1 Various Multiplicative Functions

1.1 Multiplicative Functions and The Euler Phi Function

---

1. **Introduction:** In 4.3 (Chapter 6 of the text), we looked at ϕ in Euler's Theorem. If calculating ϕ is useful, we would like to do it easily. Perhaps find some properties. The goal in this section is to introduce related concepts.

2. **Function Definitions:**

   (a) **Definition:** A function is *arithmetic* if it is defined on all positive integers.
   Ex. $f(n) = n^2$
   Ex. $f(n) = \sqrt{10 - n^2}$ is not, because it fails for $n \geq 4$.

   (b) **Definition:** An arithmetic function is *multiplicative* if, whenever $\gcd(m, n) = 1$, we have $f(mn) = f(m)f(n)$.

   (c) **Definition:** An arithmetic function is *completely multiplicative* if $f(mn) = f(m)f(n)$ always.
   Ex. $f(n) = n$ because $f(mn) = mn = f(m)f(n)$.
   Ex. $f(n) = n^3$ because $f(mn) = (mn)^3 = m^3n^3 = f(m)f(n)$.
   Ex. $f(n) = n+1$ because $f(3{\cdot}3) = f(9) = 10$ but $f(3)f(3) = 4{\cdot}4 = 16$.
   Clearly, all completely multiplicative functions are multiplicative. Are there any functions which are multiplicative but not *completely* multiplicative.

   Note: ϕ is not completely multiplicative because

   $$\phi(10)\phi(10) = 4 \cdot 4 = 16 \neq 25 = \phi(100) = \phi(10)\phi(10)$$

   Is ϕ, perhaps, multiplicative?

3. **Theorem** If f is multiplicative and $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n}$ then

   $$f(n) = f(p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n}) = f(p_1^{\alpha_1}) f(p_2^{\alpha_2}) \cdots f(p_n^{\alpha_n})$$

   Proof. This follows from being multiplicative. □

4. **Back to ϕ:**

   (a) **Theorem:** If p is prime then $\phi(p) = p - 1$

   Proof. All of $1, 2, 3 \cdots, p - 1$ are coprime to p. □

   (b) **Theorem:** If p is prime then $\phi(p^k) = p^k - p^{k-1}$.

Proof. Of all the numbers $1, 2, 3 \cdots, p-1$, the only ones which are not coprime to p^k are the multiples of p itself. Those are $p, 2p, 3p, \cdots, p^{k-1}p$ and so there are p^{k-1} of these. The remaining ones are coprime and there are $p^k - p^{k-1}$ of these. $\square$

Ex. $\phi(125) = \phi(5^3) = 5^3 - 5^2 = 100$.
Ex. $\phi(7^3) = 7^3 - 7^2 - 243 - 49 = 194$.

It is often good to note: $\phi(p^k) = p^{k-1}(p-1)$, $\phi(p^k) = p^k\left(1 - \frac{1}{p}\right)$.

(c) **Theorem:** The Euler Phi function is multiplicative.
Ex. To model the proof after $\phi(6 \cdot 5)$, where $m = 6$ and $n = 5$. List $1, 2, \cdots, 30$.

$$\begin{array}{llllll}
\boxed{1} & \boxed{7} & \boxed{13} & \boxed{19} & 25 & \\
2 & 8 & 14 & 20 & 26 & \textit{-ignore} \\
3 & 9 & 15 & 21 & 27 & \textit{-ignore} \\
4 & 10 & 16 & 22 & 28 & \textit{-ignore} \\
5 & \boxed{11} & \boxed{17} & \boxed{23} & \boxed{29} & \\
6 & 12 & 18 & 24 & 30 & \textit{-ignore}
\end{array}$$

We see that there are two rows to consider and $\phi(6) = 2$ within each of those rows there are 4 good values and $\phi(5) = 4$. So we see that two rows with four values each $= 2 \cdot 4$ values which is $\phi(6)\phi(5)$. Thus $\phi(6 \cdot 5) = \phi(6)\phi(5) = 8$.

Proof. Look at $\phi(mn)$ with $\gcd(m, n) = 1$. List them all,

$$\begin{array}{llll}
1 & m+1 & \cdots & (n-1)m+1 \\
2 & m+2 & \cdots & (n-1)m+2 \\
\vdots & \vdots & \ddots & \vdots \\
m & m+m & \cdots & (n-1)m+m = mn
\end{array}$$

Consider row r with $1 \le r \le m$. This row is $r, m+r, 2m+r, \cdots, (n-1)m+r$. All have the form $km+r$ with $0 \le k \le n-1$. Note that $\gcd(km+r, m) = \gcd(r, m)$. So the entire of row r is coprime to m if and only if r is coprime to m. So throw out those entire rows which are not coprime to m because the values are not coprime to m, hence not coprime to mn. Note that $\phi(m)$ rows remains, look at each row which remains. Each is a row r with $\gcd(r, m) = 1$. Observe that $\{0, 1, 2, \cdots, n-1\}$ is a CSOR mod n and since $\gcd(m, n) = 1$, so is the set $\{0 \cdot m + r, 1 \cdot m + r, \cdots, m(n-1) + r\}$. Note this is one of our rows, row r. Out of that CSOR, $\phi(n)$ will be coprime to n those are also coprime to m because they are in a row which survived. Thus they are coprime to mn.

Finally: $\phi(m)$ rows survive, in each $\phi(n)$ entries. Thus $\phi(m)\phi(n)$ entires coprime to mn. So $\phi(mn) = \phi(m)\phi(n)$ $\square$

(d) **Corollary:** For $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ we have:

$$\begin{aligned}
\phi(n) &= \phi(p_1^{\alpha_1} \cdots p_k^{\alpha_k}) \\
&= \phi(p_1^{\alpha_1}) \cdots \phi(p_k^{\alpha_k}) \\
&= (p_1^{\alpha_1} - p_1^{\alpha_1 - 1}) \cdots (p_k^{\alpha_k} - p_k^{\alpha_k - 1}) \\
&= p_1^{\alpha_1}\left(1 - \frac{1}{p_1}\right) \cdots p_k^{\alpha_k}\left(1 - \frac{1}{p_k}\right) \\
&= n\left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_k}\right)
\end{aligned}$$

Ex. $\phi(100) = 100(1 - \frac{1}{2})(1 - \frac{1}{5}) = 100(\frac{1}{2})(\frac{4}{5}) = 40$.
Ex. To find $\phi(432)$ we find $432 = 2^4 \cdot 3^3$ and so:

$$\phi(432) = 432\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right) = 144$$

Observation For Analysis:

- If some prime $p \mid n$ then $p - 1 \mid \phi(n)$.
- If some $p^\alpha \mid n$ then $p^{\alpha-1} \mid \phi(n)$.

This can help us with a calculation like the following.

Ex. Find all n with $\phi(n) = 6$.
First note if $p \mid n$ then $p - 1 \mid \phi(n) = 6$, thus we can only have $p - 1 = 1, 2, 3, 6 \implies p = 2, 3, 4, 7 \implies p = 2, 3, 7$ (4 is not prime). Thus the only primes are $p = 2, 3, 7$. So we now know n is of the form $n = 2^\alpha 3^\beta 7^\gamma$ with $\alpha, \beta, \gamma \geq 0$.

- If $\alpha \geq 1$ then $2^\alpha \mid n \implies 2^{\alpha-1} \mid \phi(n) = 6$ and so $\alpha = 0, 1, 2$.
- If $\beta \geq 1$ then $3^\beta \mid n \implies 3^{\beta-1} \mid \phi(n) = 6$ and so $\beta = 0, 1, 2$.
- If $\gamma \geq 1$ then $7^\gamma \mid n \implies 7^{\gamma-1} \mid \phi(n) = 6$ and so $\gamma = 0, 1$.

So then $\phi(n) = 6$ then $n = 2^\alpha 3^\beta 7^\gamma$ with $\alpha = 0, 1, 2$, $\beta = 0, 1, 2$, and $\gamma = 0, 1$. These are all neccessary but *not* sufficient, we have to check each combination.

$$
\begin{aligned}
\phi(2^0 3^0 7^0) &= 1 \\
\phi(2^0 3^0 7^1) &= 6 \\
&\vdots \\
\phi(2^0 3^2 7^0) &= 6 \\
&\vdots \\
\phi(2^1 3^2 7^0) &= 6 \\
&\vdots \\
\phi(2^1 3^0 7^1) &= 6 \\
&\vdots
\end{aligned}
$$

Thus $n = 7, 9, 14, 18$.

Ex. $\phi(n) = 97$ if $p \mid n$ then $p - 1 \mid \phi(n) = 97$, $p - 1 = 1 \implies p = 2$. Then $n = 2^\alpha$ with $\alpha \geq 0$. If $\alpha \geq 1$, then $2^\alpha \mid n \implies 2^{\alpha-1} \mid 97$ so no $\alpha \geq 1$ works, $n = 2^0$.

1.2 The Sum and Number of Divisors

---

1. **Introduction:** We can define two more related functions besides Euler's Phi function.
   Definition: $\tau(n)$ is the number of positive divisors of n.
   Definition: $\sigma(n)$ is the sum of all positive divisors of n.
   Ex. $\tau(6) = 4$ because $1, 2, 3, 6 \mid 6$.
   Ex. $\sigma(6) = 1 + 2 + 3 + 6 = 12$.

   It turns out that these are also multiplicative functions, this will allow nice formulas.

2. **Formulas:**

   (a) First note that $\tau(p^\alpha) = \alpha + 1$ because the divisors are $1, p^1, \cdots, p^\alpha$. So now for $n = p^{\alpha_1} \cdots p^{\alpha_k}$ we have

   $$\tau(n) = (\alpha_1 + 1)(\alpha_2 + 1) \cdots (\alpha_k + 1)$$

   because τ is multiplicative.

(b) Then note that $\sigma(p^\alpha) = 1 + p + p^2 + \cdots + p^\alpha = \sum_{i=0}^{n} p^i = \frac{p^{\alpha+1}-1}{p-1}$. So now for $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ we have

$$\sigma(n) = \left(\frac{p_1^{\alpha_1+1} - 1}{p_1 - 1}\right) \cdots \left(\frac{p_k^{\alpha_k+1} - 1}{p_k - 1}\right)$$

because σ is multiplicative.

Ex. If $n = 3^2 \cdot 5^5 \cdot 11$ then $\tau(n) = (2+1)(5+1)(1+1) = 36$ and then $\sigma(n) = \left(\frac{3^3-1}{3-1}\right)\left(\frac{5^6-1}{5-1}\right)\left(\frac{11^2-1}{11-1}\right)$

3. **Proving τ and σ are Multiplicative**

Theorem: Suppose $f(n)$ is multiplicative. Define $F(n) = \sum\limits_{d|n} f(d)$ (Summatory Function) i.e. $F(6) = f(1) + f(2) + f(3) + f(6)$. If the base function is multiplicative, then the summatory function is also multiplicative.

Proof. Claim $F(mn) = F(m)F(n)$ with $\gcd(m, n) = 1$. The proof then follows,

$$\begin{aligned} F(mn) &= \sum_{d|mn} f(d) \\ &= \sum_{d_1|m, d_2|n} f(d_1 \cdot d_2) \\ &= \sum_{d_1|m, d_2|n} f(d_1)f(d_2) \\ &= \sum_{d_1|m} f(d_1) \sum_{d_2|n} f(d_2) \\ &= F(m)F(n) \end{aligned}$$

□

Corollary: Let $f(n) = 1$. This is clearly multiplicative (completely multiplicative), so $F(n) = \sum\limits_{d|n} 1$ is multiplicative. But $F(n) = \tau(n)$ so τ is multiplicative.

Corollary: Let $f(n) = n$. This is also completely multiplicative, so $F(n) = \sum\limits_{d|n} f(d)$ is multiplicative. But $F(n) = \sigma(n)$ so σ is multiplicative.

1.3 Perfect Numbers and Mersenne Primes

1. **Introduction:** The definition of the sum of the divisors of a positive integer leads to the concept of a perfect number which is intrinsically connected to a Mersenne prime.

2. **Definition:** A positive integer is *perfect* if the sum of the positive divisors equals twice the integer, that is, $\sigma(n) = 2n$.
   Ex. The integer $n = 6$ is a perfect number since $\sigma(6) = 1 + 2 + 3 + 6 = 12 = 2(6)$.

3. **Finding Perfect Numbers:** It is unknown whether there are infinitely many perfect numbers and it is unknown whether there are any odd perfect numbers - all perfect numbers which have been found have been even. Currently there are only 51 known perfect numbers, the largest of which has 49724095 digits.

4. **Theorem:** If $n \in \mathbb{Z}^+$ is perfect and even if and only if $n = 2^{m-1}(2^m - 1)$ for some $m \in \mathbb{Z}$ with $m \geq 2$ and $2^m - 1$ being prime. To find perfection look at $2^m - 1$'s until we get primes!

   - $2^2 - 1 = 3$ prime! So $2^{2-1}(2^2 - 1) = 2(3) = 6$ perfect!
   - $2^3 - 1 = 7$ prime! So $2^{3-1}(2^3 - 1) = 4(7) = 28$ perfect!
   - $2^4 - 1 = 15$ nope!
   - $2^5 - 1 = 31$ prime! So $2^{5-1}(2^5 - 1) = (16)(31) = 496$ perfect!
   - $2^6 - 1 = 63$ nope!
   - $2^7 - 1 = 127$ prime! So $2^{7-1}(2^7 - 1) = 8128$ perfect!
   - $2^8 - 1 = 255$ nope!
   - $2^9 - 1 = 511 = (7)(73)$ nope!
   - $2^{10} - 1 = 1023 = (3)(11)(31)$ nope!
   - $2^{11} - 1 = 2047 = (23)(89)$ nope!

   Up until here it seemed that $2^p - 1$ is prime but not so.

   Proof.
   $\Leftarrow$: Suppose $2^m - 1$ is prime with $m \geq 2$. Define $n = 2^{m-1}(2^m - 1)$ and claim that n is perfect. Claim $\sigma(n) = 2n$, look at $\sigma(n) = \sigma(2^{m-1}(2^m - 1))$ well, $2^m - 1 \geq 3$ and is odd, 2^{m-1} is a power of 2, so $\gcd(2^{m-1}, 2^m - 1) = 1$. So, $\sigma(2^{m-1}(2^m - 1)) = \sigma(2^{m-1})\sigma(2^m - 1)$. Then observe from 5.2.2a,

   $$\sigma(2^{m-1}) = \frac{2^m - 1}{2 - 1} = 2^m - 1$$

   and

   $$\sigma(2^m - 1) = 1 + (2^m - 1)$$

   because $2^m - 1$ is prime. So $\sigma(2^{m-1})\sigma(2^m - 1) = (2^m - 1)(2^m) = 2 \cdot 2^{m-1}(2^m - 1) = 2n$. Thus, $\sigma(n) = 2n$.

$\Rightarrow$: This direction is fairly lengthy and will be omitted. It is in the text if you're interested. $\square$

5. **Theorem:** If $2^m - 1$ is prime then m is prime. I.e. if m is composite then $2^m - 1$ is composite.

   Proof. If m is composite then $m = ab$ with $a, b > 1$, then observe

   $$2^m - 1 = 2^{ab} - 1 = (2^a - 1)(2^{a(b-1)} + 2^{a(b-2)} + \cdots + 2^{a(1)} + 1)$$

   So 2^m is composite. $\square$

   All together we see,

   $$[m \text{ prime }] \Leftarrow [2^m - 1 \text{ prime }] \iff \left[2^{m-1}(2^m - 1) \text{ perfect }\right]$$

   Definition: The m^{th} Mersenne number is $M_m = 2^m - 1$.

   Definition: If p is prime and if $2^p - 1$ is also prime then $M_p = 2^p - 1$ is a Mersenne prime.

   Ex. $2^5 - 1 = 31$ is a Mersenne prime.

   Ex. 29 is a prime but not a Mersenne prime because it is not of the form $2^p - 1$.

   Suppose p is prime. We know $2^p - 1$ might be prime. Is there a way of checking besides trying all divisors?

6. **Theorem:** If p is prime, then all factors of $2^p - 1$ must have the form $2pk + 1$ for $k \in \mathbb{Z}^+$.

   Theorem: We only need to check factors of this form.

   Proof. Omitted, the proof is not long but depends on an obscure lemma related to the Eulcidean Algorithm. $\square$

   Ex. Consider $p = 11$ is prime. Look at $2^{11} - 1 = 2047$, by the theorem check $2(11)k + 1 = 22k + 1$ for $k = 1, 2, 3, \cdots$. Also only check up to $\sqrt{2047} \approx 45.24$, so only check 23 and 45. We find $2047 = (23)(89)$. Not Prime!

   Ex. Consider $p = 13$ is prime. Look at $2^{13} - 1 = 8191$, by the theorem check $2(13)k = 26k + 1$ for $k = 1, 2, 3, \cdots$. Also only check up to $\sqrt{8191} \approx 90.5$, so only check 27, 53, 79. None of the factors check so 8191 is prime.

1.4 Problems

1. Find all n satisfying $\phi(n) = 18$.
2. Show there are no n with $\phi(n) = 14$.
3. For what values of n is $\phi(n)$ odd? Justify.
4. Prove that $f(n) = \gcd(n, 3)$ is multiplicative. (This is actually true if 3 is replaced by any positive integer.)
5. Find $\tau(2 \cdot 3^2 \cdot 5^3 \cdot 11^5 \cdot 13^4 \cdot 17^5 \cdot 19^5)$
6. Find $\sigma(2 \cdot 3^2 \cdot 5^3 \cdot 11^5 \cdot 13^4 \cdot 17^5 \cdot 19^5)$
7. Find $\tau(20!)$.
8. Classify all n with $\tau(n) = 30$. Explain!
9. Prove that $\sigma(n) = k$ has at most a finite number of solutions when k is a positive integer.
10. Show that if a and b are positive integers and p and q are distinct odd primes then $n = p^a q^b$ is deficient.
11. Prove that a perfect square cannot be a perfect number.
12. Use Theorem 7.12 to determine whether each of the following Mersenne numbers is a Mersenne prime:
    (a) M_{11}
    (b) M_{21}
    (c) M_{31}