Module-3: Euler's Theorem and Dirichlet product

Objectives

- Generalization of Fermat's Little theorem by Euler.
- Definition and properties of Dirichlet's product.
- Möbius inversion formula.

Theorem 1 (Euler's theorem)**.** *Fix a positive integer m and let $a \in \mathbb{Z}$ be relatively prime to m. Then,* $a^{\varphi(m)} \equiv 1 \pmod{m}$.

Proof.
- Let $a_1, a_2, \ldots, a_{\varphi(m)}$ be the positive integers less than m that are relatively prime to m.
- We claim that the sets $S = \{aa_1 \pmod{m}, aa_2 \pmod{m}, \ldots, aa_{\varphi(m)} \pmod{m}\}$ and $T = \{a_1, a_2, \ldots, a_{\varphi(m)}\}$ are the same.

  As $\gcd(a_i, m) = 1$ and $\gcd(a, m) = 1$, by Lemma 12 of Module 1 of Chapter 2, we have $\gcd(aa_i, m) = 1$. Hence, $aa_i \equiv a_k$, for some k. Moreover, $\gcd(a, m) = 1$ implies that $aa_i \equiv aa_j \pmod{m}$ if and only if $a_i \equiv a_j \pmod{m}$. Thus, we see that each element in S is distinct and corresponds to some element of T. Also, the number of elements in the two sets are same and hence $S = T$.
- Thus, $a_1 \cdot a_2 \cdots \cdot a_{\varphi(m)} \equiv aa_1 \cdot aa_2 \cdots aa_{\varphi(m)} \pmod{m} = a^{\varphi(m)} a_1 \cdot a_2 \cdots a_{\varphi(m)} \pmod{m}$. As, $\gcd(a_i, m) = 1$, for all i, we get $\gcd(a_1 \cdot \cdots \cdot a_{\varphi(m)}, m) = 1$, and hence

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

□

Few applications of Euler's theorem

1. This gives an explicit formula for the inverse of a modulo m, $a^{-1} \equiv a^{\varphi(m)-1} \pmod{m}$.

2. Whenever p is prime $\varphi(p) = p-1$. Thus, Fermat's Little theorem (FLT) can be seen as a corollary to Euler's theorem.

3. Let $n = n_1 n_2 \cdots n_k$, where $\gcd(n_i, n_j) = 1$ for all $i \neq j$. Now by choosing

$$N_i = \frac{n}{n_i} \text{ and } y = a_1 N_1^{\varphi(n_1)} + a_2 N_2^{\varphi(n_2)} + \cdots + a_k N_k^{\varphi(n_k)},$$

we see that

$$N_i \equiv 0 \pmod{n_j} \text{ whenever } i \neq j,\ y \equiv a_i N_i^{\varphi(n_i)} \pmod{n_i} \text{ for } 1 \leq i \leq k, \text{ and } N_i^{\varphi(n_i)} \equiv 1 \pmod{n_i}.$$

Consequently, y is a solution of the system of linear equations

$$x \equiv a_i \pmod{n_i} \text{ for } 1 \leq i \leq k.$$

This gives an alternate proof of the Chinese remainder theorem.

4. Let n be an odd integer with $5 \nmid n$. Then, n divides an integer all of whose digits are equal to 1.

Proof. Since n is odd and $5 \nmid n$, $\gcd(n, 10) = 1$. So, $\gcd(9n, 10) = 1$ and hence by Euler's theorem

$$10^{\varphi(9n)} \equiv 1 \pmod{9n}.$$

Or equivalently, there exists a $k \in \mathbb{Z}$ such that $kn = \frac{10^{\varphi(9n)}-1}{9}$, an integer whose all digits are 1. □

Now we will look for an alternate proof for Euler's theorem. But this proof uses Fermat little theorem and φ is multiplicative.

Proof. First by using induction, we prove the result for $n = p^k$, where p is prime. That is we show $a^{\varphi(p^k)} \equiv 1 \pmod{p^k}$, where $(a, p) = 1$ and $k \in \mathbb{N}$. By Fermat's Little theorem the result is true for

$k=1$. Assume $a^{\varphi(p^k)} \equiv 1 \pmod{p^k}$ is true for $k=m$. That is $a^{\varphi(p^m)} = tp^m + 1$ for some $t \in \mathbb{Z}$. Now we will show the result is true for $k=m+1$. Consider

$$\begin{aligned} a^{\varphi(p^{m+1})} &= a^{p^{m+1}(1-1/p)} \\ &= a^{p(p^m(1-1/p))} \\ &= a^{p\varphi(p^m)} = (tp^m+1)^p \end{aligned}$$

Thus $a^{\varphi(p^{m+1})} = 1 + \binom{p}{1}(tp^m)^1 + \binom{p}{2}(tp^m)^2 + \cdots + (tp^m)^p$. Since $p|\binom{p}{i}$ for all $i \in \{1,2,\ldots,p-1\}$. Hence $a^{\varphi(p^{m+1})} \equiv 1 \pmod{p^{m+1}}$.

Now let $n = p_1^{r_1} \cdot p_2^{r_2} \cdots p_k^{r_k}$, then $\varphi(n) = \varphi(p_1^{r_1}) \cdot \varphi(p_2^{r_2}) \cdots \varphi(p_k^{r_k})$. Hence $a^{\varphi(n)} \equiv 1 \pmod{p_i^{r_i}}$ holds for all i whenever $(a,n)=1$. Or equivalently $p_i^{r_i} | a^{\varphi(n)} - 1$ for all $1 \le i \le k$. Finally $n | a^{\varphi(n)} - 1$ follows from the fact that $p_1^{r_1}, p_2^{r_2}, \ldots p_k^{r_k}$ are mutually relatively prime. □

Definition 2. *Let f and g be arithmetic functions. Then, their* **Dirichlet product or convolution**, *denoted $f*g$, is an arithmetic function defined as*

$$(f*g)(n) = \sum_{d|n} f(d) g\left(\frac{n}{d}\right).$$

For example, $(f*g)(10) = f(1)g(10) + f(2)g(5) + f(5)g(2) + f(10)g(1)$.

Remark 3. *Since d divides n if and only if $\frac{n}{d}$ divides n, one has $(f*g)(n) = \sum_{d|n} f\left(\frac{n}{d}\right) g(d)$. Or equivalently, putting $e = \frac{n}{d}$, we have*

$$(f*g)(n) = \sum_{ed=n} f(d) g(e),$$

where $\sum_{ed=n}$ denotes summation over all pairs d,e such that $de=n$.

Properties of Dirichlet Products:

Theorem 4. *Let f, g and h be arithmetic functions. Then,*

1. *$f*g = g*f$.*

2. $(f*g)*h = f*(g*h)$.

3. $f*I = f$.

4. $f*U = Df$.

5. $U*\mu = I$.

6. $f = Df*\mu$.

Thus, Parts 4 and 5 implies that "for any two arithmetic functions f and g, $f*U = g$ if and only if $f = g*\mu$". This is called the 'Möbius inversion formula'.

Proof. Proof of Part 1: By definition,

$$\begin{aligned}(f*g)(n) &= \sum_{ed=n} f(d)g(e) \\ &= \sum_{ed=n} g(e)f(d) = \sum_{de=n} g(d)f(e) \\ &= (g*f)(n).\end{aligned}$$

Proof of Part 2: The result directly follows from definition as

$$\begin{aligned}((f*g)*h)(n) &= \sum_{ab=n} (f*g)(a)h(b) \\ &= \sum_{ab=n} \left(\sum_{de=a} f(d)g(e) \right) h(b) \\ &= \sum_{deb=n} f(d)g(e)h(b) \\ &= \sum_{deb=n} f(d)(g(e)h(b)) \\ &= \sum_{dk=n} f(d) \left(\sum_{eb=k} g(e)h(b) \right) \\ &= \sum_{dk=n} f(d)(g*h)(k) \\ &= (f*(g*h))(n).\end{aligned}$$

Proof of Part 3: Recall that $I(n) = 1$, whenever $n = 1$ and 0, otherwise. Hence,

$$(f * I)(n) = \sum d|nf(d)I\left(\frac{n}{d}\right) = f(n)\cdot 1 + \sum_{d|n,d<n} f(d)\cdot 0 = f(n).$$

Proof of Part 4: Since $U(n) = 1$ for all n, we have, $(f * U)(n) = \sum\limits_{d|n} f(d)U\left(\frac{n}{d}\right) = \sum\limits_{d|n} f(d) = (Df)(n)$.

Proof of Part 5: Follows directly from Part 4 and Theorem 4.3 of Module 1 of Chapter 3 as $U * \mu = \mu * U = D\mu$.

Proof of Part 6: Note that using Parts 3, 4 and 5, we see that

$$f = f * I = f * (U * \mu) = (f * U) * \mu = Df * \mu.$$

□

The proof of the next result is omitted as it can be recursively verified.

Lemma 5. *Let f be an arithmetic function with $f(1) \neq 0$. Then, there exists an arithmetic function g such that $f * g = I$. Moreover, g is given by*

$$g(1) = \frac{1}{f(1)} \textit{ and } g(n) = -\frac{1}{f(1)} \sum_{d|n,d<n} g(d)f\left(\frac{n}{d}\right) \textit{ for all } n \geq 1.$$

Before stating next result note that component wise multiplication of arithmetic functions f and g denoted fg and is defined as $fg(n) = f(n)g(n)$ for all $n \in \mathbb{N}$.

Theorem 6. *Let f be a multiplicative function. Then f is completely multiplicative if and only if $f^{-1} = \mu f$*

Proof. First suppose that f is completely multiplicative. We have to show that $f^{-1} = \mu f$. Consider

$$\begin{aligned}
(f * uf)(n) &= \sum_{d|n} f(n/d)\mu(d)f(d) \\
&= f(n)\sum_{d|n} \mu(d) \\
&= f(n)\sum_{d|n} \mu(d)U(n/d) = f(n)(\mu * U)(n) \\
&= f(n)I(n) = I(n).
\end{aligned}$$

Conversely suppose that $f^{-1} = \mu f$. We have to show that f is completely multiplicative. Since f is multiplicative, it is sufficient to show that $f(p^k) = f(p)^k$ for all primes p and for all $k \in \mathbb{N}$. Suppose p be an arbitrary prime number. Then we show $f(p^k) = f(p)^k$ for all $k \in \mathbb{N}$ by induction. The result is clearly true for $k = 1$. Suppose the $f(p^t) = f(p)^t$ for all $2 \leq t < k$. Since $f^{-1} = \mu f$, we have $0 = I(p^k) = (f * \mu f)(p^k) = f(p^k) + f^{-1}(p)f(p^{k-1})$ as $\mu(p^b) = 0$ for $b \geq 2$. But $f^{-1}(p) = -f(p)$. Hence we have

$$0 = f(p^k) - f(p)f(p)^{k-1}.$$

Hence $f(p^k) = f(p)^k$. □

Corollary 7. *Let f be a multiplicative function. Then f is completely multiplicative if and only if $f^{-1}(p^k) = 0$ for all primes p and for all $k \geq 2$.*

Corollary 8. *Let f be a multiplicative function. Then f is completely multiplicative if and only if $f(g * h) = fg * fh$ for all arithmetic functions g and h.*

Proof. Suppose f completely multiplicative. Consider

$$\begin{aligned} f(g*h)(n) &= f(n)(g*h)(n) \\ &= f(n)[\sum_{d|n} g(d)h(n/d)] \\ &= \sum_{d|n} f(d)g(d)f(n/d)h(n./d) = fg * fh(n) \end{aligned}$$

Conversely suppose that $f(g * h) = fg * fh$ for all arithmetic functions g and h. Suppose $g = U, h = \mu$, then $f(g * h) = fg * fh$ becomes $I = f * uf$. □