Proof of Fermat's Little Theoerem

Ramandika Pranamulia 13512078
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
ramandika@students.itb.ac.id

***Abstract*—Discrete Mathematics has an important role in the field of Computer Science. Induction, Combinatory, and Number Theory are some fields of discrete mathematics that are learned in computer science. Induction is usually used to check whether some identity (formula) is right or not and to check whether a program has running properly as we want. Combinatory is used to count the number of ways that a combination or permutation can make without interested in the enumeration of the possible outcome. Whereas Number Theory can solve some modulus problems, which some of them(modulus problems) can't even computed by computer since the number is too large. In this paper I would like to prove the identity of Fermat's Little Theorem which has known broadly in the field of Number Theory. This theorem is used to compute the remainder of an integer powered by p-1 and divided by p, p is a prime number. The proof will use induction, combination, and fundamental number theory. So there will be three different proofs for this problem.**

***Index Terms*—induction, permutation, combination, binomial Newton, Inclusive and Exclusive.**

I. Introduction

Fermat is a French lawyer at the Parliament of Toulouse, France. He is also an amateur mathematician and broadly known by his theorem named Fermat's Last Theorem. Another of his well known theorems that is used in the field of Number Theory is Fermat's Little Theorem. This theorem made us possible to count the reminder of an integer powered by a prime number minus 1 when divided by that prime number and we are going to prove this identity.

As we know in general there are two proof methods in mathematics. Explicit proof (direct proof) and implicit proof. Explicit proof is done by showing the step how can an identity can be construct, while implicit proof is done by showing that the identity is true without showing the step how such identity can be construct. Implicit proof usually has its own step in proving identity. Induction is an example of implicit proof since we don't need to prove how a formula or identity is constructed, while linear algebra, combinatory, geometry, and number theory can be used to prove an identity or formula in explicit way.

II. Fundamental theories

2.1 Induction

Induction is an alternative way to prove an identity or formula without using direct proof. There are some types of induction. Weak induction, strong induction, and unordered induction are the examples. But to prove the Fermat's little theorem we are going to use the weak one. The principal of all induction is like a domino effect; once you fall down the first domino then the others will fall down as well. There are the base of induction and the hypothesis for every induction. The following steps will show you how to use weak induction to prove that an identity is true.

1. First prove that the identity is true for the base of induction. Usually the base is started from one or zero. Though it depends on the problem.
2. Create a hypothesis related to the identity. The hypothesis is usually stated like this "let n=k is true".
3. The last step is to prove that n=k+1 is true as well. We may use the hypothesis to prove this.

Now you might be wondering how the induction step can prove the identity. But First I am going to show you how we can prove an identity by direct proof. Say that we want to prove the identity of

$$1+2+3+\cdots+n=\frac{n(n+1)}{2}$$

The following step is direct proof for the above equation.

Let

$$1+2+3+\cdots+n=x\ .....(1)$$

Now if I reverse the order of the number, the sum of the number will still equal.

$$n+(n-1)+\cdots+1=x\ .....(2)$$

Adding the first equation (1) and the second equation (2). We will get

$$(n+1)+(n+1)+\cdots+(n+1)=2x$$

The number of (n+1) is n so the sum of the RHS(right hand side) of the equality is equal to n(n+1)

$$n(n+1)=2x$$

Solving for x we will get

$$\frac{n(n+1)}{2} = x$$

Which is equal to identity we stated above (as desired)

Now we are going to prove the above identity of arithmetic sum by induction.

1. Prove that for n=1 the equation hold

$$1 = 1.\frac{1+1}{2}$$

(Proved RHS=LHS)

2. Assume that for n=k the equation hold, so we can infer that

$$1 + 2 + \cdots + k = \frac{k(k+1)}{2}$$

(Hypothesis)

3. Now we have to prove that n=k+1 is true as well

$$1 + 2 + \cdots + k + (k+1) = \frac{(k+1)((k+1)+1)}{2}$$

Now to prove that the equation is true for n=k+1 we are using the hypothesis.

$$1 + 2 + \cdots + k = \frac{k(k+1)}{2}$$

Adding k+1 to both sides and we will get

$$1 + 2 + \cdots + k + k + 1 = (k+1) + \frac{k(k+1)}{2}$$

if we simplify the RHS we will get

$$1 + 2 + \cdots + k + k + 1 = \frac{2(k+1) + k(k+1)}{2}$$

$$= \frac{(k+1)(k+2)}{2}$$

Then we are done with our proof.

Now how can the inductions works? The idea is that when you prove the base is true (for the above case we take n=1 as the base), then by second step and third step you can prove that n=2 is true as well. If n=2 true then we can conclude that n=3 is true as well by the second and third step and so on.

2.2 Combinatory

There is two fundamental theories in combinatory, permutation and combination. Permutation is used to count the possibility of rearranging some objects by considering the sequence, while combination is not considering the sequence.

If we would like to draw one by one of r objects from n distinct objects then we can use permutation.

$$P(n,r) = \frac{n!}{(n-r)!}$$

Source ww.statistic.about.com

While if we would like to draw k objects from n distinct objects once at a time. Then the number of possible combination is

$$C_r^n = \frac{n!}{r!(n-r)!}$$

source id.wikipedia.org

2.3 Binomial Newton

Binomial Newton is an algebraic method of expanding powers of binomial. For instance expanding $(a+b)^3$

$$(a+b)^3 = a^3 + 3a^2b + 3ab^2 + b^3$$

Actually the coefficient of Binomial Newton is similar with Pascal triangle, where each entry is the sum of above it

1
1 1
1 2 1
1 3 3 1
1 4 6 4 1
1 5 10 10 5 1

Pascal Tree, source: wikipedia.org

But it seems inefficient to count a large number coefficient generating by a large power of binom. Say that we want to look for the coefficient of $a^{52}b^{47}$ of the expansion $(a-b)^{99}$. If we use the Pascal tree it will take longer time than using binomial Newton. The Binomial Newton states that

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} . a^{n-k} . b^k$$
$$k, n \in \mathbb{N}$$

2.4 Inclusive and Exclusive Principal of Set

Set is a collection of different objects (the object is unique). An object that belongs to a set is called element or member of set. There are generally two ways to represent a set, enumeration and symbolic.

Enumeration is use usually if the number of element is not so large. The following is the representation of a set A whose element is one, two, three, one hundred and discrete mathematics.

A= {1,2,3,100,discrete mathematics}
enumeration representation

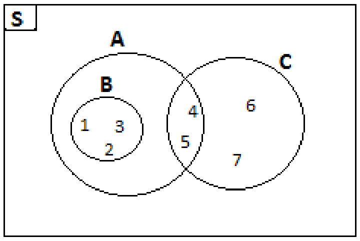
Symbolic representation is used to represent a set which element has the same properties, for example real number or integer. The following is the representation of set B whose element is real number between three and five exclusive.

$$B = \{x|x \in \mathbb{R}, 3 < x < 5\}$$

symbolic representation

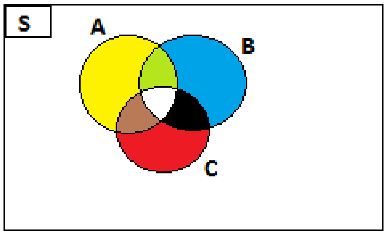
The symbol | means where, so if we interpreted the meaning of the symbol. B is a set of x, where x is element of real number between three and five.

Next we are going to talk about the Venn diagram, joint set, disjoint set, union, and intersection. First Diagram Venn is another way to represent a set in a form of diagram. The Venn diagram makes us possible to represent the intersection or union of some sets. Let A={1,2,3,4,5}, B={1,2,3}, and C={4,5,6,7}. The following is the diagram representation of these sets.



We can look from the diagram that set B is inside A. Therefore Set B is said to be the subset of A, since every element in B exists in set A. Set A and C has two intersection elements, they are four and five and we can state like this $A \cap C = \{4,5\}$. $\cap$ means intersection. While the union of A and C is represented as $A \cup C = \{1,2,3,4,5,6,7\}$. The element or member of union A and C is seven, so we could say that the cardinal of union A and C is seven. Cardinal of set A is represented by |A|.

Now let's pay attention to the cardinal of the sets. Note that |A∪C|=|A|+|C|−|A∩C| for the above diagram. Now if we have three sets whose diagram is represented as the following.



Notice that |A∪B∪C|=|A|+|B|+|C|-|A∩B|-|A∩C|-|B∩C|+|A∩B∩C|. This called as the principal of exclusion and inclusion. If we general the principal to n sets then

$$\left|\bigcup_{i=1}^{n} Ai\right| = \sum_{i=1}^{n}|Ai| - \sum_{1\le i\le j\le n}|Ai \cap Aj| + \sum_{1\le i\le j\le kn}|Ai \cap Aj \cap Ak|$$

$$- \cdots + (-1)^{n-1}|A1 \cap A2 \cap \ldots \cap An|$$

the prove can be done by advance induction method, which is not going to be done here.

2.5 Euler's phi function / totient function

Have you heard about the coprime term? Two positive integer a and b is said to be coprime to each other if the great common divisor of them is equal to one (gcd(a,b)=1). a or b hasn't to be a prime number, but we can make it sure that if both of them (a and b) are prime numbers then they are coprime. Now assume that there is a number N and once interested to look for the number of integer that less than N and coprime to N. For example if N=10 then there are four integer that less than 10 and coprime to 10, they are 1,3,7,9. Then if you have a large number N and interested to count the number of integer that less than N and coprime to N, it will be wasting time to check all of natural number less then N.

Euler as a genius mathematician had developed a formula to find the number of coprime number to N which less than N. The formula is stated as a function, named Euler's phi function. The following function is Euler's phi function

$$\varphi(N) = N\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\ldots\left(1-\frac{1}{p_n}\right)$$

$p_1, p_2, \ldots, p_n$ is the prime factor of N.

Now we will prove the above function. First notice that the fundamental theorem of arithmetic states that for every positive integer N, there is always $p_1,p_2,\ldots,p_n$ and $q_1,q_2,..,q_n$ where p_i is a prime number and q_i is a natural number such that

$$N = p_1^{q_1}.p_2^{q_n}\ldots p_n^{q_n}$$

Now if we want to search the number of integer that less than N and coprime to N, it is easier to count the number of integer that isn't coprime to N (gcd(x,N)=p_i) for some prime p_i which is a factor of N. Let say $p_i=p_1$ then the number of integer x that less than N and gcd(x,N)=p_1 is equal to N/p_1. Then the number of integer x that are coprime to N and gcd(x,N)=p_2 is equal to N/p_2. Notice that there will be double counting of the integer x whose gcd(x,N)=p_1p_2. So we must apply the principal of exclusion and inclusion. If we general it then the relation becomes

$$N - \left|\bigcup_i X_i\right| = N - \sum_i |X_i| + \sum_{i\neq j} |X_i \cap X_j| + \cdots + (-1)^n \left|\bigcap_i p_i\right|$$

$$= N - \sum_i \frac{N}{p_i} + \sum_{i\neq j} \frac{N}{p_i p_j} + \cdots + \frac{(-1)^n N}{\prod_i p_i}$$

$$= N\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\ldots\left(1-\frac{1}{p_n}\right)$$

the second step to the third step can be easily proof by induction.

III. PROOF OF FERMAT'S LITTLE THEOREM

In this section we are going to prove the well known Fermat's Little Theorem using three different proof methods (induction, combinatory, and number theory). Fermat's Little Theorem state that for every natural number a and prime number p the relation below holds.

$$a^{p-1} \equiv 1\ mod\ p$$

To simplify the step of the proof, multiply the RHS and LHS by a. Then by the property of modulo the above relation becomes

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

3.1 Using Induction

First we are going to prove the above identity of Fermat's Little Theorem by induction. Since a=1 is the smallest natural number then hold the relation so we take a=1 as the base.

1. Prove that for the base, the relation holds

$$1^{p} \equiv 1\ mod\ p$$

   since the smallest prime is 2 then p will always be a positive integer. One powered by a positive integer is always equal to one. Therefore the above identity is true

2. Let a=k true (hypothesis)

$$k^{p} \equiv k\ mod\ p$$

   assume that the relation above is true, and we will using it to prove that a=k+1 is true as well.

3. Prove that for a=k+1 the relation hold as well

$$(k+1)^{p-1} modp \equiv (k+1)\ mod\ p$$

   Notice that by binomial newton

$$(k+1)^{p} = \binom{p}{0}k^{p} + \binom{p}{1}k^{p-1} + \cdots + 1$$

   Once must pay attention that combination always produce an integer result. Since as we know the combination represents the coefficient of binomial term (which always whole number). So if we pay attention to the form of

$$\binom{p}{k} = \frac{p!}{(p-k)!.k!} \ldots 0 < k < p$$

   (p-k)! doesn't divide p, same condition prevail for k. Therefore

$$\binom{p}{k} \equiv 0\ mod\ p \quad 0 < k < p, k \in \mathbb{N}$$

$$(k+1)^{p} \equiv \binom{p}{0}k^{p} + 1\ mod\ p$$

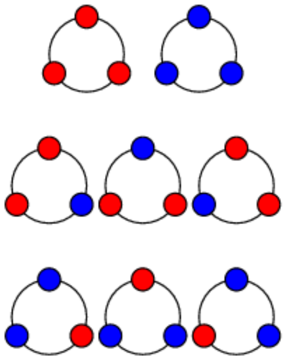
   Substitute hypothesis to the above equation

$$(k+1)^{p} \equiv k + 1\ mod\ p$$

   The proof is done and the relation is proved true (as desired)

3.2 Using Combinatory

Consider the following figures



An illustration of p=3 and x=2
source: www.artofproblemsolving.com

Consider x necklace with p beads that want to be colored by x number of colors. The total ways to color the beads is x^{p}(by considering the order) which x number of them consist of beads of the same color. For the remaining necklace there is p-1 other necklaces that similar to that necklace by rotating. It follows that

$$a^{p} - a \equiv 0\ mod\ p$$

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

3.3 Prove by Number Theory

In fact there is a general form of Fermat's Little Theorem. It's called as Euler's Theorem. The theorem states that for a positive integer N and a natural number X such that gcd(X,N)=1 (coprime) then the relation below holds

$$a^{\varphi(N)} \equiv 1\ mod\ (N)$$

Now we are going to work on the proof of the above relation. First let S be the set of integers that are coprime to N and less than N. Let a.x {x element of set S} be the set of possibly repeated integers of the form taken modulo N.

Next we will show that there are no repetitions such that $a.x_i \equiv a.x_j$ mod N that implies $x_i \equiv x_j$ (mod N). The proof is that since every element in S is smaller than N, this is not possible. Then we will show that a.x is the element of set S.This is true because $1 \le gcd(a.x,N) \le gcd(a,N).gcd(s,N) \le 1$. Therefore a.x is coprime to N.

Therefore,

$$as_1.as_2 \dots as_n \equiv s_1 s_2 \dots s_n \ (mod\ N)$$

Since $s_{1,}s_2,\dots,s_n$ are coprime to N then

$$as_1.as_2 \dots as_{\varphi(n)} = a^{\varphi(n)} \equiv 1(mod\ N)$$

Now if we would like to derive for Fermat's Little Theorem from the above relation, set N is a prime number then the number of integer that less than N and coprime to N is p-1. Therefore the relation becomes

$$a^{\varphi(n)} = a^{p-1} \equiv 1(mod\ P)$$

as desired.

IV. Conclusion

There are two ways of proof method, direct proof and implicit proof. Induction is the example of implicit proof. In the third section we have proved the Fermat's little theorem using three different methods, induction (implicit proof method), combination (explicit proof method), and number theory (explicit proof method). In the last proof we have the information that Fermat's Little Theorem is a special case of Euler's Theorem, which stated more generally about the formula.

IV. References

- ✓ Angel, Artuh. *Problem Solving Strategies.* New York :Springer
- ✓ www.artofprolemsolving.com, access date 11 November 2013
- ✓ www.brilliant.org access date 11 November 2013

Pernyataan

Dengan ini saya menyatakan bahwa makalah yang saya tulis ini adalah tulisan saya sendiri, bukan saduran, atau terjemahan dari makalah orang lain, dan bukan plagiasi.

Bandung, 12 Desember 2013

ttd

RAMANDIKA P.

Ramandika Pranamulia 13512078