Orders and Primitive Roots

Aprameya Tripathy, minor edits by Dennis Chen

NRU

Thanks to Raymond Feng for suggesting several of the problems in this handout.

§ 1 Orders

We begin by reviewing some introductory theorems.

Theorem 1 (Fermat) $a^{p-1} \equiv 1 \pmod p$ whenever p is prime and $p \nmid a$.

Theorem 2 (Euler) $a^{\phi(n)} \equiv 1 \pmod n$ whenever $\gcd(a, n) = 1$.

(If you have forgotten the proofs for these theorems, try to reprove them as an exercise or refer to **NQU-Mod**.) Notice that both Fermat and Euler are *weak*.

Example 1 (Stronger Euler on 1000) Show that there exists some $x < 400$ such that

$$a^x \equiv 1 \pmod{1000}$$

for all a relatively prime to 1000.

Solution: We claim that $x = 100$ is a satisfactory value of x.

Notice that by Euler,

$$a^{100} \equiv a^{100 \pmod{\phi(8)}} \equiv a^{100 \pmod 4} \equiv a^0 \equiv 1 \pmod 8$$

and that

$$a^{100} \equiv a^{\phi(125)} \equiv 1 \pmod{125}$$

whenever $\gcd(a, 1000) = 1$. Thus, by CRT,

$$a^{100} \equiv 1 \pmod{1000}$$

for all a relatively prime to 1000.

Often, there is a number $x < \phi(n)$ such that $a^x \equiv 1 \pmod n$ for some a. In order to properly discuss this x, we define **orders.**

Definition 1 (Orders) Let a and n be two relatively prime integers with $n > 1$. Then $\text{ord}_n(a)$ (the order of a mod n) is the smallest positive integer x such that $a^x \equiv 1 \pmod n$.

We immediately notice the following fact.

Fact 1 For relatively prime integers a and m, $a^m \equiv 1 \pmod{n}$ if and only if $\text{ord}_n(a) \mid m$.

Proof: Clearly, $a^m \equiv 1 \pmod{n}$ if $\text{ord}_n(a) \mid m$ by definition, so the if condition holds.

Now, if $a^m \equiv 1 \pmod{n}$, we see that $m \geq \text{ord}_n(a)$ by definition. Thus, from the division algorithm, there exist two integers q and r such that

$$m = q \cdot \text{ord}_n(a) + r,$$

where $0 \leq r \leq \text{ord}_n(a) - 1$ and $q > 0$. Since $a^{\text{ord}_n(a)} \equiv 1 \pmod{n}$, we see $a^{-q \cdot \text{ord}_n(a)} \equiv (1)^{-q} \equiv 1$.

Thus,

$$a^r \equiv a^{m - q \cdot \text{ord}_n(a)} \equiv 1 \pmod{n},$$

so by the minimality of $\text{ord}_n(a)$, r can't be positive (as $r \leq \text{ord}_n(a) - 1$). Thus, we must have $r = 0$, meaning $\text{ord}_n(a) \mid m$, completing the proof. ■

This fact is one of the most useful facts relating to orders - it allows us to take the order of some random value and relate it to the overall modulus. In other words, it allows us to get **global** information from **local** information - something that is very powerful in many places. We will explore two of those examples.

Example 2 (Fermat's Christmas Theorem) Show that if a prime $p > 2$ can be written as the sum of two squares, we must have $p \equiv 1 \pmod{4}$.

Solution: Suppose that $p = x^2 + y^2$ for some positive integers x and y. Clearly, $p \nmid x$ and $p \nmid y$, as if p divided either x or y, we would have $x^2 + y^2 > p$.

Since $x^2 + y^2 = p$, we see $x^2 + y^2 \equiv 0 \pmod{p}$. Thus, $(xy^{-1})^2 \equiv -1 \pmod{p}$, and (by squaring), $(xy^{-1})^4 \equiv 1 \pmod{p}$. Thus, $\text{ord}_p(xy^{-1}) \mid 4$.

Notice that if $\text{ord}_p(xy^{-1}) \mid 2$, then we would have $(xy^{-1})^2 \equiv 1 \pmod{p}$, but as we showed earlier, $(xy^{-1})^2 \equiv -1 \pmod{p}$. Since $p > 2$, this is clearly absurd, so we must have $\text{ord}_p(xy^{-1}) \nmid 2$. Since the only factor of 4 that doesn't divide 2 is 4, we must have $\text{ord}_p(xy^{-1}) = 4$.

Now, from Fermat, $(xy^{-1})^{p-1} \equiv 1 \pmod{p}$. Thus, $\text{ord}_p(xy^{-1}) = 4 \mid p - 1$, so $p \equiv 1 \pmod{4}$.

Observe how we did not *ever* try to find x, or y, or xy^{-1}. We only tried to find $\text{ord}_p(xy^{-1})$. The idea of finding orders instead of variables is quite useful.

Oftentimes, this idea works, but sometimes, we need to use another idea – exploiting minimality.

Example 3 (China TST 2006 Quiz) Find all positive integers a and n such that

$$\frac{(a+1)^n - a^n}{n}$$

is an integer.

Solution: Assume for the sake of contradiction that $n > 1$. Let p be the smallest prime that divides n (p exists as $n > 1$). Since $\frac{(a+1)^n - a^n}{n} \in \mathbb{Z}$, we must have $(a+1)^n \equiv a^n \pmod{p}$. Thus (since a is clearly not a multiple of p), $((a+1)a^{-1})^n \equiv 1 \pmod{p}$, so $\text{ord}_p((a+1)a^{-1}) \mid n$.

Observe that from Fermat, $\text{ord}_p((a+1)a^{-1}) \mid p - 1$. Thus, $\text{ord}_p((a+1)a^{-1}) \mid \gcd(p-1, n)$. Notice that if $\gcd(p-1, n) > 1$, then there is some prime $q < p$ that divides n, contradicting minimality of p. Thus, we must have $\gcd(p-1, n) = 1$, so $\text{ord}_p((a+1)a^{-1}) = 1$.

Thus,

$$(a+1)a^{-1} \equiv 1 \pmod{p} \iff a + 1 \equiv a \pmod{p} \iff 1 \equiv 0 \pmod{p},$$

a contradiction.

Thus, $n = 1$. Substituting that into the original expression, we see that

$$\frac{(a+1)^n - a^n}{n} = \frac{a+1-a}{1} = 1,$$

so $\frac{(a+1)^n - a^n}{n}$ is an integer whenever $n = 1$.

There are two main takeaways from this problem that apply to most order problems.

- The modulus is the most important: Like in the previous example, notice that the method of solving this problem was "Find n" - not "find a" (even with primitive roots, the idea is to pick a instead of finding it) It's almost always a better idea to restrict the modulus than restrict the equivalent numbers in problems like these

- Minimality arguments: Notice how important the fact that p was the smallest prime factor of n was. Without it, the problem would be much more difficult.

§ 2 Primitive Roots

We know that we always have $\text{ord}_n(a) \le \phi(n)$, but can we ever achieve the maximum? In other words, does there exist a value a for a certain n such that $\text{ord}_n(a) = \phi(n)$? What properties might this a have? In order to properly discuss these numbers, we define a **primitive root**.

Definition 2 (Primitive Root) Let a and n be two positive integers. a is called a primitive root modulo n if and only if $\text{ord}_n(a) = \phi(n)$.

Before discussing the applications of primitive roots, we prove that they always exist modulo p, where p is prime.

Definition 3 (Polynomial Ring) Let $\mathbb{Z}[x]$ be the ring of polynomials with integer coefficients.

Theorem 3 (Lagrange) Let $f(x) \in \mathbb{Z}[x]$ such that not all coefficients of f are multiples of some prime p. Then the equation

$$f(x) \equiv 0 \pmod{p}$$

has at most $\deg f$ incongruent solutions $\pmod{p}$.

Proof: We proceed with induction on $\deg f$.

Consider when $\deg f = 0$. Then, by definition, $f(x) = c$, where $p \nmid c$. Thus, the equation $f(x) \equiv 0 \pmod{p}$ has no solutions, so the claim holds in the base case.

Now, assume the claim holds for all polynomials of degree m for some $m \in \mathbb{N}$. We will show it holds for all polynomials of degree $m + 1$.

Consider some polynomial $f(x) \in \mathbb{Z}[x]$ with degree $m + 1$. If $f(x) \equiv 0 \pmod{p}$ has no solutions, the claim holds. Otherwise, assume that there exists some constant a such that $f(a) \equiv 0 \pmod{p}$. From the definition of modular arithmetic, there exists some integer q such that $f(a) - pq = 0$. From the remainder theorem, this means $x - a \mid f(x) - pq$.

Thus, there exists some $g(x) \in \mathbb{Z}[x]$ such that $f(x) = g(x) \cdot (x - a) + pq$. Thus, $f(x) \equiv g(x)(x - a) \pmod{p}$, and since $\deg(x - a) = 1$, we have $\deg g = m$. Now, notice $g(x) \equiv 0 \pmod{p}$ has at most m solutions (inductive hypothesis) and $x - a \equiv 0 \pmod{p}$ has one solution. Thus, $f(x) \equiv 0 \pmod{p}$ has at most $m + 1$ solutions, completing the inductive step and finishing the proof. ■

Fact 2 (Summing the Euler Totient Function) Over the positive integers,

$$\sum_{d|n} \phi(d) = n.$$

We can now show that primitive roots always exist modulo p where p is prime. In fact, we an prove something much stronger.

Theorem 4 (Amount of Repeating Orders) Let p be a prime, and $d \mid p-1$. Then there are exactly $\phi(d)$ elements with order d modulo p.

Proof: Consider the polynomial $x^d - 1$. Clearly, $x^{p-1} - 1 = (x^d - 1)\frac{x^{p-1}-1}{x^d-1}$. From the geometric series formula, $\frac{x^{p-1}-1}{x^d-1} \in \mathbb{Z}[x]$, and from Fermat, $x^{p-1} - 1 \equiv 0 \pmod{p}$ has $p-1$ solutions.

Now, from Lagrange, $x^d - 1 \equiv 0 \pmod{p}$ has at most d non-congruent solutions $\pmod{p}$, and $\frac{x^{p-1}-1}{x^d-1} \equiv 0 \pmod{p}$ has at most $p-d$ non-congruent solutions $\pmod{p}$. Since $(x^d-1)\frac{x^{p-1}-1}{x^d-1} \equiv 0 \pmod{p}$ has exactly p solutions $\pmod{p}$, $x^d - 1$ and $\frac{x^{p-1}-1}{x^d-1}$ must each respectively have exactly d and $p-d$ non-congruent solutions $\pmod{p}$.

Let $\Omega(q)$ be the number of prime factors of q counted with multiplicity, where $q \mid p-1$. We will show by strong induction on $\Omega(q)$ that there are $\phi(q)$ non-congruent numbers which have order q modulo p.

If $\Omega(q) = 0$, $q = 1$. Clearly, there is only one number with order $\phi(1) = 1$ modulo p, proving the first base case.

If $\Omega(q) = 1$, q would be prime. Consider the number of solutions to $x^q - 1 \equiv 0 \pmod{p}$. From Fact 1, we know that $x^q - 1 \equiv 0 \pmod{p}$ if and only if $\text{ord}_p(x) \mid q$. Since q is prime, the number of solutions to $x^q - 1 \equiv 0 \pmod{p}$ is equal to the number of solutions to $\text{ord}_p(x) = 1$ plus the number of solutions to $\text{ord}_p(x) = q$. Since there is only one x such that $\text{ord}_p(x) = 1$ and $x^q - 1 \equiv 0 \pmod{p}$ has q solutions, there are $q - 1 = \phi(q)$ numbers with order q modulo p. Thus, the second base case is true.

Now, assume that for all $q \mid p-1$ with $\Omega(q) \leq m$, $\text{ord}_p(x) = q$ has $\phi(q)$ solutions. We will show that for any $r \mid p-1$ and $\Omega(r) = m+1$, there are $\phi(r)$ solutions to $\text{ord}_p(x) = r$.

Let the proper divisors of r be $1, r_1, r_2, \ldots, r_n$. Consider the number of solutions to $x^r - 1 \equiv 0 \pmod{p}$. We know that the number of solutions to $x^r - 1 \equiv 0 \pmod{p}$ is equal to the number of solutions to $\text{ord}_p(x) = 1$ plus the number of solutions to $\text{ord}_p(x) = r_1$, $\ldots$, plus the number of solutions to $\text{ord}_p(x) = r$.

Clearly, $\Omega(r_i) \leq m$ for all $1 \leq i \leq n$. By the inductive hypothesis, there are $\phi(r_i)$ solutions to $\text{ord}_p(x) = r_i$ for all $1 \leq i \leq n$. From Fact 2, it follows that there are $\phi(r)$ solutions to $\text{ord}_p(x) = r$, completing the inductive step and finishing the proof. ■

It turns out that primitive roots exist mod n if and only if n is either $2, 4, p^k$, or $2p^k$, where p is an odd prime and k is a positive integer. This will turn out to be very useful.

Fact 3 (Primitive Root Residue System) Let p be a prime and g a primitive root modulo p. Show that

$$\{g, g^2, g^3, \ldots, g^{p-1}\} \equiv \{1, 2, 3, \ldots, p-1\} \pmod{p}.$$

Proof: Let g^m and g^n be two distinct elements in $\{g, g^2, g^3, \ldots, g^{p-1}\}$. Notice that $g^m \not\equiv g^n \pmod{p}$, as if $g^m \equiv g^n \pmod{p}$, then we would have $p-1 \mid m-n$. Thus, all the elements in $\{g, g^2, g^3, \ldots, g^{p-1}\}$ are distinct modulo p.

Thus, since there are $p-1$ elements in $\{g, g^2, g^3, \ldots, g^{p-1}\}$ and only $p-1$ non-zero residues modulo p, non-zero residues modulo p is equivalent to a certain element of the set $\{g, g^2, g^3, \ldots, g^{p-1}\} \pmod{p}$. Thus,

$$\{g, g^2, g^3, \ldots, g^{p-1}\} \equiv \{1, 2, 3, \ldots, p-1\} \pmod{p}.$$

■

Primitive roots an often be used to convert questions dealing with the set $\{1, 2, 3, \ldots, p-1\}$ into ones which deal with the set $\{g, g^2, g^3, \ldots, g^{p-1\}}$ – a powerful exchange for many reasons.

They are also typically used when orders aren't powerful enough to solve a problem.

Example 4 (Primitive Root Problem) Find all positive two digit integers $\overline{ab}$ with $a \neq b$ such that $\overline{ab} \mid k^a - k^b$ for all integers k.

Solution: Let p be any prime that divides $\overline{ab}$, and let g be a primitive root modulo p.

Since we have $\overline{ab} \mid k^a - k^b$ for all integers k, we must have $p \mid \overline{ab} \mid g^a - g^b$, so $g^a \equiv g^b \pmod{p}$. Multiplying by g^{-b}, we get $g^{a-b} \equiv 1 \pmod{p}$, so since $\text{ord}_p(g) = p-1$ (as x is a primitive root modulo p), we have $p-1 \mid a-b$. Thus, since the maximum value of $|a-b|$ is 9 and $a-b \neq 0$, we see that

$$(p-1)+1 \leq |a-b|+1 \leq 10 \Longleftrightarrow p \in \{2, 3, 5, 7\}.$$

Thus, the only primes that can divide $\overline{ab}$ when $a \neq b$ are $\{2, 3, 5, 7\}$, and if a prime p divides $\overline{ab}$, $p-1 \mid a-b$. We proceed with casework

Case 1: $7 \mid \overline{ab}$.

If $7 \mid \overline{ab}$, then $6 \mid a-b$, so either $a = b+6$ or $b = a+6$. Thus, we must have $\overline{ab} \in \{17, 28, 39, 60, 71, 82, 93\}$, but since $7 \mid \overline{ab}$, we must have $\overline{ab} = 28$. Checking (with CRT and Euler), we see $\overline{ab} = 28$ works.

Case 2: $5 \mid \overline{ab}$ and $7 \nmid \overline{ab}$.

Clearly, we must have either $b = 0$ or $b = 5$. Since $5 \mid \overline{ab}$, we have $4 \mid a-b$, so we must have either $a = b+4$, $a = b+8$, $a = b-4$, or $a = b-8$. Thus, $\overline{ab} \in \{40, 80, 45, 85, 15\}$. We can't have $\overline{ab} = 45$ or 85, as if $\overline{ab} = 45$, then $3 \mid \overline{ab}$ but $2 \nmid a-b$, and if $\overline{ab} = 85$, then $17 \mid \overline{ab}$. Now, notice that if $\overline{ab} = 40$ or 80, then $k^a - 1 \neq 0 \pmod{8}$ whenever k is even, so we must have $\overline{ab} = 15$. Checking (with CRT and Euler), we see $\overline{ab} = 15$ works.

Case 3: $3 \mid \overline{ab}$ and $5 \nmid \overline{ab}$ and $7 \nmid \overline{ab}$.

Notice that we have $\overline{ab} = 3^p \dot{2}^q$, where $p > 1$. Thus, we have $\overline{ab} \in \{27, 81, 12, 18, 24, 36, 48, 54, 72, 96\}$. We can't have $\overline{ab} \in \{27, 81, 12, 18, 36, 54, 72, 96\}$, as then $3 \mid \overline{ab}$ but $2 \nmid a-b$. Thus, $\overline{ab} \in \{24, 48\}$. Now, notice that $\overline{ab} \neq 24$, since whenever $k \equiv 2 \pmod{8}$, $k^2 - k^4 \not\equiv 0 \pmod{8}$. Thus, we must have $\overline{ab} = 48$. Checking (with CRT and Euler), we see $\overline{ab} = 48$ works.

Case 4: 2 is the only prime that divides $\overline{ab}$.

Notice that we must have $\overline{ab} = 2^a$, where $a > 1$. Thus, $\overline{ab} \in \{16, 32, 64\}$, but notice that when this is true, $\overline{ab} \nmid 2^a - 2^b$. Thus, this case gives no solutions.

Thus, the solution set is $\overline{ab} \in \{15, 28, 48\}$.

Understand why primitive roots were used and how they were used. If we have freedom to pick the values of our variables, it is often fruitful to use primitive roots.

§ 3 Problems

For some of the problems presented, it may be useful to know the **Lifting The Exponent Lemma**. We will not prove the lemma here. (If you want a thorough treatment of LTE, see Raymond Feng's **NRU-Prime**.)

Theorem 5 (Lifting The Exponent) Let $v_p(n)$ where p is prime be the number such that $p^{v_p(n)} \mid n$ and $p^{v_p(n)+1} \nmid n$.

- If an odd prime $p \mid a-b$ but $p \nmid a$ and $p \nmid b$, we have
$$v_p(a^n - b^n) = v_p(a-b) + v_p(n).$$
- If an odd prime $p \mid a+b$ but $p \nmid a$ and $p \nmid b$, we have
$$v_p(a^n + b^n) = v_p(a+b) + v_p(n)$$
if n is odd, and
$$v_p(a^n + b^n) = 0$$
if n is even.
- if $2 \mid x-y$ but $2 \nmid x$ and $2 \nmid y$, then whenever $2 \mid n$, we have
$$v_2(x^n - y^n) = v_2(x-y) + v_2(n) + v_2(x+y) - 1.$$

Minimum is [28]. Problems with the symbol are required.

> "The Mafia is grievously wounded – but not mortally."
>
> Five Families

[1] **Problem 1** Show $n \nmid 2^n - 1$ for all $n > 1$. (This is actually a weaker form of Example 3.)

[2] **Problem 2** (AIME I 2019/14) Find the least odd prime factor of $2019^8 + 1$.

[3] **Problem 3 (China TST 1993/1)** For all primes $p \geq 3$ such that $p - 1 \nmid 120$, define
$$F(p) = \sum_{k=1}^{\frac{p-1}{2}} k^{120}$$
and $f(p) = \frac{1}{2} - \left\{\frac{F(p)}{p}\right\}$, where $\{x\} = x - [x]$, find the value of $f(p)$.

[3] **Problem 4** (Euler) Prove that all factors of $2^{2^n} + 1$ are of the form $k \cdot 2^n + 1 + 1$.

[4] **Problem 5** Suppose p is a prime such that there exists an integer q such $q^2 \equiv -3 \pmod{p}$. Find all solutions to $x^3 \equiv 1 \pmod{p}$ in terms of p and q.

[6] **Problem 6** (Weak Dirichlet) Prove that there are infinite primes $p \equiv 1 \pmod{k}$.

[6] **Problem 7** (DIME 2020/14) For a positive integer n not divisible by 211, let $f(n)$ denote the smallest positive integer k such that $n^k - 1$ is divisible by 211. Find the remainder when
$$\sum_{n=1}^{210} n f(n)$$

is divided by 211.

[6✐] **Problem 8** (IMO 1999/4) Find all the pairs of positive integers (x, p) such that p is a prime, $x \leq 2p$ and x^{p-1} is a divisor of $(p-1)^x + 1$.

[9✐] **Problem 9** (IMO 1990/3) Find all positive integers n such that $n^2 \mid 2^n + 1$.

[9✐] **Problem 10** (ISL 2012/N6) Let x and y be positive integers. If $x^{2^n} - 1$ is divisible by $2^n y + 1$ for every positive integer n, prove that $x = 1$.

[13✐] **Problem 11** (ISL 2003/N7) The sequence a_0, a_1, a_2, ... is defined as follows:

$$a_0 = 2, \qquad a_{k+1} = 2a_k^2 - 1 \quad \text{for } k \geq 0.$$

Prove that if an odd prime p divides a_n, then 2^{n+3} divides $p^2 - 1$.