Number Theory 1: Mods and Divisibility

Alison Miller

June 9, 2010

(based on handouts of Melanie Wood and other MOP instructors)

Useful facts

1. Divisibility:
   - If $a \mid b$ then $|a| \leq |b|$. Inequalities are useful!
   - Division and GCDs: Euclidean algorithm, $ax + by = k(a, b)$.
   - For any positive integers a and b, we can write $a = cx$, $b = cy$ where $c = (a, b)$ and $(x, y) = 1$.
2. Primes
   - $p \mid ab$ iff $p \mid a$ or $p \mid b$.
   - Unique Factorization.
   - Infinitely many primes.
   - Bertrand's Postulate: there is a prime between n and $2n$ inclusive.
   - Dirichlet's theorem: Infinitely many primes in arithmetic progressions where $(a, d) = 1$.
3. Modular Arithmetic
   - Addition, Subtraction, Multiplication, and Division
   - Multiplicative Inverses & Complete Residue Sets
   - Powers and Fermat's Little Theorem, ϕ and Euler's extension
   - Chinese Remainder Theorem
   - $\mathbb{Z}/p\mathbb{Z}$ is a finite field.
   - $x^2 = -1 \mod p$ has a solution iff $p \equiv 1 \pmod 4$.
   - Quadratic Reciprocity.

Examples

1. Prove that $x^2 + y^2 + z^2 = 7w^2$ has no solutions in integers.

2 (Czech-Polish-Slovak '02)**.** Let n be a positive integer and p a prime such that n divides $p-1$ and p divides $n^3 - 1$. Prove that $4p - 3$ is a square.

3 (ELMO '00)**.** Let a be a positive integer and let p be a prime. Prove that there exists an integer m such that

$$m^{m^m} \equiv a \pmod{p}.$$

4. Let f_n be the nth Fibonacci number. (We use the convention $f_0 = 0$, $f_1 = 1$.) Prove that $\gcd(f_n, f_m) = f_{\gcd(m,n)}$.

Problems

5 (APMO 2002)**.** Find all positive integers a and b such that

$$\frac{a^2+b}{b^2-a} \text{ and } \frac{b^2+a}{a^2-b}$$

are both integers.

6 (Russia '01)**.** Find all primes p and q such that $p + q = (p - q)^3$.

7 (Russia '01)**.** Let a and b be distinct positive integers such that $ab(a+b)$ is divisible by a^2+ab+b^2: Prove that $|a - b| > \sqrt[3]{ab}$.

8 (Bulgaria '07)**.** Let $p = 4k+3$ be a prime number. Find the number of different residues modulo p of $(x^2 + y^2)^2$, where $\gcd(x, p) = \gcd(y, p) = 1$.

9 (MOP 2001)**.** How many ordered quadruples (x, y, z, w) are there with

$$x^2 + y^2 = z^3 + w^3 \pmod{37}?$$

10 (Japan '01)**.** Let p be a prime number and m a positive integer. Show that there exists a positive integer n such that there exist m consecutive zeroes in the decimal representation of p^n.

11 (Bulgaria '01)**.** Let p be a prime number congruent to 3 modulo 4, and consider the equation

$$(p + 2)x^2 - (p + 1)y^2 + px + (p + 2)y = 1.$$

Prove that this equation has infinitely many solutions in positive integers, and show that if $(x, y) = (x_0, y_0)$. is a solution of the equation in positive integers, then $p \mid x_0$.

12. Natural numbers a, b and c are pairwise distinct and satisfy $a|b+c+bc$, $b|c+a+ca$, $c|a+b+ab$. Prove that at least one of the numbers a, b, c is not prime.

13 (Bulgaria 2001)**.** Find all triples of positive integers (a, b, c) such that $a^3 + b^3 + c^3$ is divisible by a^2b, b^2c, and c^2a.

14 (IMO 2000)**.** Determine if there exists a number n such that n has exactly 2000 prime divisors and $2^n + 1$ is divisible by n.

15 (MOP 2004)**.** Let m and n be positive integers such that 2^m divides the number $n(n+1)$. Prove that 2^{2m-2} divides the number $1^k + 2^k + ... + n^k$ for all positive odd integers k with $k > 1$.

16 (CGMO '03)**.** Let n be a positive integer. Prove that at most half the divisors of n have last digit equal to 3.

17. Determine all positive integers n for which there exists an integer m such that $2^n - 1$ is a divisor of $m^2 + 9$.

18. Let $a_1, a_2, \ldots, a_n$ be positive integers. Show that

$$\prod_{i<j} \frac{a_i - a_j}{i - j}$$

is an integer.

19 (IMO 2003)**.** Determine all pairs of positive integers (a, b) such that $\frac{a^2}{2ab^2 - b^3 + 1}$ is a positive integer.

20 (China, 2002)**.** Sequence $\{a_n\}$ satisfies: $a_1 = 3$, $a_2 = 7$, $a_n^2 + 5 = a_{n-1}a_{n+1}$, $n \geq 2$. If $a_n + (-1)^n$ is prime, prove that there exists a nonnegative integer m such that $n = 3^m$.