Modular Arithmetic

Robin Park

October 21, 2013

1 Definitions and Notation

We denote the set $\{0, 1, 2, \cdots, n-1\}$ of integers modulo n by $\mathbb{Z}/n\mathbb{Z}$. In particular, if n is a prime p, we denote the set by $\mathbb{F}_p \cong \mathbb{Z}/p\mathbb{Z}$. Throughout this lecture, p will be assumed to be prime. We say that "a is equivalent to b modulo n" if the remainders when a and b are divided by n are equal and denote it by $a \equiv b \pmod{n}$.

2 Integral Mods

In this section, we work in $\mathbb{Z}/n\mathbb{Z}$; that is, the statement $a = b$ in $\mathbb{Z}/n\mathbb{Z}$ is equivalent to the statement $a \equiv b \pmod{n}$ in $\mathbb{Z}$. Addition, subtraction, and multiplication in $\mathbb{Z}/n\mathbb{Z}$ are done similarly as in $\mathbb{Z}$:

Lemma 1. *$\mathbb{Z}/n\mathbb{Z}$ is a commutative ring; that is, $a_n + b_n = (a+b)_n$ and $a_n b_n = (ab)_n$ for $a, b \in \mathbb{Z}/n\mathbb{Z}$.*

An *inverse* of an element a is an element a^{-1} such that $aa^{-1} = 1$. For example, the inverse of 2 in $\mathbb{Z}/9\mathbb{Z}$ is 5 because $2 \cdot 5 = 1$. Although elements in $\mathbb{Z}/n\mathbb{Z}$ for n composite do not necessarily have an inverse - for instance, 3 does not have an inverse in $\mathbb{Z}/9\mathbb{Z}$ - all nonzero elements of $\mathbb{Z}/p\mathbb{Z}$ always have an inverse. Before we can prove this, however, we invoke a theorem of Bézout:

Theorem 2 (Bézout)**.** *Let a and b be nonzero integers, and let $d = \gcd(a, b)$. Then there exist integers x and y such that*

$$ax + by = d.$$

Using this theorem, we can now prove the aforementioned fact:

Lemma 3. *Every nonzero element of $\mathbb{F}_p$ has an inverse; furthermore, $\mathbb{F}_p$ is a field.*

Proof. Let $1 \le a \le p-1$ be a nonzero element of $\mathbb{F}_p$. Since a and p are relatively prime, there exist integers x and y such that $ax + py = 1$. Now if we write $x = np + r$ for some integers n and $0 \le r \le p-1$, then $ra + (y + an)p = 1$. But taking modulo p to both sides yields $ra = 1$, implying that r is the inverse of a. □

From this fact, we can prove a well-known theorem first announced (but not proven) by Wilson:

Theorem 4 (Wilson)**.** *An integer $n > 1$ is prime if and only if $(n-1)! \equiv -1 \pmod{n}$.*

Proof. If n is prime, then we can pair each term of the product $(n-1)!$ to its inverse to obtain a product of 1, with the exception of 1 and $n-1$. Hence $(n-1)! \equiv 1 \cdot (n-1) \cdot (aa^{-1}) \cdot (bb^{-1}) \cdot \cdots \equiv n - 1 \equiv -1$.

Conversely, if n is composite, then there exists a prime q such that $q|n$, where $2 \le q \le n-2$. Suppose that $(n-1)! \equiv -1 \pmod{n}$. This would imply that $(n-1)! \equiv -1 \pmod{q}$. However, since q is included in the product $(n-1)!$, it follows that $(n-1)! \equiv 0 \pmod{q}$, contradiction. □

We define the *Euler totient function* $\phi(n)$ as the number of positive integers less than or equal to n that are relatively prime to n. If $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$ for primes p_i and positive integers e_i, then

$$\phi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right) = n \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_k}\right).$$

Theorem 5 (Euler)**.** *If a and n are relatively prime positive integers, then*

$$a^{\phi(n)} \equiv 1 \pmod{n}.$$

Proof. Consider the set $A = \{n_1, n_2, \cdots, n_{\phi(m)}\}$ such that each element is taken modulo m and its elements are pairwise relatively prime to each other. Now consider the set $B = \{an_1, an_2, \cdots, an_{\phi(m)}\}$ where a and m are relatively prime. We claim that $A = B$. Indeed, all elements of B are relatively prime to m, so if all elements of B are distinct, then B contains the same elements as A. Hence their products are equal:

$$n_1 n_2 \cdots n_{\phi(m)} \equiv an_1 \cdot an_2 \cdots an_{\phi(m)} \equiv a^{\phi(m)} n_1 n_2 \cdots n_{\phi(m)} \pmod{m}.$$

Since all n_i are relatively prime to m, it follows that $a^{\phi(m)} \equiv 1 \pmod{m}$. □

This theorem has a natural corollary when n is prime:

Corollary 6 (Fermat)**.** *For any integer a,*

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

Theorem 7 (Chinese Remainder Theorem)**.** *Suppose that x is an integer such that*

$$\begin{aligned} x &\equiv a_1 \pmod{m_1}; \\ x &\equiv a_2 \pmod{m_2}; \\ &\vdots \\ x &\equiv a_k \pmod{m_k}. \end{aligned}$$

where m_i are all relatively prime. If $M = \prod_{i=1}^{k} m_i = m_1 m_2 \cdots m_k$, then the solutions to x are given by

$$x \equiv a \pmod{M}$$

for some integer a.

The Chinese Remainder Theorem is often used to evaluate a large number modulo a factorable large number. For instance, if we were to evaluate a large number modulo 2013, we would first evaluate it modulo 3, 11, and 61, and then apply the Chinese Remainder Theorem to combine the results.

3 Residues

When solving Diophantine equations, a common technique is to compare the residues modulo some prime power of both sides. Comparing the equation modulo some other composite number is not advised, since by the Chinese Remainder Theorem you can instead separate it into its prime divisors. A set S of integers is called a *set of residue classes* modulo n if for every integer $0 \le k \le n-1$, there exists $s \in S$ such that $k \equiv s \pmod{n}$. For instance, the set of residue classes of n^2 modulo 7 is $\{0, 1, 2, 4\}$, since $n^2 \equiv 0, 1, 2, 4 \pmod{7}$ all have integer solutions, whereas $n^2 \equiv 3, 5, 6 \pmod{7}$ do not.

A technique in choosing the "right" prime to find the residue classes is choosing a prime that is one greater than a multiple of the exponents. For example, if we were dealing with a Diophantine equation with the term $x^2 + y^5$, it is a good idea to check residue classes modulo $2 \cdot 5 + 1 = 11$. This minimizes the number of residues, and will help in finding a contradiction.

4 Fractional Mods

Modular arithmetic can be extended from the integers to the rationals easily: $\frac{a}{b} \equiv ab^{-1} \pmod{n}$. For example, $\frac{1}{2} \equiv 4 \pmod{7}$ because $1 \equiv 2 \cdot 4 \pmod{7}$. However, if $\gcd(b, n) \neq 1$, then the fraction is not equivalent to anything, since there cannot exist an inverse of b.

Fractional mods are useful when proving that the numerator of a fraction is equivalent to some number modulo some number. An example of this is shown in a theorem of Wolstenholme:

Theorem 8 (Wolstenholme)**.** *For any prime number $p > 3$, the numerator of $\sum_{k=1}^{p-1} \frac{1}{k^2}$ is divisible by p when written in lowest terms.*

Proof. Note that

$$\sum_{k=1}^{p-1} \frac{1}{k^2} \equiv \sum_{k=1}^{p-1} (k^{-1})^2 \equiv \sum_{k=1}^{p-1} k^2 \equiv \frac{p(p+1)(2p+1)}{6} \pmod{p}.$$

Since neither $p \mid 2$ nor $p \mid 3$, it follows that $\frac{p(p+1)(2p+1)}{6} \equiv 0 \pmod{p}$. Hence $\sum_{k=1}^{p-1} \frac{1}{k^2} \equiv 0 \pmod{p}$, implying that the numerator is divisible by p. □

The concept of fractional mods is formalized in the set (ring) of p-adic integers.

5 Miscellaneous Theorems/Lemmas

Lemma 9 (Hensel)**.** *Let f be an integer polynomial, and let $\alpha \in \mathbb{Z}$ such that*

$$f(\alpha) \equiv 0 \pmod{p} \text{ and } f'(\alpha) \not\equiv 0 \pmod{p}.$$

Then there exists a sequence of integers $(\alpha = \alpha_0, \alpha_1, \alpha_2, \cdots)$ such that

$$f(\alpha_n) \equiv 0 \pmod{p^{n+1}} \text{ and } \alpha_{n+1} \equiv \alpha_n \pmod{p^{n+1}}.$$

Theorem 10 (Wolstenholme)**.** *For any prime $p > 3$,*

$$\binom{2p-1}{p-1} \equiv 1 \pmod{p^3}.$$

Theorem 11 (Lucas)**.** *Let $m = m_0 + m_1 p + m_2 p^2 + \cdots + m_k p^k$ and $n = n_0 + n_1 p + n_2 p^2 + \cdots + n_k p^k$ for some integers $0 \leq m_i, n_i \leq p - 1$. Then*

$$\binom{m}{n} \equiv \prod_{i=0}^{k} \binom{m_i}{n_i}.$$

Theorem 12 (Catalan Conjecture/Mihăilescu)**.** *The only positive integer solution to the equation $x^a - y^b = 1$ is $(a, b, x, y) = (2, 3, 3, 2)$.*

6 Problems

1. (National MathCounts 2011) A pile of marbles has $15^5 + 3$ marbles. It is to be divided into 7 piles with the same number of marbles in each pile. If there are x marbles left over $(0 \leq x \leq 7)$, what is the value of x?

2. (AIME I 2010) Find the remainder when $9 \times 99 \times 999 \times \cdots \times \underbrace{99\cdots9}_{\text{999 9's}}$ is divided by 1000.

3. (AIME 1989) One of Euler's conjectures was disproved in then 1960s by three American mathematicians when they showed there was a positive integer n such that $133^5 + 110^5 + 84^5 + 27^5 = n^5$. Find the value of n.

4. Find the remainder when $7^{7^{7^7}}$ is divided by 2013.

5. Let $p \geq 7$ be a prime. Prove that the number

$$\underbrace{11\cdots1}_{p-1 \text{ 1's}}$$

is divisible by p.

6. (Mathematical Reflections) Solve in integers the equation

$$x^4 - y^3 = 111.$$

7. (USAJMO 2013) Are there integers a and b such that $a^5b + 3$ and $ab^5 + 3$ are both perfect cubes of integers?

8. Prove that p divides the numerator of $\sum_{k=1}^{p-1} \frac{1}{k^4}$ when written in lowest terms.

9. Find all integer solutions of $y^2 = x^3 + 7$.

10. (Russia 2001) Find all primes p and q such that $p + q = (p - q)^3$.

11. (USAMO 2010) Let $q = \frac{3p-5}{2}$ where p is an odd prime, and let

$$S_q = \frac{1}{2 \cdot 3 \cdot 4} + \frac{1}{5 \cdot 6 \cdot 7} + \cdots + \frac{1}{q(q+1)(q+2)}.$$

Prove that if $\frac{1}{p} - 2S_q = \frac{m}{n}$ for integers m and n, then $m - n$ is divisible by p.

12. (USAMO 2005) Prove that the system

$$x^6 + x^3 + x^3y + y = 147^{157}$$
$$x^3 + x^3y + y^2 + y + z^9 = 157^{147}$$

has no solutions in integers x, y, and z.

13. (TST 2002) Let $p > 5$ be a prime number. For any integer x, define

$$f_p(x) = \sum_{k=1}^{p-1} \frac{1}{(px+k)^2}.$$

Prove that for any pair of positive integers x, y, the numerator of $f_p(x) - f_p(y)$, when written as a fraction in lowest terms, is divisible by p^3.

14. (Gabriel Dospinescu) Let $p > 5$ be a prime. Prove that p^4 divides the numerator of the fraction

$$2\sum_{k=1}^{p-1} \frac{1}{k} + p\sum_{k=1}^{p-1} \frac{1}{k^2}$$

when written in lowest terms.