Number Theory

Thomas Mildorf

Black Lecture, June 14, 2011

Let $\mathbb{Z}_m$ denote the ring $\mathbb{Z}/m\mathbb{Z}$, and let $\mathbb{Z}_m^*$ denote its group of units (residues relatively prime to m).

- (Fermat) If p is a prime, then $x^p - x = x(x-1)\cdots(x-(p-1))$ in $\mathbb{Z}_p[x]$.
- (Euler) Let $m \geq 2$ be an integer. Then $a^{\phi(m)} = 1$ for all $a \in \mathbb{Z}_m^*$.
- (Sun Tzu) Suppose $p_1^{k_1}\cdots p_n^{k_n}$ is the prime factorization of m. Then $\mathbb{Z}_m = \mathbb{Z}_{p_1^{k_1}} \times \cdots \times \mathbb{Z}_{p_n^{k_n}}$.
- (Primitive Root) Let p and k be an odd prime and a positive integer. Then the group $\mathbb{Z}_{p^k}^*$ is cyclic.
- (Quadratic Residues) When p is an odd prime number and a is an integer, the Legendre symbol $\left(\frac{a}{p}\right)$ is defined to be 0 if $p \,|\, a$, 1 if a is a square modulo p, and -1 otherwise. It has many properties:

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

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

$$\left(\frac{q}{p}\right) = (-1)^{(p-1)(q-1)/4}\left(\frac{p}{q}\right) \qquad \text{(Quadratic Reciprocity)}$$

- (Pythagorean Triples) The primitive triples a, b, c of positive integers such that $a^2 + b^2 = c^2$ can be expressed as $m^2 - n^2, 2mn, m^2 + n^2$ where m and n are positive integers.
- (Pell's Equation) Let D be positive integer that is not a perfect square. Then the equation $m^2 - Dn^2 = 1$ has the following solutions (m, n) in nonnegative integers: the trivial solution $(1, 0)$ and an infinite family $\{(m_i, n_i)\}_{i\geq 1}$ generated as

$$m_i + n_i\sqrt{D} = (m_1 + n_1\sqrt{D})^i$$

  where (m_1, n_1) is the *fundamental solution,* i.e. the one with the minimal positive n. The related equation $m^2 - Dn^2 = -1$ may not have nontrivial solutions; if it does, infinitely many (but *not* necessarily all) solutions can be generated in a similar fashion.
- (Dirichlet) An arithmetic progression of integers contains infinitely many primes, unless all of its terms share a common divisor greater than 1.
- (Lucas) $\binom{a}{b} \equiv \binom{a_k}{b_k}\cdots\binom{a_0}{b_0} \pmod{p}$, where $a_k a_{k-1}\cdots a_0$ and $b_k b_{k-1}\cdots b_0$ are the base p representations of a and b.
- (Wolstenholme) $\binom{ap}{bp} \equiv \binom{a}{b} \pmod{p^3}$ for any prime $p \geq 5$.

Suppose the positive integers are partitioned into k subsets $N_1, \ldots, N_k$.

- (Van der Waerden) There exist arbitrarily long arithmetic progressions in some subset N_i.
- (Folkman) There exist arbitrarily large sets S such that the sum of every nonempty subset of S belongs to some N_i.

Problems

All of the following problems are from 2000-2007 IMO short lists, so you should already know how to solve them.

1. Let $\tau(n)$ denote the number of positive divisors of the positive integer n. Prove that there exist infinitely many positive integers a such that the equation
$$\tau(an) = n$$
does not have a positive integer solution n.

2. Determine all positive integers $n \geq 2$ that satisfy the following condition:
for all integers a, b relatively prime to n,
$$a \equiv b \pmod{n} \quad \text{if and only if} \quad ab \equiv 1 \pmod{n}.$$

3. Determine all pairs (x, y) of integers such that
$$1 + 2^x + 2^{2x+1} = y^2.$$

4. Determine all positive integers relatively prime to all terms of the infinite sequence $a_n = 2^n + 3^n + 6^n - 1\,(n = 1, 2, 3, \ldots)$.

5. Find all pairs of natural numbers (a, b) satisfying $7^a - 3^b$ divides $a^4 + b^2$.

6. Let $b, n > 1$ be integers. Suppose that for each $k > 1$ there exists an integer a_k such that $b - a_k^n$ is divisible by k. Prove that $b = A^n$ for some integer A.

7. For $x \in (0, 1)$ let $y \in (0, 1)$ be the number whose n-th digit after the decimal point is the 2^n-th digit after the decimal point of x. Show that if x is rational, then so is y.

8. Let $a_1, a_2, \ldots$ be a sequence of integers with infinitely many positive and negative terms. Suppose that for every positive integer M the numbers $a_1, a_2, \ldots, a_M$ leave different remainders upon division by M. Prove that every integer occurs exactly once in the sequence $a_1, a_2, \ldots$.

9. Let a, b, c, d, e and f be positive integers. Suppose that the sum $S = a + b + c + d + e + f$ divides both $abc + def$ and $ab + bc + ca - de - ef - fd$. Prove that S is composite.

10. Does there exist a positive integer n such that n has exactly 2000 prime divisors and $2^n + 1$ is divisible by n?

11. Let X be a set of 10,000 integers, none of them divisible by 47. Prove that there exists a 2007-element subset Y of X such that $a - b + c - d + e$ is not divisible by 47 for any $a, b, c, d, e \in Y$.

12. We define a sequence $(a_1, a_2, a_3, \ldots)$ by setting
$$a_n = \frac{1}{n}\left(\left[\frac{n}{1}\right] + \left[\frac{n}{2}\right] + \cdots + \left[\frac{n}{n}\right]\right)$$
for every positive integer n. By $[x]$ we mean the integral part of x, the greatest integer which is less than or equal to x.

13. Determine all pairs of positive integers (a, b) such that
$$\frac{a^2}{2ab^2 - b^3 + 1}$$
is a positive integer.

14. Let k be a fixed integer greater than 1, and let $m = 4k^2 - 5$. Show that there exist positive integers a and b such that the sequence (x_n) defined by

$$x_0 = a, \quad x_1 = b, \quad x_{n+2} = x_{n+1} + x_n \quad \text{for} \quad n = 0, 1, 2, \ldots,$$

has all of its terms relatively prime to m.

15. For every integer $k \geq 2$, prove that 2^{3k} divides the number

$$\binom{2^{k+1}}{2^k} - \binom{2^k}{2^{k-1}}$$

but 2^{3k+1} does not.

16. Find all positive integers $n > 1$ for which there exists a unique integer a with $0 < a \leq n!$ such that $a^n + 1$ is divisible by $n!$.

17. 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.

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

19. Let $P(x)$ be a polynomial of degree $n > 1$ with integer coefficients and let k be a positive integer. Consider the polynomial $Q(x) = P(P(\ldots P(P(x)) \ldots))$, where P is applied k times. Prove that there are at most n integers t such that $Q(t) = t$.

20. Find all pairs of integers (m, n) such that $m^7 - 1 = (m-1)\left(n^5 - 1\right)$.

21. We call a positive integer *alternative* if its decimal digits are alternately odd and even. Find all positive integers n such that n has an alternative multiple.

22. Let b be an integer greater than 5. For each positive integer n, consider the number

$$x_n = 11 \cdots 122 \cdots 25,$$

having $n-1$ 1's and n 2's, written in base b. Prove that the following 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.

23. Find all surjective functions $f : \mathbb{N} \to \mathbb{N}$ such that for every $m, n \in \mathbb{N}$ and for every prime p, the number $f(m+n)$ is divisible by p if and only if $f(m) + f(n)$ is divisible by p.

24. Let a and b be positive integers such that $a^n + n$ divides $b^n + n$ for every positive integer n. Show that $a = b$.

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

26. Given an integer $n > 1$, denote by P_n the product of all positive integers x less than n and such that n divides $x^2 - 1$. For each $n > 1$, find the remainder of P_n on division by n.

27. Let $a > b > c > d$ be positive integers and suppose

$$ac + bd = (b + d + a - c)(b + d - a + c).$$

Prove that $ab + cd$ is not prime.

28. Let k be a postiive integer. Prove that the number $\left(4k^2-1\right)^2$ has a positive divisor of the form $8kn-1$ if and only if k is even.

29. Let n be a positive integer. Show that there exists a positive integer m such that n divides 2^m+m.

30. Let n be an integer greater than 1 and suppose that $P(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$, where $a_0, \ldots, a_n$ are integers with a_n positive. Prove that there exists a positive integer m such that $P(m!)$ is a composite number.

31. Find all pairs of positive integers $m, n \geq 3$ for which there exist infinitely many positive integers a such that
$$\frac{a^m+n-1}{a^n+a^2-1}$$
is a positive integer.

32. For a prime p and a given integer n let $\nu_p(n)$ denote the exponent of p in the prime factorization of $n!$. Given $d \in \mathbb{N}$ and $\{p_1, p_2, \ldots, p_k\}$ a set of k primes, show that there are infinitely many positive integers n such that $d | \nu_{p_i}(n)$ for all $1 \leq i \leq k$.

33. Let p be an odd prime and n a positive integer. In the coordinate plane, eight distinct points with integer coordinates lie on a circle with diameter of length p^n. Prove that there exists a triangle with vertices at three of the given points such that the squares of its side lengths are integers divisible by p^{n+1}.

34. Let p be a prime number and let A be a set of positive integers that satisfies the following conditions:

    (i) the set of prime divisors of the elements in A consists of $p-1$ elements;

    (ii) for any nonempty subset of A, the product of its elements is not a perfect pth power.

    What is the largest possible number of elements in A?

Homework

1. Does there exist an infinite sequence of positive integers, containing every positive integer exactly once, such that the sum of the first n terms is divisible by n for every n?

2. (Russia 1995) Is it possible for the numbers 1, 2, ..., 100 to be the terms of 12 geometric progressions?

3. (USA 1998) Prove that, for each integer $n \geq 2$, there is a set S of n integers such that ab is divisible by $(a-b)^2$ for all distinct $a, b \in S$.

4. (Inspired by Greece 1996) Determine the smallest number N such that among N positive integers all of whose prime factors are in the set $\{2, 3, 5\}$, there must exist 4 numbers whose product is a perfect fourth power of an integer

5. Find all ordered triples of integers (a, b, c) such that $a^2+b^2 = 2c^2$.

6. (Poland) Let p be a prime and let $S = \{1, 2, \ldots, p\}$. Determine whether there exists a permutation $\sigma : S \to S$ such that the set
$$\left\{\prod_{i=1}^{j} \sigma(i) \,|\, j \in S\right\}$$
gives a complete residue class modulo p.

7. (ISL 1991) Find all pairs of positive integers (x, p) such that p is a prime, $x \leq 2p$ and x^{p-1} is a divisor of $(p-1)^x + 1$.

8. (ISL 1992) Find all integer triples (p, q, r) such that $1 < p < q < r$ and $(p-1)(q-1)(r-1)$ is a divisor of $(pqr - 1)$.

9. (Korea) Suppose that a, b, c are positive integers such that no prime divides all three and such that $a^2 + b^2 + c^2 = 2(ab + bc + ca)$. Prove that a, b, c are perfect squares.

10. A set S of positive integers is called a *finite basis* if there exists some n such that every sufficiently large positive integer can be written as a sum of at most n elements of S. If the positive integers are partitioned into finitely many subsets, must one of them necessarily be a finite basis?

11. (MOP 2000) Find the number of 0's appearing at the end of
$$4^{5^6} + 6^{5^4}.$$

12. The set of all integers is partitioned into finitely many arithmetic progressions. Prove that some two of them have the same common difference.

13. (Putnam 1997/B5) Define $a_1 = 2, a_n = 2^{a_{n-1}}$ for $n \geq 2$. Prove that $n \,|\, a_n - a_{n-1}$.

14. (Putnam 1999/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.

15. (MOP 95?) Suppose a positive integer n is square mod p for all primes p. Must n be a square?

16. (Russia 2001) Find all n such that if a and b are coprime divisors of n then $a + b - 1$ is also a divisor of n.

17. (IMO 1990/3) Find all positive integers n such that n^2 divides $2^n + 1$.

18. (IMO 1995/6) Let p be an odd prime. Determine the number of p-element subsets of $\{1, 2, \ldots, 2p\}$ such that the sum of the elements is divisible by p.

19. (ISL 1992) Does there exist a set M of 1992 positive integers such that the sum of any nonempty subset of the elements is a perfect power (m^k, where $m, k \in \mathbb{Z}^+$ and $k \geq 2$)?

20. (CMO 2007) Show that if n is an integer greater than 1, then $2n - 1$ is prime if and only if for any n distinct positive integers $a_1, a_2, \ldots, a_n$ there exist $i, j \in \{1, 2, \ldots, n\}$ such that
$$\frac{a_i + a_j}{(a_i, a_j)} \geq 2n - 1,$$
where (x, y) denotes the greatest common divisor of x and y.

21. Suppose that $p(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + 1$ is a polynomial with nonnegative integer coefficients such that $a_i = a_{n-i}$ for $i = 1, 2, \ldots, n-1$. Show that there exist infinitely many pairs a, b of positive integers such that $a | p(b)$ and $b | p(a)$.

22. (ISL 1991) Given any integer $n \geq 2$, assume that the integers $a_1, a_2, \ldots, a_n$ are not divisible by n and, moreover, that n does not divide the sum $a_1 + a_2 + \ldots + a_n$. Prove that there exist at least n different sequences $(e_1, e_2, \ldots, e_n)$ consisting of zeros and ones such that $e_1 a_1 + e_2 a_2 + \cdots + e_n a_n$ is divisible by n.

23. (Putnam 1993) Let $x_1, x_2, \ldots, x_{19}$ be positive integers less than or equal to 93. Let $y_1, \ldots, y_{93}$ be positive integers less than or equal to 19. Prove that there exists a (nonempty) sum of some x_i equal to a sum of some y_j.

24. (Bulgaria 1996) Find all pairs of primes (p, q) such that $pq \,|\, (5^p - 2^p)(5^q - 2^q)$.

25. Find all solutions in integers to
$$x^4 + y^4 = z^2.$$

26. (Romania 1996) Find all pairs of primes (p, q) such that $\alpha^{3pq} \equiv \alpha \pmod{3pq}$ for any integer α.

27. (Russia 1996) Suppose that p is an 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.

28. (Russia 2000) Do there exist pairwise relatively prime integers $a, b, c > 1$ such that $a|2^b + 1, b|2^c + 1$, and $c|2^a + 1$?

29. (Erdős) Given $2n - 1$ integers, prove that some n of them have a sum that is divisible by n.

30. (USA TST 2003) Find all ordered triples of primes (p, q, r) such that
$$p|q^r + 1, \qquad q|r^p + 1, \qquad r|p^q + 1.$$

31. Let n be an integer greater than 1, and let $a_1, a_2, \ldots, a_n$ be not all identical positive integers. Prove that there are infinitely many primes p such that p divides $a_1^k + a_2^k + \cdots + a_n^k$ for some positive integer k.

32. Show that for all but finitely many positive integers n we have the inequality
$$\sum_{i=1}^{n} \sum_{j=1}^{n} \gcd(i, j) > 4n^2.$$
(Extra credit: show that 4 can be made arbitrarily large.)

33. Let a, b, and c be positive integers such that the product ab divides the product $c(c^2 - c + 1)$ and the sum $a + b$ is divisible by $c^2 + 1$. Prove that the sets $\{a, b\}$ and $\{c, c^2 - c + 1\}$ coincide.

34. Find all integers n for which there exists an equiangular n-gon whose side-lengths are distinct rational numbers.