + y^n = p^k$. Prove that n is a power of p.

12. (Russia 96) Find all integers k such that there exist an integer $n > 1$ and relatively prime integers x, y such that $x^n + y^n = 3^k$.

13. (Russia 00) Do there exist pairwise relatively prime integers a, b, $c > 1$ such that $a \mid 2^b + 1$, $b \mid 2^c + 1$, and $c \mid 2^a + 1$?

14. (MOP 98) Let p be a prime congruent to 3 mod 4, and let a, b, c, d be integers such that

$$a^{2p} + b^{2p} + c^{2p} = d^{2p}.$$

Show that p divides abc.

15. (USA 03) Find all ordered triples of primes (p, q, r) such that

$$p \mid q^r + 1, \qquad q \mid r^p + 1, \qquad r \mid p^q + 1.$$

16. Determine all ordered triples of integers (x, y, z) with $x \neq 0$ such that

$$2x^4 + 2x^2y^2 + y^4 = z^2.$$