Number Theory Section Summary: 7.2
Euler's Phi Function

1. Summary

   Euler's phi function is another number theoretic function, and an extremely important one as it allows us to generalize Fermat's Little Theorem (details in section 7.3). Leonhard Euler (1707-1783) is really quite an amazing character, and hopefully you enjoyed the description given of his life in section 7.1. Please do read the historical notes, and remember some of these stories!

2. **Definitions**

   Definition 7.1: For $n \geq 1$, let $\phi(n)$ denote the number of positive integers not exceeding n that are relatively prime to n.

   Problem: compute

   - $\phi(24)$ $1, 5, 7, 11, 13, 17, 19, 23$

     $= 8$

   - $\phi(32)$ $1, 3, 5, 7, 9, 11, 13, 15, 17, 19, 21, 23, 25, 27, 29, 31$

     $= 16$

     Conjecture: $\varphi(2^k) = 2^{k-1}$

   - $\phi(13)$ $= 12$

- $\phi(p)$, p prime

$$\varphi(p) = p - 1$$

3. Theorems

Theorem 7.1: If p is prime and $k > 0$, then

$$\phi(p^k) = p^k - p^{k-1} = p^k\left(1 - \frac{1}{p}\right)$$

Those not rel. prime to p^k:

$$\underbrace{1\cdot p,\ 2p,\ 3p,\ \ldots,\ p^{k-1}}\cdot p$$

$$\varphi(p^1) = p^1 - p^0 = p - 1$$

$$\varphi(32) = \varphi(2^5) = 2^5 - 2^4 = 32 - 16 = 16 \checkmark$$

Lemma: Given integers a, b, c, $\gcd(a, bc) = 1$ if and only if $\gcd(a, b) = 1$ and $\gcd(a, c) = 1$.

Proof:

$\Rightarrow$: Given $\gcd(a, bc) = 1$. $\exists\, x, y$ /

$ax + (bc)y = 1 \Rightarrow \left.\begin{array}{l} ax + b(cy) = 1 \text{ and} \\ ax + c(by) = 1 \end{array}\right\} \Rightarrow$

$\gcd(a, b) = \gcd(a, c) = 1$.

$\Leftarrow$: Assume $\gcd(a,b) = \gcd(a,c) = 1$. And BWOC assume that $\gcd(a, bc) = d > 1$. $\exists$ a prime factor p of d, so $p | a$ and $p | bc$.

$p | bc \Rightarrow p$ divides either b or c. WLOG assume $p | b$. Then $\gcd(a, b) \geq p > 1$, a contradiction.

That establishes the lemma.

Theorem 7.2: The function ϕ is a multiplicative function.

Show that $\varphi(mn) = \varphi(m)\varphi(n)$ when $\gcd(m,n)=1$.

$\gcd(km+r, m) = \gcd(r,m)$

$$\begin{array}{cccccc} \multicolumn{6}{c}{\overbrace{\qquad\qquad\qquad\qquad\qquad\qquad}^{\varphi(m) \text{ are relatively prime to } m}} \\ 1 & 2 & \cdots & r & \cdots & m \\ m+1 & m+2 & \cdots & m+r & \cdots & 2m \\ \vdots & & & & & \\ (n-1)m+1 & (n-1)m+2 & \cdots & (n-1)m+r & \cdots & nm \end{array}$$

given a column, relatively prime to m, how many within the column are relatively prime to n?
$\varphi(n)$

$\varphi(mn) = \varphi(m)\cdot\varphi(n)$

$\gcd(m,n)=1$

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30

$\varphi(30) = \varphi(10)\cdot\varphi(3)$

$\varphi(30) = 8$

Theorem 7.3: If the integer $n > 1$ has the prime factorization $p_1^{k_1}p_2^{k_2}\cdots p_r^{k_r}$, then

$$\phi(n) = (p_1^{k_1} - p_1^{k_1-1})(p_2^{k_2} - p_2^{k_2-1})\cdots(p_r^{k_r} - p_r^{k_r-1}) = n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_r}\right)$$

$$= p_1^{k_1}\left(1-\frac{1}{p_1}\right)\cdots p_r^{k_r}\left(1-\frac{1}{p_r}\right) = p_1^{k_1}\cdots p_r^{k_r}\left(1-\frac{1}{p_1}\right)\cdots\left(1-\frac{1}{p_r}\right)$$

Proof: ϕ is a multiplicative function!

Theorem 7.4: For $n > 2$, $\phi(n)$ is an even integer.

Proof: Suppose $n = 2^k$, $k \geq 2$.

$$\varphi(n) = \varphi(2^k) = 2^k\left(1-\frac{1}{2}\right) = 2^{k-1},$$

which is even since $k \geq 2$.

Consider $n \neq 2^k$ for some $k \geq 2$.

$\exists\ p > 2$, prime factor of n. So we can write $n = p^k \cdot m$ where $\gcd(p^k, m) = 1$, and $k \geq 1$.

$$\varphi(n) = \varphi(p^k \cdot m) = \varphi(p^k) \cdot \varphi(m)$$

and

$$\varphi(p^k) = p^k\left(1 - \frac{1}{p}\right) = p^{k-1} \cdot p\left(1 - \frac{1}{p}\right)$$

$$= p^{k-1}\underbrace{(p-1)}_{2 \mid p-1} \qquad (k \geq 1)$$

so $\quad 2 \mid \varphi(p^k)$.

$\therefore \quad 2 \mid \varphi(n) \quad \forall n > 2$.

#4a $\quad n$ odd $\Rightarrow \quad \varphi(\underbrace{2n}_{\gcd(2,n)=1}) = \varphi(n)$

$\therefore$ use multiplicative

$$\varphi(2n) = \varphi(2) \cdot \varphi(n) = 1 \cdot \varphi(n)$$

$$= \varphi(n)$$

#4b $\quad n$ even $\Rightarrow \quad \varphi(2n) = 2\varphi(n)$

$n = 2^k \cdot m \quad$ where $2 \nmid m$.

$2n = 2^{k+1} \cdot m$

$$\varphi(2n) = \varphi(\underbrace{2^{k+1} \cdot m}_{\gcd(2^{k+1}, m) = 1}) = \varphi(2^{k+1}) \cdot \varphi(m)$$

$$= 2^k \cdot \varphi(m)$$

$$= 2\, 2^{k-1} \cdot \varphi(m)$$

$$= 2\, \varphi(2^k) \cdot \varphi(m)$$

$$= 2\, \varphi(n)$$

#8 $n = 2^k \underbrace{p_1^{k_1} \cdots p_r^{k_r}}$ $\quad k \geq 0 \; ; \; k_i \geq 1$

$p_1 \to p_r$ are odd primes, distinct

Show that $2^r \mid \varphi(n)$

$$\varphi(n) = \varphi(2^k)\, \underbrace{\varphi(p_1^{k_1}) \cdots \varphi(p_r^{k_r})}$$

$= \varphi(2^k)$ Each term $p_i^{k_i}$ is odd, hence $\varphi(p_i^{k_i})$ is divisible by 2. (Theorem 7.4)

Hence

$$2^r \mid \varphi(n).$$

#9a Given $n, n+2$ twin primes. Then

$$\varphi(n+2) = \varphi(n) + 2.$$

$\varphi(n) = n - 1$

$\varphi(n+2) = (n+2) - 1$

$\therefore \; \varphi(n+2) = n - 1 + 2 = \varphi(n) + 2$ ✓

$\varphi(12) = \varphi(2^2) \cdot \varphi(3) = 2 \cdot 2 = 4$

$\varphi(14) = \varphi(2) \cdot \varphi(7) = 1 \cdot 6 = 6 = 4 + 2$ ✓

$\varphi(16) = \varphi(2^4) = 2^3 = 8 = 6 + 2$ ✓

$$\begin{cases} \varphi(20) = \varphi(2^2)\cdot\varphi(5) = 2\cdot 4 = 8 \\ \varphi(22) = \varphi(2)\,\varphi(11) = 1\cdot 10 = 10 = 8+2 \end{cases}$$