Order and Quadratic Reciprocity

Rishabh Das

New York City Math Team

1 Euler's Theorem

Definition (Euler's Totient Function)
Let $\varphi(n)$ denote the number of elements of $\{1, 2, \ldots, n\}$ that are relatively prime to n.

Lemma (Computing $\varphi(n)$)
If $n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$ is the prime factorization of n, then

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_k}\right) = p_1^{a_1-1} p_2^{a_2-1} \cdots p_k^{a_k-1}(p_1 - 1)(p_2 - 1)\cdots(p_k - 1)$$

This lemma will not be proven here, but can be proven using the Chinese Remainder Theorem and proving $\varphi(p^l) = p^{l-1}(p-1)$, where p is a prime.

Theorem 1 (Euler's Theorem)
If $\gcd(a, n) = 1$, then

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

Proof. Let $\{n_1, n_2, \ldots, n_{\varphi(n)}\}$ be the set of positive integers less than or equal to n that are relatively prime to n. Note that an_i is relatively prime to n. Also note that if $an_i \equiv an_j \pmod{n}$:

$$an_i \equiv an_j \pmod{n} \implies a(n_i - n_j) \equiv 0 \pmod{n}.$$

Since $\gcd(a, n) = 1$, we must have $n_i - n_j \equiv 0 \pmod{n}$. Since $1 \le n_i, n_j \le n$, this implies $n_i = n_j$, or $i = j$. Thus, $\{n_1, n_2, \ldots n_{\varphi(n)}\} \equiv \{an_1, an_2, \ldots an_{\varphi(n)}\} \pmod{n}$. Multiplying all the elements of these two sets together, we can see:

$$(n_1 n_2 \cdots n_{\varphi(n)}) \equiv a^{\varphi(n)}(n_1 n_2 \cdots n_{\varphi(n)}) \pmod{n}.$$

Since $n_1 n_2 \cdots n_{\varphi(n)}$ is relatively prime to n, $a^{\varphi(n)} \equiv 1 \pmod{n}$. □

Corollary (Fermat's Little Theorem)
If p is a prime and $p \nmid a$, $a^{p-1} \equiv 1 \pmod{p}$.

This follows since $\varphi(p) = p - 1$ for prime p.

Exercises

Exercise 1. Find the last two digits of 17^{83}

Exercise 2. Find the last two digits of 227^{227}

Exercise 3. Find the last two digits of 38^{2019}

2 Order

Definition (Order)
If $\gcd(a, n) = 1$, we denote the smallest positive integer d such that $a^d \equiv 1 \pmod{n}$ be $d = \text{ord}_n(a)$.

Note that by Euler's Theorem, $\text{ord}_n(a)$ will exist.

Theorem 2 (Fundamental Theorem of Order)
If $\gcd(a, n) = 1$ and $a^k \equiv 1 \pmod{n}$, then $\text{ord}_n(a) \mid k$.

Proof. Let $d = \text{ord}_n(a)$. By the division algorithm, we can write $k = qd + r$ where $0 \le r < d$. Then we have:

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

However, by the definition of d, we have $a^d \equiv 1 \pmod{n}$, so $a^{qd} \equiv 1 \pmod{n}$. Thus, we have $a^r \equiv 1 \pmod{n}$.
If r is a positive integer, since $r < d$, we get a contradiction of the minimality of d. Thus, $r = 0$ and $d \mid k$. □

Corollary
$\text{ord}_n(a) \mid \varphi(n)$ by Euler's Theorem and the fundamental theorem of order.

This corollary is very powerful. To show its strength, we will use an example.

Example. Find $\text{ord}_{23}(5)$

By Euler's theorem, the answer must be at most $\varphi(23) = 22$. However, without our corollary, we would have to check every single number between 1 and 21, inclusive. If we use our corollary, we can immediately find that the answer must be a divisor of 22, so it is one of $\{1, 2, 11, 22\}$. We can immediately see that it is not 1 or 2. Thus, we are left to check 11, since we already know 22 will work by Euler's Theorem.
To check if 11 works or not, we notice that $5^2 \equiv 2 \pmod{23}$. Thus:

$$5^{11} \equiv 2^5 \cdot 5 \equiv 32 \cdot 5 \equiv 9 \cdot 5 \equiv -1 \pmod{23}.$$

Since 11 does not work, $\text{ord}_{23}(5) = 22$.

If $\text{ord}_n(a) = \varphi(n)$, we call a a *primitive root* modulo n. Since $\text{ord}_{23}(5) = \varphi(23)$, 5 is a primitive root modulo 23. While it will not be proven here, there exists a primitive root modulo any prime number. (In fact, there exists a primitive root with modulo n if and only if n is of the form $1, 2, 4, p^k, 2p^k$ for an odd prime p.)

Exercises

Exercise 1. Compute $\text{ord}_{13}(3)$

Exercise 2. Compute $\text{ord}_{17}(3)$

Exercise 3. If $\text{ord}_n(a) \mid n - 1$ for all a such that $\gcd(a, n) = 1$, must n be prime?

3 Problems

Problem 1. (a) Show that if p is an odd prime such that $p \mid x^2+1$, then $p \equiv 1 \pmod 4$
(b) Show that if $p \equiv 3 \pmod 4$ and $p \mid x^2+y^2$, then $p \mid x$ and $p \mid y$.

Problem 2. (2019 AIME 1 #14) Find the least odd prime factor of 2019^8+1.

Problem 3. Let $F_n = 2^{2^n}+1$ be the nth Fermat number. Show that if p is a prime such that $p \mid F_n$, then $p \equiv 1 \pmod{2^{n+1}}$

Problem 4. Prove that if n is not of the form $1, 2, 4, p^k$, or $2p^k$ for odd primes p then there does not exist a primitive root modulo n.

Problem 5. Show that for any prime $p \neq 2, 5$, the period of the decimal representation of $\frac{1}{p}$ is $\text{ord}_p(10)$.

Problem 6. Find all n such that $n \mid 2^n-1$. (Hint: Suppose $n>1$, and let p be the smallest prime divisor of n. What can we say about p?)

Problem 7. (a) If p, q are primes such that $q \mid 1+x+x^2+\cdots+x^{p-1}$, then $q=p$ or $q \equiv 1 \pmod p$.
(b) (IMO Shortlist 2006) Find all integer solutions of the equation $\dfrac{x^7-1}{x-1} = y^5-1$

4 Legendre Symbol and Quadratic Reciprocity

Let p be an odd prime. We say a number a is a *quadratic residue* mod p if and only if there exists an integer x such that $x^2 \equiv a \pmod p$.

Theorem 3

There are exactly $\frac{p+1}{2}$ quadratic residues in the range $\{0, 1, 2, \dots, p-1\}$.

Proof. We will first deal with nonzero quadratic residues.
Let $a \not\equiv b \pmod p$. Then if $a^2 \equiv b^2 \pmod p$:

$$a^2 - b^2 \equiv 0 \pmod p$$

$$(a+b)(a-b) \equiv 0 \pmod p$$

$$a+b \equiv 0 \pmod p$$

$$a \equiv -b \pmod p$$

Thus, we pair $(1, p-1), (2, p-2), \dots, \left(\frac{p-1}{2}, \frac{p+1}{2}\right)$. When each of these residues are squared, two squares will be the same if and only if they are in the same pair. Thus, this is $\frac{p-1}{2}$ quadratic residues. 0 gives $\frac{p+1}{2}$. ☐

Definition (Legendre Symbol)

For any *odd prime* p, define

$$\left(\frac{a}{p}\right) = \begin{cases} 0 \text{ if } p|a \\ 1 \text{ if } a \text{ is a quadratic residue mod } p \\ -1 \text{ otherwise} \end{cases}$$

Corollary

There are exactly $\left(\frac{a}{p}\right)+1$ solutions to $x^2 \equiv a \pmod p$

Theorem 4 (Euler's Criterion)

$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod p$

Proof. If $p|a$ the proof is easy. If $\left(\frac{a}{p}\right)=1$, then write $x^2 \equiv a \pmod p$. Then $a^{\frac{p-1}{2}} \equiv x^{p-1} \equiv 1 \pmod p$ by Fermat.

Assume $\left(\frac{a}{p}\right) = -1$. It is clear that $\left\{a \cdot 1^2, a \cdot 2^2, \ldots, a \cdot \left(\frac{p-1}{2}\right)^2\right\}$ is a set of all non-quadratic residues, because from the proof of theorem 4.1, $\left\{1^2, 2^2, \ldots, \left(\frac{p-1}{2}\right)^2\right\}$ forms a set of all nonzero quadratic residues. Thus:

$$(p-1)! \equiv \prod_{r=1}^{\frac{p-1}{2}} (r^2)(ar^2) \equiv a^{\frac{p-1}{2}} \prod_{r=1}^{\frac{p-1}{2}} (r(p-r))^2 \equiv a^{\frac{p-1}{2}}[(p-1)!]^2$$

By Wilson's Theorem, $a^{\frac{p-1}{2}} \equiv -1 \equiv \left(\frac{a}{p}\right) \pmod p$ □

This theorem is extremely useful. It absolutely trivializes the following useful result.

Theorem 5 (Multiplicative Property of Legendre Symbol)

$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$

Proof.

$$\left(\frac{ab}{p}\right) \equiv (ab)^{\frac{p-1}{2}} \equiv a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \pmod p,$$

so $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$. □

We now will present Gauss's Lemma.

Lemma (Gauss's Lemma)

Let p be an odd prime and a be an integer relatively prime to p. Consider the set

$$S_p = \left\{a, 2a, 3a \ldots, \frac{p-1}{2} \cdot a\right\}.$$

After reducing each element in this set $\bmod p$ (such that each element is an integer between 0 and $p-1$ inclusive), let the number of elements that are larger than $\frac{p}{2}$ be n. Then $\left(\frac{a}{p}\right) = (-1)^n$.

Proof. First of all, note that there are $\frac{p-1}{2}$ elements of S_p, meaning that they are all distinct mod p. Then let $b_1, b_2, \ldots, b_m$ be the elements of S_p that are less than $\frac{p}{2}$, and $c_1, c_2, \ldots, c_n$ bet the elements of S_p that are greater than $\frac{p}{2}$. Note that $m+n=\frac{p-1}{2}$.

Consider the numbers $0 < b_1, b_2, \ldots, b_m, p - c_1, p - c_2, \ldots, p - c_n < \frac{p}{2}$. I claim all $\frac{p-1}{2}$ of these numbers are distinct. Note that $b_i \neq b_j$ and $c_i \neq c_j$ for $i \neq j$. Assume that $b_i = p - c_j$ for some i, j. Then:

$$b_i + c_j \equiv sa + ta \equiv 0 \pmod{p}$$

for some $0 < s, t \leq \frac{p-1}{2}$. Since a is relatively prime to p, we have $p \mid s + t$. However, the range condition on $s + t$ gives a contradiction.
Thus, $\{b_1, b_2, \ldots, b_m, p - c_1, p - c_2, \ldots, p - c_n\} = \{1, 2, \ldots, \frac{p-1}{2}\}$. Now we compute:

$$a(2a)(3a)\cdots\left(\frac{p-1}{2}\right)a = a^{\frac{p-1}{2}}\left(\frac{p-1}{2}\right)! \equiv (-1)^n b_1 b_2 \cdots b_m c_1 c_2 \cdots c_n \equiv (-1)^n \left(\frac{p-1}{2}\right)! \pmod{p}$$

and thus $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \equiv (-1)^n \pmod{p}$, and the proof is complete. □

Now we present Eisenstein's Lemma.

Lemma (Eisenstein's Lemma)

Let p be an odd prime and let a be an odd integer relatively prime to p. If we define $\alpha(a,p) = \displaystyle\sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{ka}{p} \right\rfloor$, then $\left(\frac{a}{p}\right) = (-1)^{\alpha(a,p)}$.

Proof. We use the same notation presented in the proof of Gauss's Lemma.
Note that $ka = p \cdot \left\lfloor \frac{ka}{p} \right\rfloor + r$ where r is the remainder when ka is divided by p. Then:

$$\sum_{k=1}^{\frac{p-1}{2}} ka = p \sum_{k=0}^{\frac{p-1}{2}} \left\lfloor \frac{ka}{p} \right\rfloor + \sum_{i=1}^{m} b_i + \sum_{j=1}^{n} c_j$$

Also check that

$$\sum_{k=1}^{\frac{p-1}{2}} k = \sum_{i=1}^{m} b_i + pn - \sum_{j=1}^{n} c_j$$

Subtracting these two statements gives

$$(a-1)\sum_{k=1}^{\frac{p-1}{2}} k = p \cdot \alpha(a,p) + 2\sum_{j=1}^{n} c_j - pn$$

Since a is odd, taking this $\bmod 2$ gives $\alpha(a,p) \equiv n \pmod{2}$, and thus we are done from Gauss's lemma. □

The Quadratic Reciprocity Law will be stated here, and its proof will be outlined as an exercise.

Theorem 6 (Quadratic Reciprocity Law)

For all odd primes $p \neq q$, we have $\left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}$

Since the legendre symbol is multiplicative, we are able to compute nearly any legendre symbol with this tool. We still must prove what $\left(\frac{2}{p}\right)$ is, which will also be an exercise.

Exercises

Exercise 1. (a) How many lattice points are strictly inside the rectangle with vertices at $(0,0), (\frac{p}{2}, 0), (\frac{p}{2}, \frac{q}{2})$ and $(0, \frac{q}{2})$?
(b) How many lattice points inside this rectangle lie on the diagonal emerging from $(0,0)$? How many below? Above?
(c) Deduce the Quadratic Reciprocity Law.

Exercise 2. Find a closed form for $\left(\dfrac{-1}{p}\right)$.

Exercise 3. Find a closed form for $\left(\dfrac{2}{p}\right)$. (Hint: Gauss's Lemma! Consider the primes mod 8.)

Exercise 4. For which odd primes p is the sum of the distinct quadratic residues a multiple of p?

Exercise 5. Compute $\left(\dfrac{6}{673}\right)$.

Exercise 6. Compute $\left(\dfrac{30}{61}\right)$.

Exercise 7. Look back to when we computed $\text{ord}_{23}(5)$. We had to manually check if it was 11 or not. Is there a way to see if $5^{11} \equiv 1 \pmod{23}$ or not without doing this?

5 More Problems

The following problems may use order, Legendre symbols, or both. Have fun!

Problem 1. Evaluate $\left(\dfrac{1\cdot 2}{p}\right) + \left(\dfrac{2\cdot 3}{p}\right) + \cdots + \left(\dfrac{(p-2)\cdot(p-1)}{p}\right)$.

Problem 2. Find, with proof, the number of x for which $1997 \in \{-1997, -1996, \ldots, 1996, 1997\}$ and $1997 | x^2 + (x+1)^2$.

Problem 3. Prove that 2 is a primitive root mod 5^n.

Problem 4. Let $F_n = 2^{2^n} + 1$ be the nth Fermat number. Show that if $n \geq 2$ and p is a prime such that $p \mid F_n$, then $p \equiv 1 \pmod{2^{n+2}}$.

Problem 5. Show that for $0 < n < p-1$, $p | 1^n + 2^n + \cdots + (p-1)^n$.

Problem 6. Find the smallest prime factor of $12^{2^{15}} + 1$.

Problem 7. (Vietnam TST 2004) Show that any number of the form $2^n + 1$ has no prime factors of the form $8k - 1$.

Problem 8. Show that when you write $2^{3^n} + 1$ as the product of as many primes as possible, at least $2n$ of them are $3 \pmod 8$.

Problem 9. (Taiwan 1997) Show that the nth Fermat number, F_n, is a prime number if and only if $F_n | 3^{\frac{F_n - 1}{2}} + 1$.

Problem 10. (USA TST 2008) Can $n^7 + 7$ be a perfect square?