mod p^k

Tristan Shin

2 Dec 2017

Throughout this handout, unless otherwise specified, p refers to a prime and p^k refers to a prime power.

1 Order

Theorem 1.1: Euler's Theorem

If a is relatively prime to n, then

$$a^{\varphi(n)} \equiv 1 \pmod{n},$$

where $\varphi(n)$ is the number of integers in $[1, n]$ relatively prime to n.

Corollary 1.2: Fermat's Little Theorem

For any prime p and integer a, $a^p \equiv a \pmod{p}$.

These theorems motivate the idea of order.

Definition. The *order* of a modulo n, also called $\operatorname{ord}_n a$, is the smallest positive integer d such that $a^d \equiv 1 \pmod{n}$.

A direct result of Euler's Theorem is that $\operatorname{ord}_n a \leq \varphi(n)$. Furthermore, experimenting with values appears to show that $\operatorname{ord}_n a \mid \varphi(n)$. In fact, the following generalization is true:

Theorem 1.3

If $a^d \equiv 1 \pmod{n}$, then $\operatorname{ord}_n a \mid d$.

Proof. Suppose not and let $d = m(\operatorname{ord}_n a) + r$ with m, r integers and $r \in (0, \operatorname{ord}_n a)$. Then

$$1 \equiv a^d \equiv a^{m(\operatorname{ord}_n a)+r} \equiv a^r \pmod{n},$$

contradiction to the minimality of $\operatorname{ord}_n a$. ■

1.1 Primitive Roots

We also like to look at when the order is as large as possible.

Definition. A *primitive root* modulo n is an integer g such that $\operatorname{ord}_n g = \varphi(n)$.

Lemma 1.4

There exists a primitive root modulo p for every prime p.

Proof. Consider the set of residues a with order d with $d \mid p-1$. Modulo p, they are roots of the polynomial $x^d - 1$ but not roots of $x^c - 1$ for any $c < d$. This implies that they are roots of the dth cyclotomic polynomial $\Phi_d(x)$. But the degree of Φ_d is $\varphi(d)$, so there are at most $\varphi(d)$ such residues a. But observe that

$$\sum_{d \mid p-1} \varphi(d) = p - 1,$$

so there are at most $p-1$ residues a relatively prime to p, with equality if and only if equality holds for each order d. In particular, this equality is true when $d = p-1$, so there are $\varphi(p-1)$ primitive roots modulo p. ■

Lemma 1.5

Let p be odd, g a primitive root modulo p. If $g^{p-1} \not\equiv 1 \pmod{p^2}$, then $g^{\varphi(p^k)} \not\equiv 1 \pmod{p^{k+1}}$ for any positive integer k.

Proof. Induct on k. The base case of $k=1$ is given. Now, suppose that the claim is true for k. Let $g^{\varphi(p^k)} = mp^k + 1$ (possible by Euler's Theorem). Then

$$g^{\varphi(p^{k+1})} = \left(mp^k + 1\right)^p \equiv 1 + mp^{k+1} \pmod{p^{k+2}}.$$

By the inductive hypothesis, $p \nmid m$, so $p^{k+2} \nmid mp^{k+1}$ and hence the last term above is *not* 1 modulo p^{k+2}. Thus, the inductive step is proven and the claim follows. ■

Theorem 1.6: Primitive Root Theorem

There exists a primitive root modulo p^k when p is odd.

Proof. Let g be a primitive root modulo p with $g \in (0, p)$. The key claim is that either g or $g + p$ is a primitive root modulo p^k.

Suppose that $g^{p-1} \not\equiv 1 \pmod{p^2}$. We show that g is a primitive root modulo p^k by induction on k. The base case of $k = 1$ is trivially true. Now, suppose that g is a primitive root modulo k. Let $d = \operatorname{ord}_{p^{k+1}} g$. Then $g^d \equiv 1 \pmod{p^k}$ also, so $p^{k-1}(p-1) \mid d$. But we also have that $d \mid \varphi\left(p^{k+1}\right) = p^k(p-1)$, so either $d = p^{k-1}(p-1)$ or $p^k(p-1)$. But Lemma 1.5 tells us that $d \neq p^{k-1}(p-1)$, so $d = p^k(p-1)$, as requested.

Now, if $g^{p-1} \equiv 1 \pmod{p^2}$, then

$$(g+p)^{p-1} \equiv g^{p-1} + (p-1)\, g^{p-2} p \not\equiv 1 \pmod{p^2},$$

so repeat the above paragraph with g replaced by $g+p$ (still a primitive root modulo p) to arrive at the conclusion that $g+p$ is a primitive root modulo p^k. ■

2 Analytic results

2.1 Hensel's Lemma

Suppose that $P(x)$ is a polynomial with integer coefficients.

Problem 2.1

Prove that $a!$ divides $P^{(a)}(n)$ for all integers n.

Proof. It suffices to prove the statement when $P = x^m$ for some non-negative integer m (the result follows by multiplying by coefficients and summing). Then

$$\frac{P^{(a)}(n)}{a!} = \frac{m(m-1)\cdots(m-a+1)}{a!} n^{m-a} = \binom{m}{a} n^{m-a},$$

an integer. ■

Remark. Use this to solve 2016 Putnam A1.

Lemma 2.2

For all integers r and t and positive integers $m \le k$,

$$P\left(r + tp^k\right) \equiv P(r) + tp^k P'(r) \pmod{p^{k+m}}.$$

Proof. Consider the Taylor series for P about r. This is

$$P(r+x) = P(r) + P'(r)\, x + \sum_{a=2}^{n} \frac{P^{(a)}(r)}{a!} x^a.$$

By Problem 2.1, all of the coefficients of this expansion are integers. But then setting $x = tp^k$ and taking modulo p^{k+m} gives the desired congruence. ■

Lemma 2.3: Hensel's Lemma

Let $m \le k$ be positive integers. If $P(r) \equiv 0 \pmod{p^k}$ and $p \nmid P'(r)$, then there exists an integer s (unique modulo p^{k+m}) such that $P(s) \equiv 0 \pmod{p^{k+m}}$ and $r \equiv s \pmod{p^k}$.

Proof. From Lemma 2.2, we have that

$$P\left(r+tp^k\right) \equiv P\left(r\right) + tp^k P'\left(r\right) \pmod{p^{k+m}}.$$

Let Q be an inverse of $P'\left(r\right)$ modulo p^m. Then choosing $t \equiv -\frac{P(r)}{p^k} \cdot Q \pmod{p^m}$ gives that the RHS is $0 \pmod{p^{k+m}}$, so we can choose $s = r + tp^k$. Since t is unique modulo p^m, s is unique modulo p^{k+m}. ■

Remark. We often use Hensel's lemma with $m = 1$.

2.2 Thue's Lemma

Often, we want to write things in modular arithmetic with small components. For example, it's easier to write a fraction in simplest form, reducing everything as small as possible.

Lemma 2.4: Thue's Lemma

Let n be a positive integer and choose positive integers X, Y with $X \leq n < XY$. Then for any integer a, we can choose integers $x \in (-X, X)$ and $y \in (0, Y)$ such that

$$ay \equiv x \pmod{n}.$$

Proof. Consider the numbers $av - u$ for $u, v \in \mathbb{Z}, 0 \leq u < X, 0 \leq v < Y$. There are $XY > n$ such pairs (u, v), so by the Pigeonhole principle, there exist two of these that are the same modulo n. Let them be $av_1 - u_1$ and $av_2 - u_2$ with $v_1 \geq v_2$. If $v_1 = v_2$, then $u_1 \equiv u_2 \pmod{n}$ are distinct, but both are in $[0, X-1] \subset [0, n-1]$, contradiction, so $v_1 \neq v_2$ and hence $v_1 > v_2$. Then

$$a\left(v_1 - v_2\right) \equiv \left(u_1 - u_2\right) \pmod{n},$$

so we have found $(x, y) = (u_1 - u_2, v_1 - v_2)$. Since $-X < u_1 - u_2 < X$ and $0 < v_1 - v_2 < Y$, this choice of x, y works. ■

There are also some modifications and corollaries.

Corollary 2.5

For any integer n, there exist integers a, b in $[-p, p]$, $b \neq 0, p, -p$, and $n \equiv \frac{a}{b} \pmod{p^2}$.

2.3 Lifting the Exponent

To extract a prime power p^k from a integer n divisible by p, we will say that $v_p\left(n\right) = k$, where k is the largest integer such that p^k divides n.

Lemma 2.6

For a prime p which divides $x-y$ but none of x, y, n,

$$v_p\left(x^n - y^n\right) = v_p\left(x-y\right).$$

Proof. Observe that

$$v_p\left(x^n - y^n\right) = v_p\left(x-y\right) + v_p\left(x^{n-1} + x^{n-2}y^2 + \ldots + xy^{n-2} + y^{n-1}\right).$$

But

$$x^{n-1} + x^{n-2}y^2 + \ldots + xy^{n-2} + y^{n-1} \equiv nx^{n-1} \pmod{p},$$

which is not 0, so the last term is 0 and hence $v_p\left(x^n - y^n\right) = v_p\left(x-y\right)$. ∎

Lemma 2.7: Lifting the Exponent

For an odd prime p which divides $x-y$ but neither of x, y,

$$v_p\left(x^n - y^n\right) = v_p\left(x-y\right) + v_p\left(n\right).$$

Proof. Induct on $v_p\left(n\right)$. The base case is Lemma 2.6. Now, suppose that the statement is true for $v_p\left(n\right) = k$, some nonnegative integer. We prove it for $v_p\left(n\right) = k+1$.

Let $n = pm$ for a positive integer m with $v_p\left(m\right) = k$. Observe that

$$\begin{aligned} v_p\left(x^n - y^n\right) &= v_p\left(x^{pm} - y^{pm}\right) \\ &= v_p\left(x^m - y^m\right) + v_p\left(x^{(p-1)m} + x^{(p-2)m}y^m + \ldots + x^m y^{(p-2)m} + y^{(p-1)m}\right). \end{aligned}$$

Let $x = y + pz$ for some integer z. Then

$$\sum_{i=0}^{p-1} x^{im} y^{(p-1-i)m} \equiv px^{(p-1)m} \equiv 0 \pmod{p}$$

but

$$\sum_{i=0}^{p-1} x^{im} y^{(p-1-i)m} \equiv \sum_{i=0}^{p-1} \left(y+pz\right)^{im} y^{(p-1-i)m} \equiv \sum_{i=0}^{p-1} \left(y^{im} + imy^{im-1}pz\right) y^{(p-1-i)m} \pmod{p^2},$$

which is

$$p\left(y^{(p-1)m} + \sum_{i=0}^{p-1} imzy^{(p-1)m-1}\right) \equiv p\left(y^{(p-1)m} + \frac{p\left(p-1\right)}{2} mzy^{(p-1)m-1}\right) \not\equiv 0 \pmod{p^2}.$$

Thus, the last term is 1 and thus the inductive step is proven. ∎

Remark. Lifting the Exponent works with $p = 2$ only when 4 divides $x-y$. Can you see why?

3 Problems

1. How many in shuffles are needed to return a deck back to original order? Out shuffles?

2. (Spring 2016 OMO #11, Tristan Shin) For how many positive integers x less than 4032 is $x^2 - 20$ divisible by 16 and $x^2 - 16$ divisible by 20?

3. (George E. Andrews) Determine all integers n such that $n^7 + n + 1$ is divisible by 343.

4. (2015 CVSC Olympiad Division #16, Adam Zheng) The smallest positive integer n such that $7^n \equiv 1 \pmod{6^9}$ can be expressed as m^2 for some positive integer m. Find m.

5. For a fixed prime p, find all positive integers n such that
$$1^n + 2^n + 3^n + \ldots + (p-1)^n$$
is not divisible by p.

6. Let n be a positive integer which is not a perfect square, and let D be a positive integer. Suppose that $\gcd(D, n) = 1$ and that $-D$ is a square modulo n. Then there exist $k, x, y \in \mathbb{Z}$ with $0 < k \le D$, $0 < |x|, |y| \le \sqrt{n}$, such that
$$x^2 + Dy^2 = kn.$$

7. (2017 SD HMMT TST #9, Tristan Shin) Determine the number of ordered pairs (a, b) of positive integers with $1 \le a \le b \le 49$ such that $(a+b)^{49}$ and $a^{49} + b^{49}$ leave the same remainder upon division by 49.

8. (1990 IMO #3) Determine all integers $n > 1$ such that
$$\frac{2^n + 1}{n^2}$$
is an integer.

9. Let a and b be two positive rational numbers such that for infinitely many positive integers n, $a^n - b^n$ is an integer. Prove that a and b are integers.

10. (Harder than 2017 TST #6) Prove that there are infinitely many triples (a, b, p) of positive integers with p prime, $a < p$, and $b < p$, such that $(a+b)^p - a^p - b^p$ is a multiple of p^5.