Orders Modulo A Prime

Evan Chen

March 6, 2015

In this article I develop the notion of the order of an element modulo n, and use it to prove the famous n^2+1 lemma as well as a generalization to arbitrary cyclotomic polynomials.

References used in preparing this article are included in the last page.

1 Introduction

I might as well state one of the main results of this article up front, so the following discussion seems a little more motivated.

Theorem 1.1

Let p be an odd prime. Then there exists an integer n such that $p \mid n^2+1$ if and only if $p \equiv 1 \pmod 4$.

By introducing the notion of order, we will prove that $p \mid n^2+1 \Rightarrow p \equiv 1 \pmod 4$. By introducing the notion of a primitive root, we will prove the converse direction. Finally, we will write down the generalized version of this n^2+1 lemma using cyclotomic polynomials.

2 Orders

Let p be a prime and take $a \not\equiv 0 \pmod p$. The **order**[1] of $a \pmod p$ is defined to be the smallest positive integer m such that

$$a^m \equiv 1 \pmod p.$$

This order is clearly finite because **Fermat's Little Theorem** tells us

$$a^{p-1} \equiv 1 \pmod p,$$

id est, the order of a is at most $p-1$.

Exhibited below are the orders of each $a \pmod{11}$ and $a \pmod{13}$.

a	mod 11	mod 13
1	1	1
2	10	12
3	5	3
4	5	6
5	5	4
6	10	12

a	mod 11	mod 13
7	10	12
8	10	4
9	5	3
10	2	6
11		12
12		2

[1]Some sources denote this as $\operatorname{ord} a \pmod p$ or $\operatorname{ord}_p a$, but we will not.

One observation you might make about this is that it seems that the orders all divide $p-1$. Obviously if $m \mid p-1$, then $a^{p-1} \equiv 1 \pmod{p}$ as well. The miracle of orders is that the converse of this statement is true in an even more general fashion.

Theorem 2.1 (Fundamental Theorem of Orders)
Suppose $a^N \equiv 1 \pmod{p}$. Then the order of $a \pmod{p}$ divides N.

Proof. Important exercise (*mandatory* if you haven't seen it before). As a hint, use the division algorithm. □

To drive the point home:

The only time when $a^N \equiv 1 \pmod{p}$ is when the order of a divides N.

That's why considering the order of an element is often a good idea when faced with such an expression. The observation that the orders all divide $p-1$ follows from combining Fermat's Little Theorem with Theorem 2.1.

Believe it or not, this is already enough to prove one direction of Theorem 1.1.

Proposition 2.2
For an odd prime p, if $n^2 \equiv -1 \pmod{p}$, then $p \equiv 1 \pmod{4}$.

Proof. The point is that squaring both sides gives $n^4 \equiv 1 \pmod{p}$. Now we claim that the order of n modulo p is exactly 4. If not, it must be either 2 or 1, which implies $n^2 \equiv 1 \pmod{p}$. But since we assumed $n^2 \equiv -1 \pmod{p}$, that's impossible.

Hence the order is 4. Since all orders divide $p-1$, we derive $4 \mid p-1$ as desired. □

Remark. Theorem 2.1 (and much of the discussion preceding it) still holds if we replace the prime p with any positive integer n such that $\gcd(a, n) = 1$. In that case we replace $p-1$ with just $\phi(n)$.

3 Primitive Roots

Now we want to prove the other direction of this. The morally correct way to do so is to use something called a primitive root.

Theorem 3.1
Let p be a prime. Then there exists an integer g, called a **primitive root**, such that the order of g modulo p equals $p-1$.

This theorem can be quoted on a contest without proof. Its proof is one of the practice problems.

The point of this theorem is that given a primitive root g, each nonzero residue modulo p can be **expressed uniquely** by g^α, for $\alpha = 1, 2, \ldots, p-1$.

Exercise 3.2. Suppose $p = 2m+1$. Verify that

$$g^m \equiv -1 \pmod{p}.$$

(If you get stuck, try reading the rest of this section first.)

Example 3.3 (Primitive Roots Modulo 11 and 13)
It turns out that $g = 2$ is a primitive root modulo both 11 and 13. Let's write this out.

2^n	mod 11	mod 13
2^1	2	2
2^2	4	4
2^3	8	8
2^4	5	3
2^5	$\boxed{10}$	6
2^6	9	$\boxed{12}$
2^7	7	11
2^8	3	9
2^9	6	5
2^{10}	1	10
2^{11}		7
2^{12}		1

I've boxed the two "half-way" points: $2^5 \equiv 10 \equiv -1 \pmod{11}$ and $2^6 \equiv 12 \equiv -1 \pmod{13}$.

Consider $p = 11$. We already know that -1 cannot be a square modulo p, and you can intuitively see this come through: since $\frac{p-1}{2} = 5$ is odd, it's not possible to cut $g^5 \equiv -1$ into a perfect square.

On the other hand, if $p = 13$ then $p \equiv 1 \pmod 4$, and you can see intuitively why $g^6 \equiv -1$ is a perfect square: just write $g^6 = (g^3)^2$ and we're home free!

See if you can use this to complete the proof of the other direction of this theorem.

Proposition 3.4
If $p \equiv 1 \pmod 4$ is a prime, then there exists an n such that $n^2 \equiv -1 \pmod p$.

Proof. Let g be a primitive root modulo p and let $n = g^{\frac{p-1}{4}}$. Why does this work? □

I had better also state the general theorem.

Theorem 3.5 (Primitive Roots Modulo Non-Primes)
A primitive root modulo n is an integer g with $\gcd(g, n) = 1$ such that g has order $\phi(n)$. Then a primitive root mod n exists if and only if $n = 2$, $n = 4$, $n = p^k$ or $n = 2p^k$, where p is an odd prime.

Exercise 3.6. Show that primitive roots don't exist modulo any number of the form pq for distinct odd primes p, q. (Use the Chinese Remainder Theorem to show that $x^{\text{lcm}(p-1,q-1)} \equiv 1$ for suitable x).

You are invited to extend the result of this exercise to prove that if $n \notin \{2, 4, p^k, 2p^k\}$ then no primitive roots exists modulo n. (This is not difficult, just a little annoying.)

4 The Cyclotomic Generalization

So we've seen the polynomial x^2+1 is somehow pretty special, in part because it divides x^4-1 and thus lets us use the idea of orders. You might also have seen the polynomials x^2+x+1 and x^2-x+1 show up in some problems; they divide x^3-1 and x^3+1, respectively, and you might suspect similar results might hold.

Our goal now is to develop a more general result involving the irreducible factors of x^n-1, thus taking us beyond just the case $n=4$. The definition is a little technical, so bear with me for a little bit.

Definition 4.1. A complex number z is called a **primitive nth root of unity** if

$$z^n = 1$$

and moreover $z^k \neq 1$ for $k = 1, 2, \dots, n-1$. In other words, z^n is the *first* power which is 1.

Exercise 4.2. Let n be a fixed integer, and define

$$\zeta_n = \cos\left(\frac{2\pi}{n}\right) + i\sin\left(\frac{2\pi}{n}\right).$$

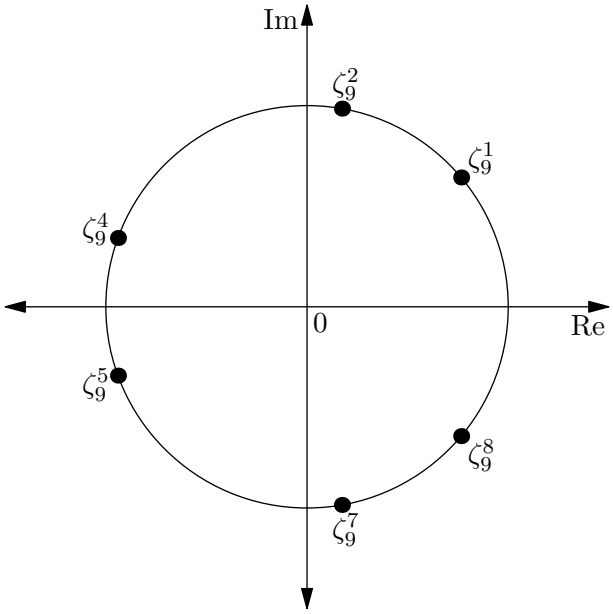
Show that the primitive nth roots of unity are exactly the numbers

$$\cos\left(\frac{2\pi k}{n}\right) + i\sin\left(\frac{2\pi k}{n}\right) = \zeta_n^k$$

where $1 \le k \le n$, and $\gcd(k,n) = 1$. In particular, the number of primitive nth roots of unity is $\phi(n)$.

Note that in particular, 1 is considered a primitive nth root of unity only when $n = 1$.

You can thus see these numbers visually on the complex plane. For example, below we exhibit the primitive 9th roots of unity, of which there are $\phi(9) = 6$.



Definition 4.3. The **nth cyclotomic polynomial** is the monic polynomial $\Phi_n(x)$ whose roots are exactly the primitive nth roots of unity; that is,

$$\Phi_n(X) = \prod_{\substack{\gcd(k,n)=1 \\ 1 \le k \le n}} \left(X - \zeta^k\right).$$

Example 4.4
Because the primitive fourth roots of unity are i and $-i$, we have

$$\Phi_4(X) = (X-i)(X+i) = X^2+1.$$

One can actually show $\Phi_n(X)$ always has integer coefficients. (In fact, it's the polynomial of *minimal* degree with this property.)

Proposition 4.5 (Cyclotomic Polynomials Divide X^n-1)
For any integer n, we have

$$X^n - 1 = \prod_{d \mid n} \Phi_d(X).$$

In particular, if p is a prime then

$$\Phi_p(X) = \frac{X^p-1}{X-1} = X^{p-1} + X^{p-2} + \cdots + 1.$$

Exercise 4.6. Prove this result. (If you don't see why, do the case $n=4$ first.)

Example 4.7
To write this lemma out explicitly for the cases $2 \le n \le 8$:

$$\begin{aligned}
X^2-1 &= (X-1)(X+1) \\
X^3-1 &= (X-1)(X^2+X+1) \\
X^4-1 &= (X-1)(X+1)(X^2+1) \\
X^5-1 &= (X-1)(X^4+X^3+X^2+X+1) \\
X^6-1 &= (X-1)(X+1)(X^2+X+1)(X^2-X+1) \\
X^7-1 &= (X-1)(X^6+X^5+X^4+X^3+X^2+X+1) \\
X^8-1 &= (X-1)(X+1)(X^2+1)(X^4+1)
\end{aligned}$$

We observe a "new" polynomial appearing at each level; these are the cyclotomic polynomials.

$$\begin{aligned}
\Phi_2(X) &= X+1 \\
\Phi_3(X) &= X^2+X+1 \\
\Phi_4(X) &= X^2+1 \\
\Phi_5(X) &= X^4+X^3+X^2+X+1 \\
\Phi_6(X) &= X^2-X+1 \\
\Phi_7(X) &= X^6+X^5+\cdots+1 \\
\Phi_8(X) &= X^4+1
\end{aligned}$$

Why is all of this in a number theory handout? Because of this:

Theorem 4.8 (Divisors of Cyclotomic Values)
Let p be a prime, n a positive integer and a any integer. Suppose that

$$\Phi_n(a) \equiv 0 \pmod{p}.$$

Then either

- a has order n modulo p, and hence $p \equiv 1 \pmod{n}$, or
- p divides n.

Remark 4.9 (How to Remember This Theorem)**.** You can kind of see why this should not be *too* surprising. The idea is that

$$\Phi_n \text{ is the polynomial which annihilates complex numbers of "order" } n.$$

So you might expect modulo p, Φ_n kills the integers which are of order n, and in particular that $p \equiv 1 \pmod{n}$ if any such integers exist. This theorem says that, except for the few "edge cases" where $p \mid n$, this intuition is right.

Proof. Suppose $\Phi_n(a) \equiv 0 \pmod{p}$. By Proposition 4.5, we deduce that $a^n - 1 \equiv 0 \pmod{p}$. So the order m of $a \pmod{p}$ divides n. Thus, we have two cases.

- If $m = n$, we are done: $n = m \mid p - 1$.
- Suppose $m < n$ (but still $m \mid n$). Now,

$$0 \equiv a^m - 1 = \prod_{d \mid m} \Phi_d(a) \pmod{p}.$$

Hence, not only do we have $\Phi_n(a) = 0$, but we also have $\Phi_d(a) = 0$ for some $d \mid m$. (Here $d \le m < n$.) Thus a is a *double root* of the polynomial

$$X^n - 1 = \prod_{d \mid n} \Phi_d(X) \pmod{p}.$$

So we can *take the derivative* of this polynomial modulo p to obtain $nX^{n-1} \pmod{p}$, without changing the fact that a is a root. If $p \mid n$ this is in fact the zero polynomial and we are done. But if $p \nmid n$ then we can only have $a \equiv 0 \pmod{p}$ (what else is a root of X^{n-1}?), which is impossible. □

So in fact, Theorem 1.1 is just the $n = 4$ case of Theorem 4.8!

5 Example Problems

Example 5.1 (MOP 2011)
Let p be a prime and n a positive integer. Suppose that p^1 fully divides $2^n - 1$ (meaning it is divisible by p but not p^2). Prove that p^1 fully divides $2^{p-1} - 1$.

Solution. Obviously $p \neq 2$, so assume p is odd.

Naturally, we consider the order of 2 modulo p; denote this number by m (so $p \mid 2^m - 1$). We automatically know that m divides both n and $p-1$. From $m \mid n$ we derive that

$$p \mid 2^m - 1 \mid 2^n - 1.$$

Now note that $2^n - 1$ has exactly one power of p in its prime factorization. Hence from the above we can deduce that $2^m - 1$ has exactly one power of p as well (it has at least one since $p \mid 2^m - 1$ and at most one since it divides $2^n - 1$). In this way we've eliminated n entirely from the problem.

So it remains to show that, if p^1 divides $2^m - 1$, then $2^{p-1} - 1$ does not gain any prime factors of p. So we consider the quotient

$$\frac{2^{p-1}-1}{2^m-1} = 1 + 2^m + (2^m)^2 + \cdots + (2^m)^{\frac{p-1}{m}-1}.$$

Our goal is to show this isn't divisible by p. Taking it modulo p, however, we get

$$\frac{2^{p-1}-1}{2^m-1} \equiv \underbrace{1+1+\cdots+1}_{\frac{p-1}{m} \text{ terms}} = \frac{p-1}{m} \pmod{p}$$

Since $0 < \frac{p-1}{m} < p$, the conclusion follows. □

If you really understand the above example, you have my permission to look up the so-called "Lifting the Exponent" lemma, which you may find useful in the practice problems. The reason I don't include it here is that I find many students commit the result to memory without actually understanding the proof of the lemma. Actually, the proof of the lemma is extremely natural, and if you understand the above solution you should not have much difficulty proving the lemma yourself. Specifically, you need only check that

- If $a \equiv b \not\equiv 0 \pmod{p}$ and $p \nmid n$, then $\frac{a^n-b^n}{a-b} \not\equiv 0 \pmod{p}$, and
- If $p \mid t$ and $a \not\equiv 0 \pmod{p}$ then p fully divides $\frac{1}{t}\left((a+t)^p - a^p\right)$.

Once you can prove this, you immediately obtain the following.

Lemma 5.2 (Lifting the Exponent)
Let p be an odd prime and let $\nu_p(n)$ be the exponent of p in the prime factorization of n. If $a \equiv b \not\equiv 0 \pmod{p}$ then $\nu_p(a^n - b^n) = \nu_p(n) + \nu_p(a-b)$.

On many olympiad problems, one only needs a particular case of this lemma (e.g. $\nu_p(n) = 0$) and it is completely reasonable to re-derive that special case on the spot. This is exactly what I did in MOP 2011.

Example 5.3 (Folklore)
Find all positive integers n such that n divides $2^n - 1$.

Solution. As you might guess after some experimentation, the only n which works is $n = 1$. It's obvious that n has to be odd (since $2^n - 1$ is always odd). But how can we show this?

Let us first consider any prime p dividing n. We get that $p \mid 2^n - 1$, or $2^n \equiv 1 \pmod{p}$. So practically the problem is saying that

For any prime $p \mid n$, the order of 2 mod p also divides n.

(If we're really unlucky, we might have to consider prime powers too, but whatever.)

This gives us an idea: let's take the *smallest* prime p dividing n (noting that $p > 2$). Let m denote the order of 2 modulo p (keeping in mind that $p \neq 2$). Then the order m has to divide n, but it also has to divide $p-1$. This can only occur if $m = 1$, which is impossible! □

The above solution illustrates a trick perhaps worth mentioning explicitly.

Lemma 5.4 (GCD Trick)
If $a^m \equiv 1 \pmod N$ and $a^n \equiv 1 \pmod N$ then

$$a^{\gcd(m,n)} \equiv 1 \pmod N.$$

This is just the famous fact that $\gcd(a^m - 1, a^n - 1) = a^{\gcd(m,n)} - 1$ phrased using modular arithmetic.

Finally, here is a fun and perhaps somewhat unexpected application of cyclotomic polynomials. In fact, you may have seen the special case $n = 4$ already; now that we have the full cyclotomic generalization we can prove a much more general fact.

Example 5.5 (Weak Dirichlet)
Show that there are infinitely many primes which are congruent to 1 modulo n for any positive integer n.

Solution. Suppose there were only finitely many such primes p_1, p_2, …, p_N. Look at the number

$$M = \Phi_n(np_1p_2 \dots p_N).$$

As a polynomial, $\Phi_n(X)$ has roots which are all roots of unity (meaning they have norm 1), so its constant term can only be ± 1. Now take p dividing M, and apply Theorem 4.8. □

6 Practice Problems

Not all of the problems below actually invoke the concept of order in the solution. However, the intuition about how exponents behave should nonetheless prove useful (hopefully).

Problem 6.1. The decimal representations of $\frac{1}{7}$, $\frac{2}{7}$, …, $\frac{6}{7}$ are $0.\overline{142857}$, $0.\overline{285714}$, …, $0.\overline{857142}$, which surprisingly are all cyclic shifts of each other. Is this a coincidence?

Problem 6.2 (Euler)**.** Prove that all factors of $2^{2^n} + 1$ are of the form $k \cdot 2^{n+1} + 1$.

Problem 6.3 (IMO 2005/4)**.** Determine all positive integers relatively prime to all terms of the infinite sequence $a_n = 2^n + 3^n + 6^n - 1$ for $n \geq 1$.

Problem 6.4. Let n be a positive integer and $p > n + 1$ a prime. Prove that p divides

$$1^n + 2^n + \cdots + (p-1)^n.$$

Problem 6.5 (China TST 2006)**.** Find all positive integers a and n such that

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

is an integer.

Problem 6.6 (Romania TST 1996)**.** Find all primes p and q such that for every integer n, the number $n^{3pq} - n$ is divisible by $3pq$.

Problem 6.7 (HMMT November 2014)**.** Determine all positive integers $1 \le m \le 50$ for which there exists an integer n for which m divides $n^{n+1} + 1$.

Problem 6.8 (Taiwan IMO 2014 Team Selection Quiz)**.** Alice and Bob play the following game. They alternate selecting distinct nonzero digits (from 1 to 9) until they have chosen seven such digits, and then consider the resulting seven-digit number (i.e. $\overline{A_1B_2A_3B_4A_6B_6A_7}$). Alice wins if and only if the resulting number is the last seven decimal digits of some perfect seventh power. Please determine which player has the winning strategy.

Problem 6.9 (Shortlist 2006 N5)**.** Show that

$$\frac{x^7 - 1}{x - 1} = y^5 - 1$$

doesn't have integer solutions.

Problem 6.10 (IMO 1990/3)**.** Find all positive integers n such that n^2 divides $2^n + 1$.

Problem 6.11. Let $p > 5$ be a prime. In terms of p, compute the remainder when

$$\prod_{m=1}^{p-1} \left(m^2 + 1\right)$$

is divided by p.

Problem 6.12 (Online Math Open)**.** Find all integers m with $1 \le m \le 300$ such that for any integer n with $n \ge 2$, if $2013m$ divides $n^n - 1$ then $2013m$ also divides $n - 1$.

Problem 6.13 (Shortlist 2012 N2)**.** Find all positive integers $x \le y \le z$ which obey

$$x^3(y^3 + z^3) = 2012(xyz + 2).$$

Problem 6.14 (USA TST 2008)**.** Prove that $n^7 + 7$ is never a perfect square for positive integers n.

Problem 6.15 (USAMO 2013/5)**.** Let m and n be positive integers. Prove that there exists an integer c such that cm and cn have the same nonzero decimal digits.

Problem 6.16 (IMO 2003/6)**.** Let p be a prime number. Prove that there exists a prime number q such that for every integer n, the number $n^p - p$ is not divisible by q.

Problem 6.17. Prove that modulo any prime p there exists a primitive root!

7 Hints

6.1. 10 is a primitive root modulo 7.

6.2. It's sufficient to prove the result when m is prime. Find the order of 2.

6.3. Try to pick $n = -1$.

6.4. Eradicated by primitive roots.

6.5. What happens when $a = 1$? Mimic the example.

6.6. First show $\{3, p, q\}$ are distinct. Then use primitive roots modulo p and q to get some divisibility relations, and finish by bounding.

6.7. All odd m work. For the other cases, use the $n^2 + 1$ lemma.

6.8. Primitive roots exist modulo prime powers. This is a fairly dumb game and Alice wins. (Also, don't forget the word "distinct".)

6.9. The left-hand side is the seventh cyclotomic polynomial.

6.10. Use the smallest prime trick, but this time $p = 3$ is a possibility. Use lifting the exponent to eliminate it.

6.11. Evaluate the polynomial $\prod_{m=1}^{p-1}(X + m)$ carefully mod p, and plug in $X = \pm i$.

6.12. Call a number *good* if $n^n \equiv 1 \pmod m \Rightarrow n \equiv 1 \pmod m$. Characterize all good numbers. (For example, why is 10 good?)

6.13. This problem is a little involved. First limit the possible values of x. Then try and show $503 \mid y + z$. Set $y + z = 503k$ and do some bounding.

6.14. Add 121 to both sides.

6.15. $10 \pmod{7^k}$.

6.16. For this to work we must have $q = pk + 1$. Then $n^p \equiv p \Leftrightarrow 1 \equiv p^k$. See if you can pick a q such that p has order r modulo q but $k \not\equiv 1 \pmod r$, where r is a prime of your choice.

6.17. From [4]: Consider the cyclotomic polynomial $\Phi_{p-1}(X) \mid X^{p-1} - 1$. Show that it factors completely modulo p, and pick any root.

References

[1] **Exponents and Primes**, by Alexander Remorov, Canada IMO 2010 Winter Training.

[2] **Order and Primitive Roots**, Canada IMO 2010 Summer Training.

[3] **Exponents in Number Theory**, Evan Chen, 2014 A* Winter Math Camp.

[4] **Cyclotomic Polynomials in Olympiad Number Theory**, Lawrence Sun.

[5] **Elementary Properties of Cyclotomic Polynomials**, Yimin Ge.

[6] **Lifting the Exponent**, Amir Hossein.