Congruential Number Theory

Reid Barton

Black & Blue, June 26, 2003

Tools

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 additive 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 not divisible by p, $a \equiv b \pmod{p^k}$ iff $a^p \equiv b^p \pmod{p^{k+1}}$.

Other related facts: quadratic reciprocity and Dirichlet's Theorem.

Warm-ups

1. Find all positive integers m such that $\mathbb{Z}_m$ has a primitive root.
2. (a) Find the smallest integer n with the following property: if p is an odd prime and a is a primitive root modulo p^n, then a is a primitive root modulo every power of p.
   (b) Show that 2 is a primitive root modulo 3^k and 5^k for every positive integer k.
3. (a) Let $\Phi_m(x)$ denote the m^{th} cyclotomic polynomial. Show that for any positive integer n, all prime factors of $\Phi_m(n)$ relatively prime to m are congruent to 1 modulo m. (For example, if $m = 4$, this says that $n^2 + 1$ has no prime factor congruent to 3 modulo 4.)
   (b) Deduce the following special case of Dirichlet's Theorem: For any positive integer m, there are infinitely many primes congruent to 1 modulo m.
4. Determine whether there exist positive integers $n_1, n_2, \ldots, n_k > 1$ such that $n_1 \mid 2^{n_2} - 1$, $n_2 \mid 2^{n_3} - 1$, $\ldots$, $n_{k-1} \mid 2^{n_k} - 1$, $n_k \mid 2^{n_1} - 1$.
5. (Ireland 96) If p is a prime, show that $2^p + 3^p$ cannot be a perfect power.
6. (MOP 02 Homework) Given an odd prime p, find all functions $f : \mathbb{Z} \to \mathbb{Z}$ satisfying the following two conditions:
   - $f(m) = f(n)$ for all $m, n \in \mathbb{Z}$ such that $m \equiv n \pmod{p}$;
   - $f(mn) = f(m)f(n)$ for all $m, n \in \mathbb{Z}$.

Problems

1. (MOP 00) Find the number of zeros at the end of the number
$$4^{5^6} + 6^{5^4}.$$
2. (Putnam 97/B5) Define $a_1 = 2$, $a_n = 2^{a_n - 1}$ for $n \geq 2$. Prove that $a_{n-1} \equiv a_n \pmod{n}$.
3. (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.
4. (IMO 99/4) Find all pairs of positive integers (n, p) such that
   - p is a prime number,
   - $n \leq 2p$, and
   - n^{p-1} divides $(p-1)^n + 1$.
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. (IMO 00/5) Does there exist a positive integer n such that n divides $2^n + 1$ and n has exactly 2000 prime factors?
14. (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 $c \mid 2^a + 1$?
15. (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.
16. Find all ordered triples of primes (p, q, r) such that
$$p \mid q^r + 1, \qquad q \mid r^p + 1, \qquad r \mid p^q + 1.$$