Euler’s Phi Function

- Let $\phi(n)$ denote the number of positive integers $m \in \{1, 2, \ldots, n\}$ such that $\gcd(m, n) = 1$, where $n \geq 2$.
  - $\phi(p) = p - 1$ for prime $p$.
  - $\phi(1) = 1$ by convention.

- It is a computationally hard problem without the knowledge of $n$’s factorization.
  - Related to the security of some cryptographical systems such as RSA.
Euler’s Phi Function: The Formula

**Theorem 61** Let \( n = p_1^{e_1} p_2^{e_2} \cdots p_t^{e_t} \) be the prime factorization of \( n \). Then

\[
\phi(n) = n \prod_{i=1}^{t} \left(1 - \frac{1}{p_i}\right).
\]

- Let \( c_i \) be the condition that a number from \( \{1, 2, \ldots, n\} \) is divisible by \( p_i \).
- The desired number is

\[
\phi(n) = N(c_1 c_2 \cdots c_t).
\]

- For distinct \( i_1, i_2, \ldots, i_k \),

\[
N(c_{i_1} c_{i_2} \cdots c_{i_k}) = \frac{n}{p_{i_1} p_{i_2} \cdots p_{i_k}}.
\]
The Proof (concluded)

- By the principle of inclusion and exclusion,

\[
\phi(n) = N(c_1 c_2 \cdots c_t) = \sum_{k=0}^{t} (-1)^k \sum_{1 \leq i_1 < \cdots < i_k \leq t} \frac{n}{p_{i_1} p_{i_2} \cdots p_{i_k}}
\]

\[
= n \sum_{k=0}^{t} (-1)^k \sum_{1 \leq i_1 < \cdots < i_k \leq t} \frac{1}{p_{i_1} p_{i_2} \cdots p_{i_k}}
\]

\[
= n \prod_{i=1}^{t} \left(1 - \frac{1}{p_i}\right). \tag{51}
\]
An Example

• Suppose \( n = p_1^{e_1} p_2^{e_2} p_3^{e_3} \).

• Then

\[
\begin{align*}
\phi(n) &= n \left( 1 - \frac{1}{p_1} \right) \left( 1 - \frac{1}{p_2} \right) \left( 1 - \frac{1}{p_3} \right) \\
&= n \left[ 1 - \left( \frac{1}{p_1} + \frac{1}{p_2} + \frac{1}{p_3} \right) + \left( \frac{1}{p_1 p_2} + \frac{1}{p_1 p_3} + \frac{1}{p_2 p_3} \right) \\
&\quad - \frac{1}{p_1 p_2 p_3} \right].
\end{align*}
\]

• This may help convince you that Eq. (51) on 423 is correct.
Application: $\phi(2^n)$

$$\phi(2^n) = 2^n \prod_{p | 2^n, p \text{ prime}} \left(1 - \frac{1}{p}\right)$$

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

$$= 2^{n-1}.$$

Indeed, the only numbers in $\{1, 2, \ldots, 2^n\}$ relatively prime with 2 are the $2^n/2 = 2^{n-1}$ odd numbers.
Euler’s Phi Function Is Multiplicative

• Let $n = m_1m_2$, where $\gcd(m_1, m_2) = 1$.

• Let $m_1 = p_1^{e_1}p_2^{e_2} \cdots p_s^{e_s}$ be the prime factorization of $m_1$.

• Let $m_2 = p_{s+1}^{e_{s+1}}p_{s+2}^{e_{s+2}} \cdots p_t^{e_t}$ be the prime factorization of $m_2$.

• From the formula on p. 422,

\[
\phi(m_1m_2) = \phi(n) = n \prod_{i=1}^{t} \left(1 - \frac{1}{p_i}\right) = m_1 \prod_{i=1}^{s} \left(1 - \frac{1}{p_i}\right) m_2 \prod_{i=s+1}^{t} \left(1 - \frac{1}{p_i}\right) = \phi(m_1) \phi(m_2).
\]
An Identity for Euler’s Phi Function

**Theorem 62** Let $1 = d_1 < d_2 < \cdots < d_m = n$ be the positive divisors of $n \in \mathbb{Z}^+$. Then $\sum_{i=1}^{m} \phi(d_i) = n$.

- Define

$$A_i \equiv \{ k \in \mathbb{Z}^+ : \gcd(k, n) = d_i, k \leq n \}.$$  

- $\{ A_1, A_2, \ldots, A_m \}$ is a partition of $\{ 1, 2, \ldots, n \}$.
  - For $1 \leq i \leq n$, $\gcd(i, n) \in \{ d_1, d_2, \ldots, d_m \}$.
  - And $\gcd(i, n)$ is unique.

- Thus $n = \sum_{i=1}^{m} |A_i|$.
The Proof (concluded)

• Now, \( k \in A_i \) if and only if \( k \leq n \) and

\[
gcd\left(\frac{k}{d_i}, \frac{n}{d_i}\right) = 1.
\]

• Hence

\[
|A_i| = |\{ j \in \mathbb{Z}^+ : j \leq \frac{n}{d_i}, \gcd(j, \frac{n}{d_i}) = 1 \}|,
\]

which equals \( \phi(\frac{n}{d_i}) \) by the definition of the phi function.

• Finally,

\[
n = \sum_{i=1}^{m} |A_i| = \sum_{i=1}^{m} \phi\left(\frac{n}{d_i}\right) = \sum_{i=1}^{m} \phi(d_i).
\]
A Loose Lower Bound for the Phi Function\textsuperscript{a}

\textbf{Theorem 63 (Hardy \& Wright, 1979)}
\[ \phi(n) > n/(6 \ln \ln n) \text{ for } n > 3. \]

\textsuperscript{a}Godfrey Harold Hardy (1877–1947) and Edward Maitland Wright (1906–2005).
Godfrey Harold Hardy (1877–1947)
Permutations without Fixed Points

• Write a permutation $f$ on $\{1, 2, \ldots, n\}$ as

$$
\begin{pmatrix}
1 & 2 & \cdots & n \\
f(1) & f(2) & \cdots & f(n)
\end{pmatrix}
$$

• There are $n!$ permutations.

• Permutation $f$ has a fixed point at $i$ if $f(i) = i$.
  – $i$ is invariant under $f$.

• When $i$ is a fixed point, then $f \cdot f \cdots f(i) = i$ for any $m \geq 0$. 
Number of Permutations without Fixed Points

What is the number of permutations without fixed points?

• Let $F_X$ be the number of permutations that fix all $i \in X$.

• By the principle of inclusion and exclusion, the desired number is

$$\sum_{X \subseteq \{1,2,\ldots,n\}} (-1)^{|X|} F_X.$$ 

• $F_X = (n - |X|)!$ as those numbers not in $X$ form a permutation.

---

*aLet $c_i$ denote the condition that $i$ is a fixed point. Then the desired number is

$$N(\overline{c_1 \ c_2 \cdots \ c_n}) = \sum_{k=0}^{n} (-1)^k \sum_{1 \leq i_1 < i_2 < \ldots < i_k \leq n} N(c_{i_1} c_{i_2} \cdots c_{i_k}) = \sum_{k=0}^{n} (-1)^k \sum_{\{i_1,i_2,\ldots,i_k\} \ F \{i_1,i_2,\ldots,i_k\}} F X \subseteq \{1,2,\ldots,n\} (-1)^{|X|} F_X.$$

©2018 Prof. Yuh-Dauh Lyuu, National Taiwan University
The Proof (concluded)

- The desired number is

\[ \sum_{X \subseteq \{1,2,\ldots,n\}} (-1)^{|X|}(n - |X|)! = \sum_{k=0}^{n} (-1)^k \binom{n}{k} (n - k)! \]

\[ = n! \sum_{k=0}^{n} \frac{(-1)^k}{k!} \quad (52) \]

\[ \approx \frac{n!}{e}, \]

where \( e = 2.71828 \ldots \).

- A constant fraction of permutations have no fixed points!

- Or, if one picks a random permutation, with roughly 40% chance, that permutation will have no fixed points!
Derangements (Also P. 432)

- A derangement is a permutation of 1, 2, \ldots, n in which 1 is not in the first place, 2 is not in the second place, etc.\(^{a}\)

- How many derangements of 1, 2, \ldots, n are there?

- Let \(c_i\) denote the condition that \(i\) is in the \(i\)th place.

- The desired number is \(N(\overline{c_1 c_2 \cdots c_n})\), which equals

\[
d_n \triangleq \sum_{i=0}^{n} (-1)^i \binom{n}{i} (n - i)! = n! \sum_{i=0}^{n} (-1)^i \frac{1}{i!} \approx e n! \quad (53)
\]

by Eq. (52) on p. 434.

\(^{a}\)Just a permutation without fixed points!
A Combinatorial Identity for $d_n$

- Let $d_k$ denote the number of derangements of $1, 2, \ldots, k$.
- By convention, $d_0 = 1$.
- Any permutation of $1, 2, \ldots, n$ can have $n - k$ fixed points for some $k$, with the rest being deranged.
- There are $\binom{n}{n-k} = \binom{n}{k}$ choices for the fixed points.
- Hence

$$n! = \sum_{k=0}^{n} \binom{n}{k} d_k. \quad (54)$$

- Alternatively,

$$1 = \sum_{k=0}^{n} \frac{d_k}{k! (n-k)!}.$$
An Example

One can numerically verify identity (54) on p. 436 with the following data:

\[
\begin{align*}
  d_0 &= 1, d_1 = 0, \\
  d_2 &= 1, d_3 = 2, \\
  d_4 &= 9, d_5 = 44, \\
  d_6 &= 265, \\
  d_7 &= 1854, \\
  d_8 &= 14833, \\
  d_9 &= 133496, \\
  d_{10} &= 1334961.
\end{align*}
\]
A Variation on Derangement

• How many permutations of 1, 2, . . . , n are there such that \(i\) is not in the \((i - 1)\)st place for \(2 \leq i \leq n\)?
  – For example, 12345 (but not 23451).

• Let \(c_i\) denote the condition that \(i\) is in the \((i - 1)\)st place.

• Now \(N(c_i) = (n - 1)!\), \(N(c_i c_j) = (n - 2)!\) with \(i \neq j\), etc.

• The desired number \(N(\overline{c_2 c_3 \cdots c_n})\) equals

\[
n! - \binom{n-1}{1}(n-1)! + \binom{n-1}{2}(n-2)! - \cdots
\]

by the principle of inclusion and exclusion.
A Variation on Derangement (continued)

\[
\begin{align*}
\sum_{i=0}^{n-1} (-1)^i \binom{n-1}{i} (n-i)! \\
&= \sum_{i=0}^{n-1} (-1)^i \frac{(n-1)! (n-i)}{i!} \\
&= n! + \sum_{i=1}^{n-1} (-1)^i \frac{(n-1)! (n-i)}{i!} \\
&= n! + \sum_{i=1}^{n-1} (-1)^i \frac{n!}{i!} - \sum_{i=1}^{n-1} (-1)^i \frac{(n-1)!}{(i-1)!} \\
&= \sum_{i=0}^{n-1} (-1)^i \frac{n!}{i!} - \sum_{i=1}^{n-1} (-1)^i \frac{(n-1)!}{(i-1)!}
\end{align*}
\]
A Variation on Derangement (concluded)

\[\begin{align*}
&= \sum_{i=0}^{n-1} (-1)^i \frac{n!}{i!} + \sum_{i=0}^{n-2} (-1)^i \frac{(n-1)!}{i!} \\
&= \sum_{i=0}^{n-1} (-1)^i \frac{n!}{i!} + \sum_{i=0}^{n-2} (-1)^i \frac{(n-1)!}{i!} \\
&\quad + \left[ (-1)^n \frac{n!}{n!} + (-1)^{n-1} \frac{(n-1)!}{(n-1)!} \right] \\
&= \sum_{i=0}^{n} (-1)^i \frac{n!}{i!} + \sum_{i=0}^{n-1} (-1)^i \frac{(n-1)!}{i!} \\
&= d_n + d_{n-1}
\end{align*}\]

(55)

from Eq. (53) on p. 435.
A Simpler Proof

- Again, how many permutations of 1, 2, ..., n are there such that \( i \) is not in the \((i - 1)\)st place for \( 2 \leq i \leq n \)?

- Consider a permutation of 1, 2, ..., n, where
  1. \( i \) is not in the \((i - 1)\)st place for \( 2 \leq i \leq n \).
  2. 1 is not in the \( n \)th place.

- There are \( d_n \) of such permutations as they are but derangements with the location restrictions shifted.

- The 2nd condition that 1 is not in the \( n \)th place is extra.

- So we need to add to \( d_n \) the number of permutations that satisfy condition 1 but not condition 2.
A Simpler Proof (concluded)

- So consider permutations of 1, 2, \ldots, n such that
  1. $i$ is not in the $(i - 1)$st place for $2 \leq i \leq n$.
  2. 1 is in the $n$th place.
- Remove 1 and rename $i$ as $i - 1$ for $2 \leq i \leq n$.
- The results are permutations of 1, 2, \ldots, $n - 1$ such that $i$ is not in the $i$th place for $1 \leq i \leq n - 1$.
- They are simply derangements of 1, 2, \ldots, $n - 1$.
- Their count is $d_{n-1}$, as desired.
Another Variation on Derangement

• Let $A \subseteq \{1, 2, \ldots, n \}$.

• How many permutations of $1, 2, \ldots, n$ induce a derangement of $A$?
  – The original derangement is a special case with $A = \{1, 2, \ldots, n \}$.

• Assume $A = \{1, 2, \ldots, m \}$, where $m \leq n$, without loss of generality.

• Let $c_i$ denote the condition that $i$ is in the $i$th place.
Another Variation on Derangement (concluded)

• The desired number is $N(c_1 c_2 \cdots c_m)$, which equals

$$\sum_{i=0}^{m} (-1)^i \binom{m}{i} (n - i)!$$

by the principle of inclusion and exclusion.

• Compare it with $d_n$ in Eq. (53) on p. 435:

$$\sum_{i=0}^{n} (-1)^i \binom{n}{i} (n - i)!.$$
Theorem 64  The number of integer solutions of
\[ x_1 + x_2 + \cdots + x_n = r, \text{ where } 0 \leq x_1, x_2, \ldots, x_n < b, \text{ is} \]
\[
\frac{\lfloor r/b \rfloor}{\sum_{m=0}^{|r/b|} (-1)^m \binom{n}{m} \binom{n + r - mb - 1}{r - mb}}.
\]

- The number of nonnegative integer solutions of
\[ x_1 + x_2 + \cdots + x_n = r \]
is
\[ N \triangleq \binom{n + r - 1}{r} \]
by p. 85.
The Proof (continued)

• Now impose upper bounds

\[ 0 \leq x_1, x_2, \ldots, x_n < b. \]

• Let \( c_i \) denote the condition that \( b \leq x_i \).

• \( N(c_i) \): The number of solutions satisfying \( c_i \) equals

\[
\binom{n + r - b - 1}{r - b}
\]

as we are solving \( x_1 + x_2 + \cdots + x_n = r - b \) for nonnegative integer solutions.
The Proof (continued)

- $N(c_i c_j)$: The number of solutions satisfying $c_i \land c_j$ with $i \neq j$ equals
  \[
  \binom{n + r - 2b - 1}{r - 2b}
  \]
  as we are solving $x_1 + x_2 + \cdots + x_n = r - 2b$.

- And so on.

- Of course, we cannot satisfy more than $\lfloor r/b \rfloor$ conditions $c_i$. 
The Proof (continued)

• Our goal is

\[ N(\overline{c_1 c_2 \cdots c_n}) \].

• Recall the inclusion-exclusion principle (47) on p. 415:\(^a\)

\[ N(\overline{c_1 c_2 \cdots c_n}) = \sum_{m=0}^{\lfloor r/b \rfloor} (-1)^m S_m. \]

\(^a\)The definition of \( S_m \) appeared on p. 414.
The Proof (concluded)

• The number of $N(c_i)$ terms in $S_1$ is $\binom{n}{1}$.
• The number of $N(c_i c_j)$ terms in $S_2$ is $\binom{n}{2}$.
• And so on.
• Finally,

$$N(\overline{c_1 c_2 \cdots c_n}) = \sum_{m=0}^{\lfloor r/b \rfloor} (-1)^m S_m$$

$$= \sum_{m=0}^{\lfloor r/b \rfloor} (-1)^m \binom{n}{m} \binom{n + r - mb - 1}{r - mb}.$$
An Example

- What is the number of positive integers $x$, where $x \leq 999$, whose sum of the 3 digits equals 20?
  - E.g., 389 and 776.
- Use $x_i$ to denote $x$’s $i$th digit.
- Now the problem is equivalent to $x_1 + x_2 + x_3 = 20$, where $0 \leq x_i < 10$.
- Equation (56) on p. 445 says the answer is
  \[
  \binom{3}{0} \binom{3+20-1}{20} - \binom{3}{1} \binom{3+20-10-1}{20-10} + \binom{3}{2} \binom{3+20-20-1}{20-20} = 36.
  \]
Generalized Principle of Inclusion and Exclusion $E_m$

- Let $E_m$ denote the number of elements in $S$ that satisfy exactly $m$ of the $t$ conditions.
  - The principle of inclusion and exclusion corresponds to $E_0$.
  - Recall Eq. (47) on p. 415:
    \[ E_0 = S_0 - S_1 + S_2 - \cdots + (-1)^t S_t. \]
Generalized Principle of Inclusion and Exclusion $E_m$ (concluded)

- Then\(^{a}\)

\[
E_m = S_m - \binom{m+1}{1}S_{m+1} + \binom{m+2}{2}S_{m+2} - \cdots + (-1)^{t-m}\binom{t}{t-m}S_t \\
= \sum_{k=m}^{t} (-1)^{k-m}\binom{k}{k-m}S_k \\
= \sum_{k=m}^{t} (-1)^{k-m}\binom{k}{m}S_k.
\]

\(^{a}\)The definition of $S_k$ appeared on p. 415.
The Proof

• If $x \in S$ satisfies fewer than $m$ conditions, then $x$ should contribute zero to $E_m$.
  – Indeed, it contributes zero to

  \[ S_m, S_{m+1}, \ldots, S_t. \]

• If $x \in S$ satisfies exactly $m$ conditions, then $x$ should contribute one to $E_m$.
  – It contributes one to $S_m$.
  – It contributes zero to

  \[ S_{m+1}, S_{m+2}, \ldots, S_t. \]
The Proof (continued)

- If $x \in S$ satisfies $m < r \leq t$ of the conditions $c_i$, then $x$ should contribute zero to $E_m$.

- Indeed, it is counted $\binom{r}{m}$ times in $S_m$, $\binom{r}{m+1}$ times in $S_{m+1}$, ..., and $\binom{r}{r}$ times in $S_r$.

- It is counted zero times for all terms beyond $S_r$.

- The total count is therefore

$$
\sum_{k=m}^{r} (-1)^{k-m} \binom{k}{m} \binom{r}{k}.
$$

a\text{Recall Eq. (48) on p. 415.}
The Proof (concluded)

By Newton’s identity (p. 32),

\[
\sum_{k=m}^{r} (-1)^{k-m} \binom{k}{m} \left( \binom{r}{k} \right) = \sum_{k=m}^{r} (-1)^{k-m} \binom{r}{m} \binom{r-m}{k-m}
\]

\[
= \sum_{k=0}^{r-m} (-1)^{k} \binom{r}{m} \binom{r-m}{k}
\]

\[
= \binom{r}{m} \sum_{k=0}^{r-m} (-1)^{k} \binom{r-m}{k}
\]

\[
= \binom{r}{m} (1 - 1)^{r-m} = 0.
\]
Permutations with $m$ Fixed Points

- Recall from p. 432 that a bijective function $f$ on \{1, 2, \ldots, n\} has a fixed point at $i$ if $f(i) = i$.

- What is the number of permutations with $m$ fixed points?

- Let $c_i$ denote the condition that $i$ is a fixed point.

- Then\(^a\)

\[
S_k = \binom{n}{k} (n-k)! = \frac{n!}{k!}.
\] (58)

\(^a\)The definition of $S_k$ appeared on p. 415.
The Proof (concluded)

• From Eq. (57) on p. 452,

\[
E_m = \sum_{k=m}^{n} (-1)^{k-m} \binom{k}{k-m} S_k
\]

\[
= \sum_{k=m}^{n} (-1)^{k-m} \binom{k}{k-m} \frac{n!}{k!}
\]

\[
= \frac{n!}{m!} \sum_{k=m}^{n} (-1)^{k-m} \frac{1}{(k-m)!}.
\]

• For example, \( E_{n-2} = n(n-1)/2 \) (permutations with \( n-2 \) fixed points).
Generalized Principle of Inclusion and Exclusion $L_m$

- Let $L_m$ denote the number of elements in $S$ that satisfy at least $m$ of the $t$ conditions.

- Then\(^a\)

$$L_m = S_m - \binom{m}{m-1} S_{m+1} + \binom{m+1}{m-1} S_{m+2}$$
$$\quad \quad - \cdots + (-1)^{t-m} \binom{t-1}{m-1} S_t$$
$$\quad = \sum_{k=m}^{t} (-1)^{k-m} \binom{k-1}{m-1} S_k. \quad \quad (59)$$

\(^a\)Compare it with Eq. (57) on p. 452: $E_m = \sum_{k=m}^{t} (-1)^{k-m} \binom{k}{m} S_k.$
The Proof

• By definition,

\[ L_m - L_{m+1} = E_m \]

for \( m < t \) by definition.

• Now we prove the identity by induction on \( m \).

• First note that \( E_t = L_t = S_t \).

• Inductively, assume that

\[ L_{m+1} = \sum_{k=m+1}^{t} (-1)^{k-(m+1)} \binom{k-1}{m} S_k. \]

• Also \( E_m = \sum_{k=m}^{t} (-1)^{k-m} \binom{k}{m} S_k \) from (57) on p. 452.
The Proof (concluded)

• Finally, $L_m$ equals

\[
L_{m+1} + E_m
\]

\[
= \sum_{k=m+1}^{t} (-1)^{k-(m+1)} \binom{k-1}{m} S_k + \sum_{k=m}^{t} (-1)^{k-m} \binom{k}{m} S_k
\]

\[
= S_m + \sum_{k=m+1}^{t} (-1)^{k-m} \left[ - \binom{k-1}{m} + \binom{k}{m} \right] S_k
\]

\[
= S_m + \sum_{k=m+1}^{t} (-1)^{k-m} \binom{k-1}{m-1} S_k \quad \text{by Lemma 2 on p. 31}
\]

\[
= \sum_{k=m}^{t} (-1)^{k-m} \binom{k-1}{m-1} S_k.
\]
Permutations with Fixed Points

- Consider permutations of \( \{1, 2, \ldots, n\} \).
- Let \( c_i \) stand for the condition that \( i \) is a fixed point.
- From Eq. (59) on p. 458 with \( m = 1 \), the number of permutations with at least one fixed point is

\[
L_1 = \sum_{k=1}^{t} (-1)^{k-1} S_k.
\]
The Proof (concluded)

• Recall that Eq. (58) on p. 456 says

\[ S_k = \frac{n!}{k!}. \]

• Hence\(^a\)

\[ L_1 = \sum_{k=1}^{n} (-1)^{k-1} S_k \]

\[ = n! \sum_{k=1}^{n} (-1)^{k-1} \frac{1}{k!} \]

\[ \approx n! \left( 1 - \frac{1}{e} \right). \]  

\(^a\) An alternative proof is via Eq. (52) on p. 434.
Checking for Consistency

• The sum of the number of permutations without fixed points \((E_0)\) and those with fixed points \((L_1)\) should be \(n!\).

• Indeed, from Eq. (52) on p. 434 for \(E_0\) and Eq. (60) on p. 462 for \(L_1\),

\[
n! \sum_{k=0}^{n} \frac{(-1)^k}{k!} + n! \sum_{k=1}^{n} \frac{(-1)^{k-1}}{k!} = n!.
\]

• Note that \(E_0\) is \(d_n\), the number of derangements.