Republic of Iraq

Ministry of Higher Education and Scientific Research

Maysan University

Department of Mathematics

Euler's and Fermat's theorem

Research submitted to the Council of the College of Education, Department of Mathematics, which is part of the requirements for obtaining a bachelor's degree in mathematics

Written by :

Malak Nizar Hassan

Supervision

بسم الله الرحمن الرحيم

إِنَّمَا يَخْشَى اللَّهَ مِنْ عِبَادِهِ الْعُلَمَاءُ

"سورة فاطر، آية: 28"

صدق الله العلي العظيم

الاهداء

إلى قائم آل محمد إمام العصر والزمان الحجة المنتظر (عج) .

إلى من افضالها على نفسي، ولم لا ؟ فقد ضحت من أجلي ولم تدخر جهداً في سبيل إسعادي على الدوام . . . . . (أمي الحبيبة) .

إلى صاحب الوجه الطيب، والأفعال الحسنة، الذي لم يبخل علي طيلة حياته . . (والدي العزيز) .

إلى من اضاءوا لي طريق العلم، اساتذتي الأفاضل، . . . . إلى من تشرفت بمعرفتهم أصدقائي الأعزاء اهدي لكم ثمرة جهدي المتواضع .

"الشكر وتقدير"

كن عالماً ، فإن لم تستطع فكن معلماً ، فإن لم تستطع فأحب العلماء ، فإن لم تستطع فلا تبغضهم.

أتقدم بخالص الشكر والتقدير إلى والدي العزيزين، اللذين كانا لي النور الذي أستنير به في حياتي، وزرعا في نفسي القيم والمبادئ السامية.

كما أخص بالشكر أساتذتي الأفاضل، الذين لم يدخروا جهداً في تعليمنا وتوجيهنا ، فكان لهم الفضل بعد الله فيما وصلنا إليه.

ولا أنسى زملائي الأعزاء، الذين كانوا خير رفقاء في هذه المسيرة، فبالتعاون والمشاركة تحقق هذا الإنجاز.

ومن الله التوفيق والسداد

اقرار المشرف

أشهد أن هذا البحث المرسوم : (Euler's and Fermat's theorem)

الذي تقدم به الطالبة (ملاك نزار حسن) , قد جرى تحت أشرافي

في جامعة ميسان / كلية التربية / قسم الرياضيات

وهو جزء من متطلبات نيل درجة البكالوريوس في كلية التربية / قسم الراضيات . . . .

اقرار المشرف

أسم المشــرف : تغريد عبد الكريم

الدرجة العلمية : مساعد مدرس

بناء على توصيات المشرف ارشح هذا البحث للمناقشة

م . احمد كريم مطشر

رئيس قسم الرياضيات

2025 / /

Chapter One

Euler's Theorem

Euler's Theorem

1.1 Theorem 1: Let m >1 and gcd (a,m)=1.

Then

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

Proof: Let $\{r_1, ..., r_{\phi(m)}\}$ be a RSR modulo m.

Then $\{ar_1, ..., ar_{\phi(m)}\}$ is a RSR modulo m1, too.

Therefore, for all i, there is a unique j so that $r_i \equiv ar_j \pmod{m}$.

Then

$a^{\phi(m)} \prod_{i=1}^{\phi(m)} r_i = \prod_{i=1}^{\phi(m)} (ar_i) \equiv (\prod_{i=1}^{\phi(m)} r_i) \pmod{m}$.

Since gcd $(\prod_{i=1}^{\phi(m)} r_i, m) = 1$, we can cancel and get $a^{\phi(m)} \equiv 1 \pmod{m}$.

Example 1: Let m=13×23=299 , where 13 and 23 are primes.

Then

$\phi(m)=\phi(299)=(13-1)(23-1)=12\times22=264$.

Note that gcd(5,299)=1 , Euler's Theorem says $5^{264} \equiv 1 \pmod{299}$,

that is, $299 \mid (5^{264}-1)$.

Example 2 : of the use of Euler's theorem.

Find the two low-order decimal digits of 33862513^{119442}.

First, 33862513≡13 (mod 100), so the answer is the same as the two low-order deci- mal digits of 13^{119442}

(because $(100k + 13)^n \equiv 13^n \pmod{100}$ and the two low-order decimal digits of m are m mod 100).

Second,

$\phi(100)=\phi(2^2)\phi(5^2)=2(2-1)\cdot 5(5-1)=40$.

Now 119442≡2 (mod 40), so by Euler, $13^{119442}\equiv 13^2 \pmod{100}$.

Finally, $33862513^{119442}\equiv 13^{119442}\equiv 13^2 = 169\equiv 69 \pmod{100}$,

and the two low-order decimal digits of 33862513^{119442} are 69.

1.2 A Corollary of Euler's Theorem

Here is an alternate way to compute the mul- tiplicative inverse $a^{-1}$of a modulo m: Recall that $a^{-1}$is the residue class mod m such that $a^{-1}a \equiv aa^{-1} \equiv 1 \pmod{m}$. It is defined only when gcd(a,m)=1 In that situation we have $a^{\phi(m)}\equiv 1 \pmod{m}$ by Euler's Theorem.

Factoring out one a gives

$$a \cdot a^{\phi(m)-1} \equiv 1 \pmod{m}$$

whence $a^{-1}\equiv a^{\phi(m)-1} \pmod{m}$. For a prime modulus p we have $a^{-1}\equiv a^{p-2} \pmod{p}$.

For large m, computing a^{-1}mod m by this for- mula requires roughly the same number of bit operations as computing a^{-1}mod m by the Ex- tended Euclidean Algorithm. (The latter must be used if one does not know ϕ(m).)

ler's generalization

Theorem 2: The set Z_n^x of nonzero elements of Z_n that are not zero divis forms a group.

Proof:

closed:

Suppose that a and b are not 0 nor zero divisors. We n to show that ab is neither 0 nor a zero divisor.

Since a and b are not 0 nor zero divisors, ab $\neq$ 0.

Now suppose that (ab) c=0.

Then a(bc)=0. Since a is not 0 nor a zero divisors, bc=0.

By the same token bc=0 implies c=0 Thus ab is nor zero divisor.

1.3 Euler's Ø-function

Definition :

The Euler's Ø-function Ø(n) is defined as the number of elements in Z_n^x (By Theorem 19.3,$\phi(n)=\{1\leq k \leq n:gcd(k,n)=1\}$.)

Example 3 :

1. Z_{12}^x={1,5,7,11} .Thus $\phi(12)=4$.
2. Z_{15}^x={1,2,4,7,8,11,13,14}, and $\phi(15)=8$.

Remark

In general, $\phi(n)=n\prod_{p\,|_{n,p\ primes}}(1-1/p)$.

Euler's theorem

1.3 Theorem 4: Euler's theorem

Let n be a positive integer. Then for all integers a relatively prime to n, we have

$$a^{\phi(m)} \equiv 1 \bmod n.$$

Proof:

Similar to the proof of Fermat's theorem. (Apply the Lagrange theorem to the group Z_n^x)

Example 4:

Let us compute 4^{99} mod 35. We have $4^{\emptyset(35)} \equiv 1$ mod 35

i.e.. $4^{24} \equiv 1$ mod 35. Thus, $4^{99} \equiv 4^3 = 64 \equiv 29$ mod 35.

Proof:

Let $\{r_1, ..., r_{\phi(m)}\}$ be a RSR modulo m. Then $\{ar_1, ..., ar_{\phi(m)}\}$ is a RSR modulo m too. Therefore, for all i, there is a unique j so that $r_i \equiv ar_j$ (mod m) .

Then

$$\boldsymbol{a^{\phi(m)} \prod_{i=1}^{\phi(m)} r_i = \prod_{i=1}^{\phi(m)} (ar_i) \equiv \left(\prod_{i=1}^{\phi(m)} r_i\right)} \text{ (mod m) .}$$

Since gcd $\left(\prod_{i=1}^{\phi(m)} r_i, m\right) = 1$, we can cancel and get $a^{\phi(m)} \equiv 1$ (mod m).

Chapter Two

Fermat's "Little" Theorem

Fermat's "Little" Theorem

2.1 Theorem 1: Let p be prime and a be an integer which is not a multiple of p. Then

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

Proof: Since gcd (a,p)=1, the set

{ai mod p;i =1,...,p−1} is the same as the set {1,...,p−1}. Therefore,

$$\boldsymbol{a^{p-1} \prod_{i=1}^{p-1} i = \prod_{i=1}^{p-1} (ai) \equiv \left(\prod_{i=1}^{p-1} i\right).1} \pmod{p}.$$

Since gcd $(\prod_{\mathbf{i=1}}^{\mathbf{p-1}} \mathbf{i}, \mathbf{p})$=1 , we can cancel and get $a^{p-1} \equiv 1 \pmod{p}$.

Example 1: 97 is prime and 2 is not a multiple of 97, so $2^{96} \equiv 1 \pmod{97}$.

2.1 Fermat's theorem

Theorem 2: (Little theorem of Fermat)

Let p be a prime. Then for all integers a not divisible by p, we have

$$a^{p-1} \equiv 1 \bmod p.$$

Proof:

The group Z_p^x has p−1 elements. Then by the Lagrange theorem (Theorem 10.10),

for all a ∈ Z_p^x , $a^{p-1} \equiv 1 \bmod p$.

2.3 Corollary and examples

Corollary 1: Let p be a prime. Then

$$a^p \equiv \text{a mod p}$$

for all a ∈Z

Example 1. Let us compute the remainder of 7^{103} when divided by 17.

Solution:

By Fermat's theorem, we have $7^{16} \equiv 1 \bmod 17$. Thus,

$$\mathbf{7^{103} = 7^{6\times16+7} = (7^{16})^6(7^7) \equiv 7^7 = 7(7^3)^2 = 7(343)^2 \equiv 7.9 \equiv 12 \bmod 17}.$$

Example 2 : Prove that $n^{33}-n$ is divisible by 15 for all n.

Solution:

We need to show that $n^{33}-n$ is divisible by bot and 5. Here we demonstrate $n^{33}-n \equiv 0 \pmod 5$, and learn $n^{33}-n \equiv 0 \bmod 3$ as an exercise.

If 5|n, then $n^{33}$is clearly congruent to n modulo 5. If 5|n
$n^{33} - n = n(n^{32}-1) = n((n^4)^8)8-1) \equiv n(1-1) = 0$

Finding a^{-1}modulo n using the Euclidean algorithm

Example 3 : Find the multiplicative inverse of 11 modulo 29.

Solution: We have

$$29 = 2 \times 11 + 7$$

$$11 = 1 \times 7 + 4$$

$$7 = 1 \times 4 + 3$$

$$4 = 1 \times 3 + 1.$$

Thus

$1 = 4 - 1 \times 3$

$=4-1\times(7-1\times4)=2\times4-1\times7 =2\times(11-1\times7)-1\times7=2\times11-3\times7$
$=2\times11-3\times(29-2\times11)=8\times11-3\times29$

We see that the multiplicative inverse of 11 modulo 29 is

Chapter Three

FERMAT'S LITTLE THEOREM AND EULER'S GENERALIZATION

FERMAT'S LITTLE THEOREM AND EULER'S GENERALIZATION

3.1: FERMAT'S LITTLE THEOREM

Theorem 1 :

One form of Fermat's Little Theorem states that if p is a prime and if a is an integer then p|a^p –a

For example 3 : divides $2^3-2=6$ and $3^3-3=24$ and $4^3-4=60$ and $5^3-5=120$ Similarly, 5 divides $2^5-2=30$ and $3^5-3=240$ et cetera.

Obviously a^p−a factors as a(a^{p-1}−1) So if p ł a then we have

$$p|a^{p-1}-1$$

This gives another common form of Fermat's Little Theorem. For example, 3 divides $5^2-1=24$ and $4^2-1=15$ and $2^2-1=3$ Also, 5 divides $2^4-1=15$ and $3^4-1=80$ and $4^4-1=255$, and 7 divides$2^6-1=63$ et cetera. After Gauss introduced congruences, the theorem was typically written

$$a^p \equiv a \bmod p$$

or, equivalently,

$$a\neq 0 \bmod p \Rightarrow a^{p-1} \equiv 1 \bmod p$$

Exercise 1. Show that these two versions of Gauss's form of Fermat's Little Theorem are

equivalent. In other words, show

version 1<===> version 2

Finally, using the more modern notion of a finite field F_p with p elements, we can write the theorem as

$$a \in F_p \Rightarrow a^p = a$$

or, equivalently,

$$a \in F_p^x \Rightarrow a^{p-1} = 1$$

We will discuss three different proofs of Fermat's Little Theorem. The shortest is a proof using group theory: Suppose a is in the unit group F_p^x. By a theorem of group theory, if |G| is the order of the group, then $a^{|G|}$ is the identity. The order of the unit group is p−1, so a^{p-1}=1. This proof is very economical, but will only appeal to readers who have studied group theory. Furthermore, it is a relatively late proof, and uses concepts that were not available to Fermat, Euler, and Gauss.

3.2. INDUCTION BASED PROOF

The first of the two highlighted proofs of Fermat's Little Theorem uses induction and binomial coefficients.

Theorem 1: (Fermat's Little Theorem). Let a be an integer, and let p be a prime. Then

$$a^p \equiv a \bmod p$$

Proof: Fix the prime p. First we prove the result for natural numbers n by induction. The base case is trivial:

$$0^p \equiv 0 \bmod p.$$

Now suppose $n^p \equiv n$ modulo p. By the binomial theorem

$$(\boldsymbol{n+1})^{\boldsymbol{p}} = \boldsymbol{n^p} \binom{p}{1} \boldsymbol{n^{p-1}} + \binom{p}{2} \boldsymbol{n^{p-2}} + \ldots + \binom{p}{p-2} \boldsymbol{n^2} + \binom{p}{p-1} \mathbf{n} + \mathbf{1}$$

The formula for the binomial coefficients is

$$\binom{p}{k} = \frac{p!}{k!(p-k)!}$$

and when $1 \le k \le p-1$ we have p dividing the numerator, but not the denominator. Thus, for all $1 \le k \le p-1$,

$$\binom{p}{k} \equiv 0 \bmod p.$$

Hence

$$(n+1)^p \equiv n^p + 0 + \ldots + 0 + 1 \equiv n^p + 1 \bmod p.$$

By induction, we have the result for all n ≥ 0. For negative a, choose n ≥ 0 so that a≡ n modulo p. Since the result holds for n, it holds for a as well. Thus the result holds for all a∈Z.

3.3 ERMUTATION BASED PROOF

Now we give a second proof of Fermat's theorem. This involves permuting the order of factors of (p−1)!. Recall that a permutation map on a finite set is just a bijection from the set to itself.

For Fermat's theorem we only need the following lemma form m=p pa prime. However, the general case is no harder to prove.

Lemma 1. Let m > 1 be an integer, and let a ∈ Z_m^x . Then the function μ_a defined by the rule x ↦ a . x is a bijection $Z_m^x \rightarrow Z_m^x$.

Proof: Observe that

$$\mu_a\,(\mu_{a^{-1}}(x)) = \mu_a\,(a^{-1}\,x) = a(a^{-1}x) = x.$$

Similarly $\mu_{a^{-1}}(\mu_a(x))=x$. Thus $\mu_{a^{-1}}$ is the inverse of the function μ_a. Since μ_a has an inverse, it is a bijection.

Corollary 2. Let p be an prime. If a∈F_p^x then a,2a,...,(p−1)a are distinct, and every element of F_p^x is in the sequence. In particular, this list is a permutation of the list 1,2,3,...,p−1.

Proof: The injectivity of $\mu_a$tells us that the terms are distinct, and the surjectivity tells us that every element of F_p^x is on the list.

Exercise 2. Make a table showing all the values of the functions μ_3: $F_5^x \rightarrow F_5^x$. Observe that multiplication by 3 (modulo 5) permutes {1,2,3,4}.

Exercise 3: Make a table showing all the values of the functionsμ_4: $F_{15}^x \rightarrow F_{15}^x$.

Here is the permutation based proof:

Theorem 3: (Fermat's Little Theorem): Let p be a prime. If a∈ F_p^x then a^{p-1}=1.

Proof:

Let u=1·2·3⋯ (p−1) = (p−1)! considered as an element of F_p. Since u is the product of units, u is also a unit. By Corollary 2,

$$(a)\,(2a)\,(3a)\,\ldots\,((p-1)\,a) = 1\cdot 2\cdot 3\ldots(p-1) = u$$

since both sides are the product of the same elements, possibly in a different order. Observe that

$$(a)\,(2a)\,(3a)\ldots((p-1)\,a) = 1\cdot 2\cdot 3\ldots\,(p-1)\,a^{p-1} = u a^{p-1}$$

(move all the a terms to the right). Thus

$$u a^{p-1} = u.$$

Since u is a unit, we can multiply by its inverse . So a^{p-1} =1.

3.4 EULER'S THEOREM

The famous mathematician Euler was fascinated with the number theoretic work of Fermat. In fact, Euler's interest in number theory is largely due to his study of Fermat's writings. Fermat did not leave a proof of his Little Theorem in his published writings, but Euler, once he learned of the statement, was able to figure out a proof. Next Euler thought about how to generalize this result to a modulus m that is not prime. His key idea was to develop his function φ(m), and replace p−1 with φ(m). This is motivated by the fact that Z_p has p−1 units, but in general Z_m has φ(m) units. The proof follows closely the permutation based version of the proof of Fermat's theorem.

Lemma 2: Let m>1 be an integer and let $u_1,\ldots,u_{\varphi(m)}$ be the (distinct) elements of Z_m^x. If a∈Z_m^x then the terms of the sequence a $au_1,\ldots,au_{\varphi(m)}$ are distinct, and every element of Z_m^x is in the sequence.

Proof: This follows from the fact that μa is a bijection (Lemma 1).

Theorem 4 : (Euler's Theorem). Let m>1 be an integer. If a∈ Z_m^x then $a^{\varphi(m)}$ =1.

Proof: LetZ_m^x ={ u_1,...,$u_{\varphi(m)}$} By the above lemma, and the commutative law of multi-plication,

$$u_1,...,u_{\varphi(m)}=(a\ u_1)\cdots(a\ u_{\varphi(m)_3})=a^{\varphi(m)}\cdot(u_1,...,u_{\varphi(m)}).$$

(The first equality is true since the second product has the same factors as the first, but typically in a different order. The second is true based on moving a to the front. Observe that there are φ(m) occurances of a since there are φ(m) units.)

Let u=u_1,...,$u_{\varphi(m)}$.

Observe that u is a unit by the closure property. Thus

$$u=a^{\varphi(m)}\ u.$$

Now multiply both sides by the inverse of u .

3.5 Wilson's Theorem

In the permutation based proof of Fermat's theorem we used (p−1)! in the field F_p. We didn't have to calculate its value, since it cancelled at the end of the proof. However, it is interesting to note that it is just -1. We begin with a short lemma.

Lemma 3: Let p>2 be a prime and let a∈Z_p^x . Then a=a^{-1} if and only if a is 1 or -1.

Proof: One direction is clear. For the other, suppose that a=a^{-1}. Multiplying both sides by a gives a^2=1. In other words, a^2−1=0. This implies that (a−1)(a+1)=0. Since F_p is an integral domain, we have a−1=0 or a+1=0. Thus a=1 or a=−1.

Exercise 5: Show that x↦x^{-1} is a bijection of Z_m^x . Conclude from this that (p−1)! is its own multiplicative inverse in F_p. The above lemma tells us that (p−1)! is either 1 or -1. The next exercise shows that is cannot be 1 but must be -1.

Theorem 5 : (Wilson's Theorem): Let p be a prime. Then (p−1)!≡−1 mod p.

Proof: If p=2 then it is clear, so assume p>2. If we multiply all the elements of F_p^x together we get

$$1 \cdot 2 \cdots (p-1) = (p-1)!$$

Now reorder the elements of F_p^x as $a_1, a_2, \ldots, a_{p-1}$ so that a_1=1, so that a_2=−1, and, for i>1 so that a_{2i}−1 and a_{2i} are multiplicative inverses to each other. [64] We can do this by the previous lemma: an element and its inverse pair up to give two distinct elements except for 1 and -1. Consider the product:

$$a_1, a_2, \ldots, a_{p-1} = 1 \cdot (-1) \cdot (a_3 \cdot a_4) \cdots (a_{p-2} \cdot a_{p-1}) = 1 \cdot (-1) \cdot 1 \cdots 1 = -1$$

By the commutative law of multiplication in F_p;

$$(p-1)! = 1 \cdot 2 \cdots (p-1) = a_1 \cdots a_{p-1} = -1.$$

Example 1: Consider 6! modulo 7:

$6! \equiv 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \equiv 1 \cdot 6 \cdot (2 \cdot 4) \cdot (3 \cdot 5) \equiv 1 \cdot -1 \cdot (1) \cdot (1) \equiv -1 \bmod 7.$

From a direct calculation 6! + 1= 721 is seen to be divisible by 7.

المصادر

1) **Yifan yang spring 2007**

2) **February 2002.**