6.S096: Number Theory January 17, 2024

Lecture 2— Euler and Fermat's Theorems

A. Anas Chentouf, M. Wacyl Meddour, M.A.O. *Scribe:*

1 Modular exponentiation

Computing exponential operations has always been a painful process. Indeed, repeated multiplications can get pretty large pretty fast. As such, we would like to resort to the tools of modular arithmetic in order to get some information about exponentials without necessarily computing them directly.

For example, we may want to find the units digit of a number. To no surprise, this is the remainder of the number after Euclidean division by 10, so we simply want to compute its residue modulo 10. Compatibility of multiplication can help us solve some cases instantaneously. For example, the last digit of $9^{12345321}$ will necessarily be a 9. The reason is that :

$$9^{12345321} \equiv (-1)^{12345321} \equiv -1 \equiv 9 \pmod{10}.$$

The same reasoning applies when considering the last digit of an exponent with base $19, 29, \ldots$

What if we want to compute the last digit of 3^{2222} ? Well, one can notice that $3^{2222} = 9^{1111}$ and so the last digit is a 9. For odd powers though, we have to extract a 3 first as follows :

$$3^{4445} \equiv 3 \cdot 3^{4444} \equiv 3 \cdot 9^{2222} \equiv 3 \pmod{10}.$$

Notice here that we cannot simply reduce the exponent modulo 10. Indeed, $7 \equiv 4 \pmod 3$ but $2^4 \equiv 1 \pmod 3$ and $2^7 \equiv 2 \pmod 3$. Indeed, **we can exchange the base but never the exponent**. We will see later that the exponent can still be simplified by reducing it modulo something other than n.

2 Fermat's Theorem

We will now explore the first non-trivial theorem concerning exponentiation in modular arithmetic - Fermat's Little Theorem.

Theorem 2.1: Fermat's (Little) Theorem

Let p be a prime number and x be any integer. Then

$$x^p \equiv x \pmod{p}.$$

Particularly, if $p \nmid x$ then

$$x^{p-1} \equiv 1 \pmod{p}.$$

Proof. The second part of the theorem follows from the fact that $p \nmid x$ means $\gcd(p, x) = 1$ (because p is prime) so that x is invertible mod p.

Consider the sets $S = \{1, 2, 3, 4, \ldots, p-1\}$ and $S' = \{x, 2x, 3x, 4x, \ldots, (p-1)x\}$. No element of S or S' is divisible by p (why?). Now, if $ix \equiv jx$ for some i, j, then since x is invertible mod p we get that $i \equiv j \pmod{p}$. This means that all elements of S' have distinct non-zero residues mod p. Since there are $p-1$ of them, they must represent all non-zero residues mod p, i.e $1, 2, \ldots, p-1$. Hence, the product of the elements in both sets is equal modulo p:

$$(1x) \cdot (2x) \cdot (3x) \ldots (p-1)x \equiv 1 \cdot 2 \cdot 3 \ldots (p-1) \pmod{p}.$$

Therefore, $x^{p-1}(p-1)! \equiv (p-1)! \pmod{p}$ and since $p \nmid (p-1)!$, we have that it is invertible modulo p and thus $x^{p-1} \equiv 1 \pmod{p}$, as desired. □

Effectively, Fermat's Theorem states that we can reduce our exponents modulo $p-1$ when working modulo p for p **prime**. The only case to be careful with is when the base is 0 mod p, in which case the residue is trivially 0 in the first place.

Example.

> If, for example we pick $p = 7$ and $x = 2$, then Fermat's Theorem tells us directly that $2^6 \equiv 1 \pmod{7}$. Indeed: $2^6 = 64 = 63 + 1 = 7 \cdot 9 + 1$, but the result is quite easy in this case. Note that this result can help us compute factually every power of 2 modulo 7. The reason is that even though we cannot reduce the exponent modulo 7, we definitely can modulo 6! Given any positive integer k, we have that
>
> $$2^{6k+2} \equiv 2^{6k} \cdot 2^2 \equiv (2^6)^k \cdot 2^2 \equiv 1^k \cdot 2^2 \equiv 4 \pmod{7},$$
>
> and we can do similarly for other residue classes modulo 6. Thanks to this, one can directly tell that $2^{6^{123}+2} \equiv 4 \pmod{7}$ without even slightly computing the (humongous) LHS.

We can also solve some equations using Fermat's theorem. For example, if we want to find all integers x for which $7|x^8 - 1$, this is equivalent to $x^8 \equiv 1 \pmod 7$. Since clearly $7 \nmid x$, $x^6 \equiv 1 \pmod 7$ and thus the equation is equivalent to $x^2 \equiv 1 \pmod 7$, the only solutions of which are integers $x \equiv \pm 1 \pmod 7$.

3 Euler's Theorem and φ

We now tackle a generalization of Fermat's result for arbitrary moduli n. The first remark is that if $x^k \equiv 1 \pmod n$ for some integer x and positive integer k, then clearly $\gcd(x, n) = 1$. Indeed, if $d|\gcd(x, n)$ then $d|x^k$ so it divides its remainder modulo n (since $d|n$) and thus $d|1$, so $\gcd(x, n) = 1$.

In the proof of Fermat's Theorem, we made use of the fact that all integers $1, 2, \ldots, p-1$ are coprime to p when p is prime. As such, we are motivated to only look at residues modulo n that are coprime to n. Since $p - 1$ was the needed power for Fermat's Theorem, we expect the number of coprime residues to also be the correct exponent in the general case.

Definition 3.1: Euler's Totient Function

Let n be a positive integer. $\varphi(n)$ is defined as the number of integers $1 \leq k \leq n$ for which $\gcd(k, n) = 1$, i.e :

$$\varphi(n) = \#\text{ of residues modulo } n \text{ coprime to } n$$

The function φ (read as "phi") is known as *Euler's totient function.*

Let us calculate the first values of φ to see how it looks like:

n	Coprime values	$\varphi(n)$
1	1	1
2	1	1
3	1, 2	2
4	1,3	2
5	1,2,3,4	4
6	1,5	2
7	1,2,3,4,5,6	6
8	1,3,5,7	4
9	1,2,4,5,7,8	6
10	1,3,7,9	4
11	1,2,3,4,5,6,7,8,9,10	10
12	1,5,7,11	4

Although no clear pattern seem to appear, we can still deduce some information about Euler's totient function. For example, it seems like $\varphi(n)$ is even for every $n \geq 3$. This turns out to be true because if $\gcd(n, k) = 1$ then $\gcd(n, n-k) = 1$ and as such we can pair up the elements coprime to n less than n as pairs of the form $(k, n-k)$. This pairing up does not work only when $k = \frac{n}{2}$ (we would count it twice), but then $\gcd(n, \frac{n}{2}) = \frac{n}{2}$ and the only value for which this is 1 is $n = 2$. So this is indeed true for $n \geq 3$.

Theorem 3.2: Euler's Theorem

Let n be a positive integer and let x be an integer such that $\gcd(x, n) = 1$. Then:

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

There are numerous consequences of Fermat's theorem. As we have seen above, it allows us to work modulo $p-1$ on exponents if p is prime, i.e that for positive integers x, y, n and for a prime p we have :

$$x^y \equiv x^{y+n(p-1)} \pmod{p}$$

Combining Fermat's Theorem with the Chinese Remainder Theorem can also help us compute the remainder of certain powers modulo product of primes. For example, if we want to find the remainder of $N = 4^{60609}$ modulo 21, we can see that $N \equiv 4^{60609} \equiv 1^{60609} \equiv 1 \pmod{3}$ and that $N \equiv 4^{60609} \equiv 4^3 \cdot 4^{6 \cdot 10101} \equiv 4^3 \equiv 2^6 \equiv 1 \pmod{7}$ by Fermat's Theorem. Hence, we are assured by CRT that $4^{60609} \equiv 1 \pmod{21}$. The same now applies to Euler's theorem.

The importance of Euler's theorem lies in the fact that we can effectively work modulo $\varphi(n)$ on the exponent for as long as the base is coprime to our moduli n. Since $\varphi(p) = p-1$ for p prime, Euler's Theorem generalizes Fermat's. The proof is essentially the same, as one would consider the set of residues coprime to n, multiply each element by x, and argue that the products of the two sets are congruent.

Let us look at some examples to illustrate the strength of Euler's theorem. Going back to our first digit problem, we can now effectively calculate the first digit of x^k for any $x \equiv 1, 3, 7, 9 \pmod{10}$. For example, we can see that

$$17^{12345} \equiv 17 \cdot 17^{12344} \equiv 17 \cdot 17^{4 \cdot 3086} \equiv 17 \equiv 7 \pmod{10}$$

since $\varphi(10) = 4$ and so $17^{4k} \equiv 1 \pmod{10}$ by Euler's Theorem.

In order to fully make use of the strength of Euler's Theorem, we would like to be able to compute arbitrary values of $\varphi(n)$ given an integer n.

Thankfully though, we can prove some elementary formulas for computing $\varphi(n)$ that can help us find its value in some cases. I have regrouped these essential properties in the following proposition :

Proposition 3.3: Properties of Euler's Totient Function

Let m, n be positive integers and let p be a prime. Then the following results hold.

(i) $\varphi(p^n) = p^n - p^{n-1} = p^{n-1}(p-1)$.

(ii) If $\gcd(m, n) = 1$ then $\varphi(mn) = \varphi(n) \cdot \varphi(m)$

(iii) $\varphi(n) = n \prod_{\substack{p|n \\ p \text{ prime}}} \left(1 - \frac{1}{p}\right)$

Proof. To prove (i), note that if $1 \leq k \leq p^n$ is an integer then $\gcd(p^n, k) > 1$ if and only if $p|k$. As such, to count the k's for which $\gcd(n, k) = 1$, we just count the multiples of p less than p^n and substract them from p^n. Naturally, there are $\frac{p^n}{p} = p^{n-1}$ multiples of p less than p^n, so indeed $\varphi(p^n) = p^n - p^{n-1}$.

To prove (ii), we apply the Chinese Remainder Theorem to find a one-to-one corrspondence between residues coprime to mn (there are $\varphi(mn)$ of them) nd pairs of residues coprime to n and m respectively (there are $\varphi(n)\varphi(m)$ of them).Given a and b two residues for which $\gcd(a, n) = \gcd(b, m) = 1$, then one can find a unique residue c mod mn such that $c \equiv a \pmod{n}$ and $c \equiv b \pmod{m}$. But $\gcd(c, mn) = \gcd(c, m) \cdot \gcd(c, n) = \gcd(a, n) \cdot \gcd(b, m) = 1$ since $\gcd(m, n) = 1$. Chinese Remainder Theorem guarantees that this map is well-defined. Since we can retrieve residues mod m and mod n from a residue mod mn uniquely, this ensures that there is a one-to-one correspondence between the two, and as such $\varphi(mn) = \varphi(m)\varphi(n)$, as desired.

The last result follows from applying (i) and (ii) and is left as an exercise. □

4 Modular Order

We conclude this lecture by talking about the notion of order modulo n. As concluded before, if $x^k \equiv 1 \pmod{n}$ for some integer $k > 0$, then $\gcd(x, k) = 1$, and

similarly, Fermat and Euler's Theorems gives us examples of such k's. We now explore another important exponent.

Definition 4.1: Order

Let n be a positive integer and let x be an integer coprime to n. The smallest positive integer k for which $x^k \equiv 1 \pmod{n}$ is called the *order of x mod n* and is denoted by $\text{ord}_n(x)$.

The first remark is that $\text{ord}_n(x)$ exists for every x coprime to n. The reason is that $\varphi(n)$ is a valid candidate for the order, so we just check the integers k from 1 to $\varphi(n) - 1$ to see if $x^k \equiv 1 \pmod{n}$. If so, we pick the first one that satisfies the condition and that's our order. Otherwise, our order is $\varphi(n)$ itself. In fact, it suffices to check integers in this interval which divide $\phi(n)$, as we now prove.

Proposition 4.2: Order Divisibility

Let n be a positive integer and let x be an integer coprime to n. Let $k = \text{ord}_n(x)$ and let m be a positive integer for which $x^m \equiv 1 \pmod{n}$. Then, $k|m$.

In other words, the order of x mod n divides every exponent m for which $x^m \equiv 1 \pmod{n}$.

Proof. By the definition of order, we have that $m \geq k$. Applying Euclidean division of m by k to write it as $m = kq + r$ where $0 \leq r < k$ and $q \geq 1$. Then

$$1 \equiv x^m \equiv x^{kq+r} \equiv (x^k)^q \cdot x^r \equiv x^r \pmod{n}.$$

Since $r < k$, then this forces $r = 0$ by definition of k (as the smallest positive integer satisfying that condition), and so $k|m$, as desired. □

Although this property seems quite random, it is extremely important from both a theoretical and a computational point of view, and we will see this when we learn group theory. This also means that the integers $k$for which $x^k \equiv 1 \pmod{n}$ are EXACTLY the multiples of $\text{ord}_n(x)$, giving us a full categorization of the set of "modulos" we can work with in the exponent.

Second, coupling this result with Euler's theorem yields that $\text{ord}_n(x)|\varphi(n)$! It means that to find the order of x mod n, its enough to check the divisors of $\varphi(n)$ until finding the valid order. It also means that if $x^k \equiv 1 \pmod{n}$ for some arbitrary k, then $\text{ord}_n(x)|\gcd(k, \varphi(n))$.

Let us look at the following two examples. First, notice that even though $\varphi(7) = 6$, 6 is not the order of every element modulo 7. For example, $2^3 \equiv 1 \pmod 7$ and as such 3 is the order of 2 mod 7. This means that when the base is 2, we can effectively work modulo 3 in the exponent when working overall modulo 7.

Finally, if we want to find all integers x for which $x^4 \equiv 1 \pmod 7$, notice that $7 \nmid x$ and as such $x^6 \equiv 1 \pmod 7$ by Fermat's Theorem. So, the order of x mod 7 divides both 6 and 4, so it divides their GCD, i.e 2. So $\text{ord}_7(x)|2$ and as such $x^2 \equiv 1 \pmod 7$.

5 Primitive Roots

We have proven that the order of x modulo n is a divisor of $\phi(n)$. One may wonder what the extreme cases are. The first occurs when $\text{ord}_n(x) = 1$, and this implies $x \equiv 1 \bmod n$, which is not that interesting. The other extreme case occurs when $\text{ord}_n(x) = \varphi(n)$, and is much more interesting.

Definition 5.1: Primitive Roots

If $\text{ord}_n(g) = \varphi(n)$, then g (and its residue class) are said to be *primitive roots* modulo n.

Naturally, there are some questions to ask here.

1. For which moduli are there primitive roots?
2. How many primitive roots are there?

We answer the first question, but without providing an entire proof.

Theorem 5.2: Existence of Primitive Roots

primitive root exists modulo n if and only if $n = 2, 4, p^k$ or $2p^k$ where p is an odd prime and $k \geq 1$.

Af, but before doing so, we introduce an auxiliary lemma. This lemma justified why we often denote primitive roots by g - because they are generators!

Proposition 5.3: Primitive Roots are Generators

If g is a primitive root modulo n, then $\{g^0, g^1, \cdots, g^{\phi(n)-1}\}$ is the complete set of invertible residues modulo n.

Proof. There are $\varphi(n)$ invertible residues, and so it suffices to prove that the elements in the set $\{g^0, g^1, \cdots, g^{\phi(n)-1}\}$ are pairwise distinct modulo n. In fact, assume that $g^i \equiv g^j \bmod n$, for some $i \geq j$. then $g^{i-j} \equiv 1 \bmod n$, but note that $i - j < \varphi(n)$, and so $i - j = 0$ by the definition of primitive roots. □

Theorem 5.4: Number of Primitive Roots

If there exists a primitive root modulo n, then there are exactly $\varphi(\varphi(n))$ of them.

Proof. Consider a primitive root g. Note that by Proposition 5.3, the set $\{g^i\}_{i=0}^{\varphi(n)-1}$ contains all invertible residues, and hence all primitive roots. Note that g^i is a primitive root if and only if the smallest positive k such that $g^i k \equiv 1 \bmod n$ is $k = \phi(n)$. Alternatively, the smallest k such that $ik \equiv 0 \bmod \varphi(n)$ is $\varphi(n)$. In other words, i must be coprime to $\varphi(n)$, and there are exactly $\varphi(\varphi(n))$ such residues. □

In fact, we just proved the following result.

If g is a primitive root modulo n, then g^i is a primitive root modulo n if and only if i is coprime to $\varphi(n)$.