Number Theory Section Summary: 7.2
Euler's Phi Function

"conjecture"

$\varphi(p^k) = k(p$

$(p-1)\cdot p^k$

1. Summary

Here's another number theoretic function, Euler's phi function: Euler is quite a character, and hopefully you enjoyed the description given of his life in section 7.1. This function is a pre-requisite to a generalization of Fermat's Little Theorem, which is brought out in section 7.3.

$\varphi(2^4) = \cancel{4}\ 16$

$\varphi(3^2) = 3 \cdot 3 = 9$

2. **Definitions** $\varphi(p^k) = p^k - p^{k-1}$

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

- $\phi(30)$ $= 8$
- $\phi(16)$ $\phi(p)$, p prime

$\varphi(27)$

$1, 7, 11, 13, 17, 19, 23, 29$

$\varphi(16) = 8$ $\qquad \varphi(p) = p-1$

$\varphi(27) = 18$ $\qquad \varphi(p^k)$

3. **Theorems**

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

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

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

Theorem 7.2: The function ϕ is a multiplicative function.

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

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

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

$\varphi(p^k) = p^{k-1}(p-1)$

Proof (Theorem 7.2): Show that

$\varphi(m \cdot n) = \varphi(m) \cdot \varphi(n)$ when $\gcd(m, n) = 1$

$$
\begin{array}{ccccc}
1 & 2 & 3 & \cdots & m \\
m+1 & m+2 & m+3 & \cdots & 2m \\
2m+1 & 2m+2 & 2m+3 & \cdots & 3m \\
\vdots & \vdots & \vdots & & \vdots \\
(n-1)m+1 & (n-1)m+2 & (n-1)m+3 & \cdots & n\cdot m
\end{array}
$$

① Focus on the columns, the r^{th} column:

$$
\begin{array}{c}
r \\
m+r \\
2m+r \\
\vdots \\
(n-1)m+r
\end{array}
$$

Claim: if one element in the column is relatively prime to m, then they all are.

If $\gcd(km+r, m) = 1$, then

$\gcd(jm+r, m) = 1$

where $0 \le k, j \le n-1$

If $a = km+r$, then

$\gcd(a, m) = \gcd(m, r)$

(Lemma, p 27). Therefore the claim is established: every element in the column has the same gcd as r & m.

Now $\varphi(m)$ of the numbers

$1, 2, \ldots, m$ are relatively prime to m.

$\therefore$ $\varphi(m)$ columns of numbers are relatively prime to m.

Within a column (say the r^{th}) relatively prime to m, how many are also relatively prime to n?

① No two elements in the column are congruent mod n

② The elements in a column are equivalent to a full set of residues, $0, \ldots, n-1$

③ $s \equiv t \pmod{n} \Rightarrow$

$$[\gcd(s,n) = \gcd(t,n)]$$

④ Conclude that there are $\varphi(n)$ relatively prime to n per column.

① Consider

$$km + r \equiv jm + r \pmod{n}$$

$$\Rightarrow \quad km \equiv jm \pmod{n}$$

$$\Rightarrow \quad k \equiv j \pmod{n}$$

But $0 \leq k, j < n$, so $k = j$.

$\Rightarrow$ ②

③: Assume $s \equiv t \pmod{n}$. So

$$s = t + qn$$

Therefore

$$\gcd(s, n) = \gcd(t + qn, n)$$
$$= \gcd(t, n)$$

by dusty lemma, p 27.

So there are $\varphi(n)$ per column relatively prime to n.

Example: $mn = 12$, so $m = 3$ & $n = 4$

$\varphi(3) = 2$

$\varphi(4) = 2$

1	2	3
4	5	6
7	8	9
10	11	12

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

Lemma: $\gcd(a, m) = 1$ and $\gcd(a, n) = 1$

$$\Longleftrightarrow \gcd(a, mn) = 1$$

$\Leftarrow$: Assume $\gcd(a, mn) = 1$. Then

$\exists x, y$ / $ax + mny = 1$

so

$$ax + m(ny) = 1 \implies$$
$$\gcd(a, m) = 1$$

(and symmetrically for n)

$\Rightarrow$: (by contradiction)

Assume $\gcd(a,m) = \gcd(a,n) = 1$, but $d = \gcd(a, mn) \neq 1$. Then d has a prime factor p, $\ni$ $p|a$ and $p|mn$.

WLOG assume $p|m$ (p must divide one or the other of m or n). Then

$$\gcd(a,m) = p \neq 1.$$

Contradiction.

All those elements in the matrix that "double up" (that are simultaneously relatively prime to m & n) are exactly the set of elements relatively prime to mn.

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

#3 p.133

$m = 3^k \cdot 568$

$n = 3^k \cdot 638$

$\left.\begin{array}{c} \tau \\ \sigma \\ \varphi \end{array}\right\}$

$m = 3^k \cdot 2^3 \cdot 71$

$n = 3^k \cdot 2 \cdot 11 \cdot 29$

$$\tau(m) = (k+1)(3+1)(1+1) \qquad = 8(k+1)$$

$$\tau(n) = (k+1)(1+1)(1+1)(1+1) \qquad = 8(k+1)$$

$$\sigma(m) = \frac{3^{k+1}-1}{2} \cdot \frac{2^4-1}{1} \cdot \frac{71^2-1}{70} \qquad = \{\ \}\, 15 \cdot 72$$

$$\sigma(n) = \frac{3^{k+1}-1}{2} \cdot \frac{2^2-1}{1} \cdot \frac{11^2-1}{10} \cdot \frac{29^2-1}{28} \qquad = \{\ \}\, 3 \cdot 12 \cdot 30$$

$$= \{\ \}\, 1080$$

✓

$$\frac{a^2-1}{a-1} = a+1$$

Compare $\varphi(548)$ + $\varphi(638)$

$$\varphi(568) = 568 \cdot \left(1-\tfrac{1}{2}\right)\left(1-\tfrac{1}{71}\right) = 280$$

$$\varphi(638) = 638 \left(1-\tfrac{1}{2}\right)\left(1-\tfrac{1}{11}\right)\left(1-\tfrac{1}{29}\right) = 280$$

#8 $\quad n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}\, m \qquad \Big|\ p_i \neq 2$

Conclude that $2^r \mid \varphi(n)$. $\qquad \Big|\ \gcd(m, p_i) = 1$

$$\varphi(n) = \underbrace{\varphi(p_1^{k_1})}\ \underbrace{\varphi(p_2^{k_2})} \cdots \underbrace{\varphi(p_r^{k_r})}\ \varphi(m)$$

every one is even:

$$\varphi(p_i^{k_i}) = 2q_i, \quad \text{where } q_i \in \mathbb{N}$$

$$\varphi(n) = 2^r q_1 q_2 \cdots q_r \cdot \varphi(m)$$

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

9a) Given n & $n+2$ twin primes; show that $\varphi(n+2) = \varphi(n) + 2$

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

b) Given p, $2p+1$ prime & odd; then $n = 4p$ satisfies $\varphi(n+2) = \varphi(n)+2$.

$$\varphi(n) = \varphi(4 \cdot p) = \varphi(4) \cdot \varphi(p) \qquad \underline{\gcd(4,p)=1}$$
$$= 2 \cdot (p-1) = 2p-2$$
$$\varphi(4p+2) = \varphi(2 \cdot (2p+1))$$
$$= \varphi(2) \cdot \varphi(2p+1)$$
$$= 1 \cdot [(2p+1)-1]$$
$$= 2p$$
$$\varphi(n+2) = 2p = (2p-2)+2 = \varphi(n)+2$$