13

Euler's Theorem

and

Fermat's Little Theorem

The formulas of this section are the most sophisticated number theory results in this book. The reason I am presenting them is that by use of graph theory we can understand them easily. Fermat was a great mathematician of the 17th century and Euler was a great mathematician of the 18th century. Therefore it is no surprise that Euler's theorem is a generalization of Fermat's Little Theorem.[1] Ordinarily the elegant approach is to do the more general case and then to do the less general case as an application of that. The proper pedagogical approach is almost always the opposite and therefore mirrors the historical development. This is the rare instance where I believe the best pedagogical approach is to do the general case first. In fact the best way to view Euler's theorem is through group theory. Group theory is a subject of abstract algebra that very important to advanced discrete mathematics as well as advanced geometry and many other topics. It is no coincidence that the graphical proof of Euler's theorem here is closely related to the subject of graphical representation of groups. To any one who wants to get into group theory, the book I recommend as a first book is *Groups and Their Graphs* by Grossman, and Magnus.[2]

---

[1]I can't refer to Fermat's Little Theorem by FLT as that also stands for the more celebrated *Fermat's Last Theorem*.

[2]It is a relatively inexpensive paperback published by the Mathematical Association of America in Washington, D. C.

Euler's theorem requires use of a function known as the *Euler phi function* or *totient function* and denoted by $\phi(n)$. $\phi(n)$ is defined for the positive integer n, as the number of positive integers less than n that are relatively prime to n ($\phi(1)$ is arbitrarily defined as 1). Values for the first twenty cases are given in the accompanying table. The ϕ function has many interesting properties which amongst other things greatly simplify the problem of computing $\phi(n)$. The only obvious property is that if p is a prime, $\phi(p) = p-1$.

n	$\phi(n)$
1	1
2	1
3	2
4	2
5	4
6	2
7	6
8	4
9	6
10	4
11	10
12	4
13	12
14	6
15	8
16	8
17	16
18	6
19	18
20	8

Let n be any positive integer. Then, by definition there are $\phi(n)$ numbers in Z_n that are relatively prime to n. If a and b are two of these numbers, then so is ab. This follows from Euclid's Lemma by contradiction. Suppose ab was not relatively prime to n. Then there is some prime p that divides ab and divides n. By Euclid's Lemma, p must divide a or b. Suppose for example that p divides a, then a and n both have p as a factor and are not relatively prime. This contradicts our assumptions. Hence, ab is relatively prime to n.

The Structure U_n

We will denote the integers in Z_n that are prime to n, by U_n (U stands for units: defined in section 11 as the elements with inverses). We have just shown that U_n is closed under multiplication (mod n). It is not closed under addition. We can see this by looking at U_4. 1 is an element of U_4, but $1 + 1 = 2$ is not. Hence when we look at U_n, we will be interested in the $\phi(n)$ elements of U_n under multiplication only. Since 1 is relatively prime to n for any n, we will always have that 1 belongs to U_n. Furthermore we can show that if $a \in U_n$, then there is an element a', such that $a \cdot a' = 1$. To show this, we first establish that we have cancellation. We

saw earlier that if $ca \equiv cb \pmod{n}$ then $a \equiv b \left(\mod \frac{n}{GCD(c,n)} \right)$. However, in U_n each element is relatively prime to n. This gives us, that $a \equiv b \pmod{n}$. In other words, in U_n, there is cancellation. Now suppose that $a \in U_n$. Then a^2, a^3, a^4,... belong to U_n as well. Since there are only a finite number of elements in U_n, there must be some $a^i = a^j$, where $i < j$. By cancellation, we get $a^{j-i} = 1$.[1] Hence each element in U_n has an inverse in U_n, which is a^{j-i-1}. (This also follows from Bezout's Lemma.)

Let us examine U_9 as a representative case of U_n. U_9 has $\phi(9) = 6$ elements which are {1, 2, 4, 5, 7, 8}. Consider the two graphs in **Figure 1**. In the top graph each arrow represents multiplication by 4. In the bottom graph, each arrow represents multiplication by 2. I make two claims about these graphs.

1. Under multiplication by a given element a, the graph will consists of cycles (each node has one arc entering and one arc leaving).
2. The cycles corresponding to a given multiplier, are of the same length.

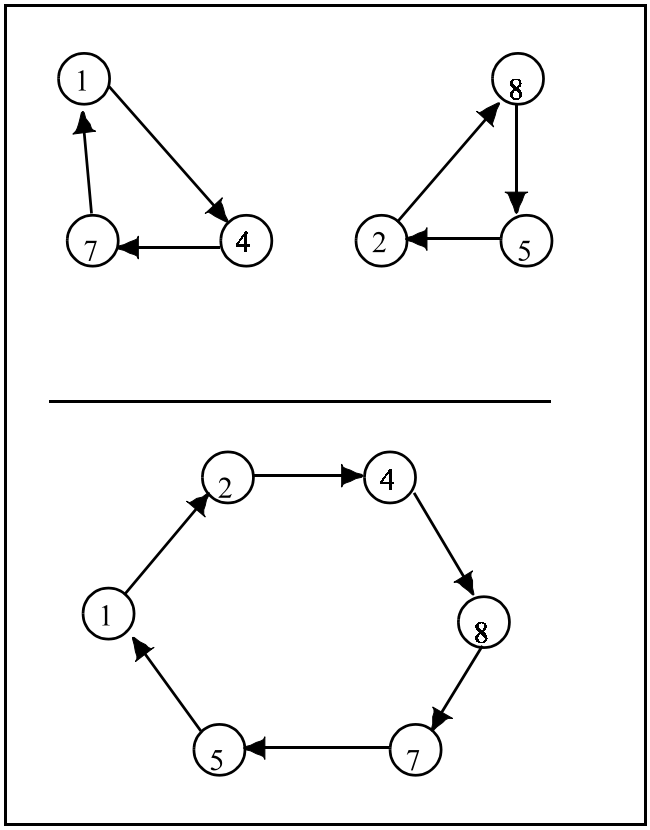

Figure 1 Two graphs of U_9

In the example U_9, when we multiply by 4, the cycles are of length 3, and when we multiply by 2, the cycles are of length 6

[1]Just cancel out a's one at a time until there are no more left on one side.

(and there is only one cycle). Suppose than in U_n, that our multiplier is m. If we have two arrows entering a node x (representing multiplication by m) then we have two points nodes, u and v, such that mu = mv. By cancellation, we get u = v and that implies only one arrow enters a given node. Since there are $\phi(n)$ arrows leaving $\phi(n)$ nodes, but only one arrow enters a given node, then there must be an arrow entering each node. This shows that the graph consists of cycles. We must show that each cycle is of the same length. In fact, if m is the multiplier, then the length of each cycle is k, where k is the smallest power such that $m^k = 1$ (we saw above that such a k must exists when we showed that each element has an inverse). If x is an element of U_n, then $xm^k = x$. Suppose on the other hand $xm^h = x$, where h is a positive integer less than k. By cancellation, we get $m^h = 1$, contradicting the definition of k as the smallest such power.[1] Hence, each cycle must of the same length.

Euler's Theorem

Suppose, $a \in U_n$. We have shown above that if we multiply each element of U_n by a, we get cycles of equal length. This length, in fact is the smallest power k such that $a^k = 1$. Since each element of U_n belongs to one such cycle, we have that k must divide the number of elements of U_n which is $\phi(n)$: i.e. there is some positive number c such that $\phi(n) = kc$. We have then that $a^{\phi(n)} = a^{kc} = 1^c = 1$. Putting this all together, we get Euler's Theorem:

$$a \perp n \Rightarrow a^{\phi(n)} \equiv 1 \pmod{n}$$

[1]This uses the fact that x, like all elements in U_n as well as m is relatively prime to n.

Example To compute $4^{100} \pmod 9$, we use that fact that $4 \perp 9$ (they are relatively prime). This implies that $4^{\phi(9)} \equiv 4^6 \equiv 1 \pmod 9$. Hence $4^{100} \equiv \left(4^6\right)^{16} 4^4 \equiv 4^4 \equiv 1 \left(\text{mod } 9\right)$.

Fermat's Little Theorem

Fermat's Little Theorem is the special case of Euler's Theorem where n is a prime. In that case $\phi(p) = p-1$. The condition that GCD(a, p) = 1 (also denoted by $a \perp p$) is equivalent to saying that p does not divide a, i.e. $p \nmid a$. This gives us:

$$p \nmid a \quad \Rightarrow \quad a^{p-1} \equiv 1 \pmod p$$

- ☐ **Exercise 1** Compute $1000^{10} \pmod{11}$
- ☐ **Exercise 2** Compute $25^{15} \pmod{31}$
- ☐ **Exercise 3** Compute $27^9 \pmod{20}$

If we multiply both sides by a, we get a statement that is true even if p|a.

$$a^p \equiv a \pmod p$$

1. Fermat's Little Theorem applies here. The answer is 1.

2. If we rewrite this as $5^{30} \pmod{31}$, Fermat's Little Theorem applies again and we get 1.

3. We have that $27 \perp 20$, also that $\phi(20) = 8$. By Euler's theorem: $27^8 \equiv 1 \pmod{20}$. Hence $27^9 \equiv 27 \equiv 7 \pmod{20}$. The answer is 7.