Orders

Stuyvesant Senior Math Team

Aditya Pahuja

August 14, 2025

Contents

0 Introduction

This is a short lesson on the extremely well-behaved properties of exponents in number theory. The classic example of this is, of course, Fermat's little theorem, which tells you that $a^x \pmod p$ is periodic in x with period (at most) $p-1$ for p prime.

It turns out that we can take this much further, and the main way to get information out of such expressions is through the lens of *orders*.

1 Definitions and Starting Steps

First, the following notation, if you haven't seen it before, is a useful shorthand: for a given prime p and integer n, the **p-adic valuation** of n, denoted by $\nu_p(n)$, is the largest integer e such that $p^e \mid n$. That is, $\nu_p(n)$ is the exponent of p in the prime factorization of n.

When $\gcd(a,n) = 1$, the **order** of a number a modulo n, denoted $\text{ord}_n(a)$, is the smallest positive integer d for which

$$a^d \equiv 1 \pmod n.$$

Fermat's little theorem and Euler's generalization tell us that, in fact, $d \mid \varphi(n)$. We can more strongly say the following:

Theorem 1.1. If $a^k \equiv 1 \pmod n$, then $\text{ord}_n(a)$ divides k.

Proof. Let d be the order of a, and write $k = qd + r$, where $0 \le r < d$. Then,

$$a^{qd} \cdot a^r \equiv a^r \equiv 1 \pmod n.$$

If $0 < r < d$, then we have found a positive integer smaller than d for which $a^r \equiv 1 \pmod r$, which contradicts the minimality of the order; thus, $r = 0$, which means d divides k. □

A number g is a **primitive root** modulo n if

$$\text{ord}_n(g) = \varphi(n).$$

You can view this as saying "Euler's theorem is sharp (i.e. gives the strongest possible bound on the order) when g is a primitive root."

Example 1.1

For example, 2 is a primitive root modulo 11, because

$$\begin{aligned} 2^1 &\equiv 2 \pmod{11} & 2^6 &\equiv 9 \pmod{11} \\ 2^2 &\equiv 4 \pmod{11} & 2^7 &\equiv 7 \pmod{11} \\ 2^3 &\equiv 8 \pmod{11} & 2^8 &\equiv 3 \pmod{11} \\ 2^4 &\equiv 5 \pmod{11} & 2^9 &\equiv 6 \pmod{11} \\ 2^5 &\equiv 10 \pmod{11} & 2^{10} &\equiv 1 \pmod{11} \end{aligned}$$

so 10 is the smallest x for which $2^x \equiv 1 \pmod{11}$.

In fact, we could've been more careful about how we verified this: $\text{ord}_{11}(2)$ must divide $\varphi(11)$, so we only needed to check 1, 2, 5, and 10 — although this really means we only had to check 2 and 5 in the first place, so I was very inefficient!

(How many exponents do you need to check for a general prime p?)

Exercise 1.2. Find all the primitive roots modulo 11, 13, and 17. How many primitive roots are there modulo p for prime p?

Exercise 1.3. What other patterns do you notice in the table? (There are many!)

A natural question now is to ask "When do primitive roots exist?" It turns out that this has a very nice answer, although its proof (in part) is deferred to the Cyclotomic Polynomials unit.

Theorem 1.2 (Existence of primitive roots)**.** Primitive roots exist mod 2, 4, p^k, and $2p^k$ for odd primes p.

Showing that primitive roots exist is hard without some additional machinery; however, showing that they don't is doable, since we just have to find a smaller value than $\varphi(n)$ for the order.

Proof of nonexistence. We want to show nonexistence of a primitive root modulo n for $n \notin \{2, 4, p^k, 2p^k\}$.

We consider three cases: either n is a power of two greater than 4, n has at least two (distinct) odd prime factors, or n is the product of a power of two greater than 2 and a prime power.

First, suppose $n = 2^k$ for $k \geq 3$. Since $\varphi(2^k) = 2^{k-1}$, it suffices to show that

$$a^{2^{k-2}} \equiv 1 \pmod{2^k}$$

if $\gcd(a, n) = 1$. Let $S = a^{2^{k-2}} - 1$, so difference of squares says

$$\begin{aligned} S = (a^{2^{k-3}} + 1)(a^{2^{k-3}} - 1) &= (a^{2^{k-3}} + 1)(a^{2^{k-4}} + 1)(a^{2^{k-4}} - 1) \\ &= (a^{2^{k-3}} + 1)(a^{2^{k-4}} + 1)(a^{2^{k-5}} + 1)(a^{2^{k-5}} - 1) \\ &= \cdots \\ &= (a^{2^{k-3}} + 1)(a^{2^{k-4}} + 1) \cdots (a^2 + 1)(a^2 - 1). \end{aligned}$$

Taking mod 4, we have $a^{2^m} + 1 \equiv 2 \pmod 4$ whenever $m \geq 1$, so $\nu_2(a^{2^m} + 1) = 1$, since it's even but not a multiple of four. Additionally, $a^2 - 1$ is a multiple of 8. This means that $\nu_2(S) = k - 3 + 3$, so $S \equiv 0 \pmod{2^k}$, which is what we want!

We now prove two critical claims that help us finish off the other cases.

Claim 1.3 — Let m and n be relatively prime. Then, the order of a number mod mn is at most $\operatorname{lcm}(\varphi(m), \varphi(n))$.

Proof. Observe that

$$a^{\operatorname{lcm}(\varphi(m),\varphi(n))}$$

is $1 \pmod m$ and $1 \pmod n$, so by CRT it is $1 \pmod{mn}$ as desired. □

Claim 1.4 — For all $m > 2$, $\varphi(m)$ is even.

Proof. Whenever m is divisible by an odd prime p, $\varphi(m)$ is divisible by $p-1$, using the explicit formula for $\varphi(m)$. Then, $p-1$ is even, implying $\varphi(m)$ is also even.

If m is a power of two, then $\varphi(m) = \frac{m}{2}$, which is at least two and thus even because $m > 2$. □

Remark 1.5. There is also a cute bijective proof I am fond of which involves showing that numbers relatively prime to m come in pairs of the form $(r, m-r)$.

Finally, let n have prime factorization $p_1^{e_1}p_2^{e_2}\cdots p_r^{e_r}$ (so $e_i = \nu_{p_i}(n)$) with $r \geq 2$, in accordance with the second and third cases. Claim 1.5 then says that

$$\operatorname{ord}_n(a) \leq \operatorname{lcm}(\varphi(p_1^{e_1}), \varphi(p_2^{e_2}), \ldots, \varphi(p_r^{e_r})).$$

We can then find two prime powers among the $p_i^{e_i}$ greater than two (in the second case, the two odd prime powers; in the third case, the only two available prime powers). Letting $p_1^{e_1}$ and $p_2^{e_2}$ be these two prime powers, Claim 1.6 shows that $\varphi(p_1^{e_1})$ and $\varphi(p_2^{e_2})$ are even, so their least common multiple is less than their product.

Therefore, the value of $\operatorname{ord}_n(a)$ is bounded above by

$$\operatorname{lcm}(\varphi(p_1^{e_1}), \varphi(p_2^{e_2}), \ldots, \varphi(p_r^{e_r})) \lneq \varphi(p_1^{e_1})\varphi(p_2^{e_2})\cdots\varphi(p_r^{e_r}) = \varphi(p_1^{e_1}p_2^{e_2}\cdots p_r^{e_r}) = \varphi(n),$$

with the equality at the end being a result of the fact that $\varphi(a)\varphi(b) = \varphi(ab)$ when $\gcd(a,b) = 1$. □

Here's some extra content for the people who read the lecture notes. You may have noticed this $\operatorname{lcm}(\varphi(p^k), \varphi(q^m), \ldots)$ construct showing up a lot. This is because it naturally gives the maximal possible order modulo n (well, almost — you really want to halve $\varphi(2^k)$ for $k \geq 3$, whenever it shows up).

The true maximum-order function is the **Carmichael function**: supposing n has prime factorization $p_1^{e_1}p_2^{e_2}\cdots p_k^{e_k}$, the Carmichael function $\lambda(n)$ is defined as

$$\lambda(n) = \begin{cases} \frac{1}{2}\varphi(n) & n = 2^r \text{ for } r \geq 3 \\ \varphi(n) & n = p^r \text{ for odd primes } p, \text{ or } n = 1, 2, 4 \\ \operatorname{lcm}(\lambda(p_1^{e_1}), \lambda(p_2^{e_2}), \ldots, \lambda(p_k^{e_k})) & \text{otherwise.} \end{cases}$$

We can therefore sharpen Euler's theorem by saying

Theorem 1.6 (Stronger Euler's theorem)**.** For any relatively prime numbers $n \geq 2$ and a,

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

Finally, another small teaser for the Cyclotomic Polynomials unit: for which a and k does there exist a prime p for which $\operatorname{ord}_p(a) = k$?

2 Fermat's Christmas Theorem

We now introduce a very powerful theorem involving sums of two squares.

Theorem 2.1 (Fermat's Christmas Theorem)**.** Let n be an integer. Then, all odd prime factors of n^2+1 are $1 \pmod 4$.

Proof. This is not too hard with the theory in the previous section. The main idea is to observe that

$$n^2 \equiv -1 \pmod p$$

implies $n^4 \equiv 1 \pmod p$, so the order of n divides 4. However, 1 and 2 can obviously not be the order of n (otherwise n^2 would be $1 \pmod p$), hence the order is 4. Then,

$$4 \mid \varphi(p) = p-1$$

which by definition means $p \equiv 1 \pmod 4$. □

Conversely, we can also prove the following:

Theorem 2.2. If $p \equiv 1 \pmod 4$, then there exists an n for which p divides n^2+1.

Proof. We want to find a number whose order is 4 modulo p. To do this, we will exploit primitive roots: we already know that a primitive roots g has order $p-1$, so $a = g^{\frac{p-1}{4}}$ must have order 4. (You can also find a construction using Wilson's theorem.) □

The more general upshot of this is that we can always force the order to be any factor of $\varphi(n)$ if a primitive root exists.

Exercise 2.1. Extend the result of Exercise 1.2 — given a divisor d of $p-1$, how many of $\{1, 2, \ldots, p-1\}$ have order d?

We can say a little bit about general sums of squares, too. The following corollary is also referred to as Fermat's Christmas Theorem, and it is essentially equivalent.

Corollary 2.3. If a and b are positive integers, then $p \mid a^2+b^2$ implies

- $p = 2$, or
- $p \mid \gcd(a, b)$, or
- $p \equiv 1 \pmod 4$.

To belabor the point, if p is $3 \pmod 4$ and divides a^2+b^2, you know that it *has* to divide a and b separately. One immediate result of this is that $\nu_p(a^2+b^2)$ has to be even, just by successively dividing out p from a and b.

Remark 2.4 (Not orders, but interesting)**.** In fact, the set of sums of two squares can be characterized as "numbers for which $\nu_p(n)$ is even whenever $p \equiv 3 \pmod 4$." This is quite a bit stronger than Corollary 2.4!

3 Walkthroughs

Example 3.1

Find all positive integers n for which n divides $2^n - 1$.

Walkthrough. We will show that only $n = 1$ works. Assume for the sake of contradiction that $n > 1$, and take a prime $p \mid n$. The main idea then is to control the order of 2 (mod p)

(a) Let $d = \text{ord}_p(2)$. Show that $d \mid \gcd(n, p-1)$.

(b) Find a p such that $\gcd(n, p-1) = 1$.

(c) Conclude that the order of d modulo this choice of p is 1.

(d) Deduce a contradiction.

Example 3.2 (Qiao Zhang)

Find all integers n for which the sequence

$$\nu_2(3^0 - n),\ \nu_2(3^1 - n),\ \nu_2(3^2 - n),\ \ldots$$

is unbounded.

Walkthrough. We want

$$3^k \equiv n \pmod{2^m}$$

to have solutions for arbitrarily large m.

(a) Show that n is odd.

(b) What do we know about n by taking mod 8?

(c) List out all the possible values of $3^k \pmod{2^m}$ for $m = 4$, $m = 5$, and $m = 6$. Out of the remaining possible values of $n \pmod{2^m}$, which ones appear in your lists?

(d) Conjecture the general answer. What does this tell you about the order of 3 modulo 2^m?

(e) Show that the order of 3 is 2^{m-2} and conclude.

The most interesting part of this solution is **(d)**. We are leveraging the fact that the size of the range of $a^x \pmod n$ is precisely $\text{ord}_n(a)$, which means that computing the order lets us show that each of the 1 (mod 8) and 3 (mod 8) residues *must* appear in the image of 3^k. (This is also what tells you that part **(c)** is not very computationally intensive — at most, you will have to list out 28 numbers. Even going out to $m = 7$ is not so bad.)

Example 3.3 (USA TST 2008/4)
Prove that $n^7 + 7$ is not a perfect square for any integer n.

Walkthrough. Let's suppose that $n^7 + 7 = m^2$.

(a) Show that n cannot be less than zero.

(b) The crux of the problem is this pretty funny step: add a particularly nice three-digit integer c to both sides so that we have something to work with. (Hint: c is a square.)

(c) Prove that $n \equiv 1 \pmod 4$ and thus $n^7 + 7 + c$ has a prime factor that is $3 \pmod 4$.

(d) How many factors of p does $n + 2$ have?

(e) Get a contradiction by showing that $\nu_p(n^7 + 7 + c) = \nu_p(n + 2)$.

Funny observation: this solution is entirely reliant on the fact that, in fact, $n^7 - 7$ is a perfect square for some integer n.

Exercise 3.4. Prove that $n^3 + 7$ is not a perfect square for any integer n.

4 Extra Problems

4.1 Warm-ups

Problem 4.1 (USAMTS 2009 Round 2 Problem 2)

Prove that if a and b are positive integers such that 7^{2009} divides $a^2 + b^2$, then 7^{2010} divides ab.

Problem 4.2 (2019 AIME I/14)

Find the least odd prime factor of $2019^8 + 1$.

4.2 Random interesting order-adjacent things

Problem 4.3

Show that the Carmichael function has the promised maximal-order property: for each n, show that there exists an a such that $\text{ord}_n(a) = \lambda(n)$, and prove that no number has an order larger than $\lambda(n)$. Then, show that $\lambda(n) \mid \varphi(n)$ for all n.

Problem 4.4 (Carmichael numbers)

Fermat's little theorem tells us that $a^{p-1} \equiv 1 \pmod{p}$ for all primes p, as long as $\gcd(a, p) = 1$. Unfortunately, the converse fails to hold: it turns out that there exist composite integers n for which $a^{n-1} \equiv 1 \pmod{n}$ for all a satisfying $\gcd(a, n) = 1$. These are a type of pseudoprime (literally, fake prime) called **Carmichael numbers**.

Let n be a Carmichael number.

(a) Show that n is odd and squarefree (i.e. isn't divisible by the square of a prime).

(b) Can n have exactly two prime factors?

(c) What is the first Carmichael number? Parts (a) and (b) should narrow this search to about 20 numbers.

Problem 4.5 (Euler's criterion for quadratic residues)

A number r is a **quadratic residue** modulo n if is a perfect square mod n; that is, $x^2 \equiv r \pmod{n}$ for some integer x. Given that p is prime and does not divide a, prove that a is a quadratic residue if and only if

$$a^{\frac{p-1}{2}} \equiv 1 \pmod{p}.$$

Problem 4.6

Let $n \geq 2$ be an integer. For which values of k is the function $f(x) = x^k$ surjective modulo n? We say that a function g is surjective modulo n if, as x varies through the integers, $g(x)$ takes on all n possible values mod n.

4.3 Some actual contest problems

Problem 4.7 (HMMT November 2014 G10)

Suppose that m and n are integers with $1 \leq m \leq 49$ and $n \geq 0$ such that m divides $n^{n+1} + 1$. What is the number of possible values of m?

Problem 4.8 (MOP 2011)

Let p be a prime and n a positive integer. Suppose that $\nu_p(2^n - 1) = 1$. Must $\nu_p(2^{p-1} - 1) = 1$?

★ **Problem 4.9** (Krishna Pothapragada)

Show that, for all even integers n, the number of divisors of n does not divide $n^2 + 1$.

★ **Problem 4.10** (USEMO 2019/4)

Prove that for any prime p, there exists a positive integer n such that

$$1^n + 2^{n-1} + 3^{n-2} + \cdots + n^1 \equiv 2020 \pmod{p}.$$

★ **Problem 4.11** (IMO 1990/3)

Find all positive integers n for which n^2 divides $2^n + 1$.

5 Solutions to Walkthroughs

5.1 Solution 3.1

The answer is only $\boxed{n = 1}$, which clearly works because $1 \mid 2^1 - 1$. We now show that no other n work.

Suppose for the sake of contradiction that some $n > 1$ works. Let p be the smallest prime dividing n and d the order of n modulo p. Then, we have

$$2^{p-1} \equiv 1 \pmod{p}, \quad 2^n \equiv 1 \pmod{p}.$$

This means $d \mid p - 1$ and $d \mid n$, so d divides their greatest common divisor. However, since p is the smallest prime dividing n and all the divisors of $p - 1$ are smaller than p, $\gcd(n, p - 1) = 1$. This means $\operatorname{ord}_p(n)$ divides 1 and is therefore equal to 1, implying

$$2^1 \equiv 1 \pmod{p},$$

which is a contradiction.

5.2 Solution 3.2, Qiao Zhang

The answer is $\boxed{\text{all integers of the form } 8k + 1 \text{ and } 8k + 3}$.

Even n obviously don't work because $3^k - n$ is odd, and numbers that are $5 \pmod 8$ or $7 \pmod 8$ fail because $3^k - n$ is never divisible by 8 (just by reducing mod 8), so it remains to show that the rest of the numbers do work.

The key insight is that

> **Claim 5.1 —** As m goes from 1 to 2^{m-2}, $3^k \pmod{2^m}$ cycles through all the $1 \pmod 8$ and $3 \pmod 8$ residues modulo 2^m.

Proof. First, we show that $\operatorname{ord}_{2^m}(3) = 2^{m-2}$ — to show this, it suffices to prove that the order doesn't divide 2^{m-3}. In particular, we have

$$\begin{aligned} 3^{2^{m-3}} - 1 &= (3^{2^{m-4}} + 1)(3^{2^{m-4}} - 1) \\ &= (3^{2^{m-4}} + 1)(3^{2^{m-5}} + 1)(3^{2^{m-5}} - 1) \\ &= (3^{2^{m-4}} + 1)(3^{2^{m-5}} + 1)(3^{2^{m-6}} + 1)(3^{2^{m-6}} - 1) \\ &= \cdots \\ &= (3^{2^{m-4}} + 1)(3^{2^{m-5}} + 1) \cdots (3^m + 1)(3^m - 1), \end{aligned}$$

so $\nu_2(3^{2^{m-3}} - 1)$ is equal to $m - 4 + 3 = m - 1 < m$, hence $3^{2^{m-3}}$ is not $1 \pmod{2^m}$ as desired.

This means that $3^1, 3^2, \ldots, 3^{2^{m-2}}$ are all distinct modulo 2^m, since otherwise we could take two of them and divide to get $3^{\text{smaller number}} \equiv 1 \pmod{2^m}$. Moreover, none of these 2^{m-2} residues are even (cutting the possible space of numbers in half) or $5 \pmod 8$ or $7 \pmod 8$ (cutting the possible space of numbers in half again), so these residues map exactly to all the $1 \pmod 8$ and $3 \pmod 8$ residues. □

For example, the claim says that I should expect $3^k \pmod{32}$ to give me the 8 values 1, 3, 9, 11, 17, 19, 25, and 27 as k varies, which is in fact what happen (try it yourself!)s.

Finally, this means $3^k \equiv n \pmod{2^m}$ always has a solution for $n \equiv 1 \pmod 8$ or $n \equiv 3 \pmod 8$, regardless of how large m is, so $\nu_2(3^k - n)$ is unbounded for the claimed values of n.

5.3 Solution 3.3, USA TST 2008/4

Suppose for contradiction that

$$n^7 + 7 = m^2$$

for some integer m. Then, adding 121, we get

$$n^7 + 2^7 = m^2 + 11^2.$$

If n is even, then m is odd; however, the left-hand side is $0 \pmod 4$ because it's a multiple of 2^7, while the right-hand side is $2 \pmod 4$. Thus, n is odd, and more specifically $1 \pmod 4$.

By Christmas theorem, the primes dividing $m^2 + 11^2$ are either $1 \pmod 4$ or factors of $\gcd(m, 11)$. In the latter case, $\gcd(m, 11)$ is either 1 or 11, so if a prime divides $m^2 + 11^2$, it's either $1 \pmod 4$ or 11. Factoring the left-hand side then shows

$$(n+2)(n^6 - 2n^5 + 4n^4 - 8n^3 + 16n^2 - 32n + 64) = m^2 + 11^2.$$

Since $n+2 \equiv 3 \pmod 4$, it has a prime factor that is $3 \pmod 4$, so $11 \mid n+2$. Additionally, $\nu_{11}(n+2)$ is odd because, again, $n + 2 \equiv 3 \pmod 4$.

Now, since $n \equiv -2 \pmod{11}$, the other factor of $n^7 + 2^7$ is

$$n^6 - 2n^5 + 4n^4 - 8n^3 + 16n^2 - 32n + 64 \equiv 64 \cdot 6 \equiv 10 \pmod{11}$$

and thus not a multiple of 11.

Putting it all together,

$$\nu_{11}(m^2 + 11^2) = \nu_{11}(n^7 + 2^7) = \nu_{11}(n+2)$$

because $n^6 - 2n^5 + 4n^4 - 8n^3 + 16n^2 - 32n + 64$ doesn't contribute any factors of 11. However, $\nu_{11}(m^2 + 11^2)$ is even since $11 \equiv 3 \pmod 4$, while $\nu_{11}(n+2)$, as established earlier, is odd. This is our desired contradiction.