**Fermat's Little Theorem (FLT)**

**Wilson's Theorem**: If \( p \) is prime, then \( (p-1)! \equiv -1 \pmod{p} \)

**FLT**: Let \( p \) be a prime. Let \( a \in \mathbb{Z}^+ \), \( (a, p) = 1 \).

Then \( a^{p-1} \equiv 1 \pmod{p} \)

**Proof**: Consider the sequence of integers

\[ a, 2a, 3a, \ldots, (p-1)a \]

**Claim**: These integers are all different \( \pmod{p} \) and none is congruent to zero \( \pmod{p} \).

From the claim it follows that the \( p-1 \) numbers above when considered \( \pmod{p} \) must be the numbers \( 1, 2, \ldots, p-1 \) in some order.

Therefore, \( a \cdot (2a) \cdot (3a) \cdot \ldots \cdot (p-1)a \equiv 1 \cdot 2 \cdot 3 \cdot \ldots \cdot (p-1) \pmod{p} \)

\[ (p-1)! \]

(i.e. multiplying by \( a \) is reordering)

Since \( a \cdot (2a) \cdot (3a) \cdot \ldots \cdot (p-1)a \equiv a \cdot (1 \cdot 2 \cdot 3 \cdot \ldots \cdot p-1) \)

we get \( a^{p-1} \equiv (p-1)! \pmod{p} \)

Wilson's Theorem

\[ a^{p-1} \equiv 1 \pmod{p} \]

\[ a^{p-1} \equiv 1 \pmod{p} \]
We now prove the claim:

→ Suppose \( kα \equiv k'α \pmod{p} \). Note \( α' \) exists since \((α, p) = 1\).

Then \( kαα^{-1} \equiv k'αα^{-1} \pmod{p} \) \(⇔\) \( k \equiv k' \pmod{p} \)

Since \( 1 \leq k < k' \leq p - 1 \) we conclude \( k = k' \).

→ Suppose \( kα \equiv 0 \pmod{p} \). Then \( p|k \) or \( p|α \)

which is impossible because \( 1 \leq k < p - 1 \) and \((α, p) = 1\).

Corollary: \( \overset{\Large{\pmod{p}}}{α} \equiv α \pmod{p} \) \(∀α \in \mathbb{Z} \).

Proof: If \( p|α \) then \( p|α^p \) and \( α \equiv 0 \equiv α^p \pmod{p} \)

If \( p∤α \) then \((α, p) = 1 \implies \overset{\Large{\text{FLT}}}{α^{p-1}} \equiv 1 \pmod{p} \implies \overset{\Large{\pmod{p}}}{α} \equiv α \pmod{p} \)

Corollary: \( \overset{\Large{\pmod{p}}}{α^2} \equiv α \pmod{p} \)

Proof: \( \overset{\Large{\text{FLT}}}{α} \equiv 1 \pmod{p} \implies \overset{\Large{\text{FLT}}}{α(α^2)} \equiv 1 \pmod{p} \)

that is \( α^2 \) satisfies the congruence \( \overset{\Large{\text{FLT}}}{α \equiv 1} \pmod{p} \implies \overset{\Large{\text{FLT}}}{α^2} \equiv α \pmod{p} \)

Corollary: \( \overset{\Large{\text{FLT}}}{α^2} \equiv α \pmod{p} \)

Proof: If \( d = 2 \) there is nothing to do. Suppose \( d > 2 \).

We have \( d = d + (p - 1)k \) for \( k > 0 \). Then

\[
α = α^{d} \overset{\Large{\text{FLT}}}{\equiv α \cdot (α^{p-1})^{k} \equiv α \cdot 1 \equiv α \pmod{p}}
\]
EXAMPLE: (i) Compute \( 3^{201} \pmod{11} \).

We have \( 3^{201} = (3^{20})^{10} \cdot 3 \equiv 1^{20} \cdot 3 \equiv 3 \pmod{11} \) (FLT)

(ii) Compute \( 2^{180} \pmod{89} \).

Note that \( p = 89 \) is prime and \( p-1 = 88 \).

Since \( 2^{88} \equiv 4 \pmod{88} \) \( \Rightarrow 2^{180} \equiv 2^4 \equiv 16 \pmod{89} \)

**PRIMALITY TESTING**

The converse of Wilson's theorem gives a primality test.

**Prop:** Let \( N \in \mathbb{Z}_{>1} \).

If \( (N-1)! \equiv -1 \pmod{N} \) then \( N \) is prime.

**Proof:** Suppose \( N = ab \). We will show that \( a = 1 \).

We can assume \( 1 \leq a < N \), note \( a \mid (N-1)! \).

We have \( (N-1)! \equiv -1 \pmod{N} \) \( \Rightarrow N \mid (N-1)! + 1 \)

\( \Rightarrow a \mid (N-1)! + 1 \implies a \mid ((N-1)! + 1 - (N-1)! = 1 \)

\( \Rightarrow a = 1 \)

So any factorization of \( N \) has 1 on it \( \Rightarrow N \) is prime.

This test is not practical because computing \( (N-1)! \pmod{N} \) is hard.
Fermat's Test: Let $1 < b < N$

If $b^{N-1} \not\equiv 1 \pmod{N} \implies N$ is composite

Proof: If $N$ is prime we have $(b,N) = 1$ since $b \not\equiv 0 \pmod{N}$

By FLT we have $b^{N-1} \equiv 1 \pmod{N}$ \qed

Example: $2^{90} \equiv 64 \pmod{91}$

Since $64 \not\equiv 1 \pmod{91}$ it follows that 91 is composite

Def: If $N$ is composite but $b^{N-1} \equiv 1 \pmod{N}$ for some $b$

in $1 < b < N$ we say that $N$ is a pseudoprime in base $b$.

Example: (i) $2^{340} \equiv 1 \pmod{341}$ but $341 = 11 \cdot 31$

$\implies 341$ is a pseudoprime in base 2.

(ii) $3^{340} \equiv (3^4)^{85} \cdot 3 \equiv 1^{85} \cdot 3 \pmod{31}$

By FLT

Since $3^{10} \equiv (3^3)^3 \equiv (-4)^3 \equiv 25 \pmod{31}$

We have $3^{340} \not\equiv 1 \pmod{31}$ $\implies 3^{340} \not\equiv 1 \pmod{341}$

(if $a \equiv b \pmod{m}$ then $a \equiv b \pmod{n}$ $\forall n|m$)

Thus 341 fools Fermat's test in base 2 but not in base 3.
DEF: We call an integer $N$ a \underline{Carmichael number} if it is a pseudoprime for every base $b \leq N$ such that $(b, N) = 1$.

It is not obvious that they exist.

The next theorem provides a classification of CN that (conset): A composite $N > 2$ is a Carmichael number if and only if

(i) $N$ is squarefree (i.e. $N = p_1 \cdots p_k$)

(ii) if $p | N$ is prime then $p - 1 | N - 1$

To prove the implication $\Rightarrow$ we need the notion of primitive root which will be introduced later. So we will only prove $\Leftarrow$.

Proof or $\Leftarrow$: Let $k \in \mathbb{Z}$, $(k, N) = 1$.

We have $N = p_1 \cdots p_k$ with $p_i$ distinct (from (i))

We have $N - 1 = (p_i - 1)k_i$ for some $k_i \in \mathbb{Z}$ (from (ii))
THEN \( l_0 \equiv (l_{i-1}^{p_i-1})^{k_i} \equiv 1^{k_i} \equiv 1 \pmod{p_i} \) \( \forall i \) (**) \\
\text{FLT} \\
(l_i, N) = 1 \Rightarrow (l_i, p_i) = 1 \\
\text{This means that the system} \\
\begin{align*}
X &\equiv a \pmod{p_i} \\
X &\equiv 1 \pmod{p_k}
\end{align*} \\
\text{has the solution} \, X = l_0^{N-1}. \text{ Clearly it also has} \\
\text{the solution} \, X = 1. \text{ Then by the uniqueness part} \\
of \text{ CRT,} \, l_0^{N-1} \equiv 1 \pmod{p_i \cdots p_k = N} \)

\[\text{LEM: An alternative to CRT: From (*) we have} \]
\[p_i \mid l_0^{N-1} \forall i \Rightarrow \text{LCM}(p_1, \ldots, p_k) \mid l_0^{N-1} - 1\]
\[p_1 \text{ are distinct primes} \Rightarrow p_1 \cdots p_k = N\]

\[\text{Example:} \, 567 = 3 \times 11 \times 17 \text{ is a Carmichael number}\]
\[\text{since} \, 3 - 1 = 2, \, 11 - 1 = 10, \, 17 - 1 = 16\]
\[\text{all divide} \, 567 - 1 = 560 = 2^4 \times 5 \times 7\]
Miller's Test:

1. Let \( N \) be an odd positive integer.
2. Suppose it is a pseudoprime in base \( b \geq 2 \).
   That is, \( b^{\frac{N-1}{2}} \equiv 1 \pmod{N} \).
3. Let \( x = b^{\frac{N-1}{4}} \pmod{N} \).

Recall: If \( N \) is prime and \( x_0^2 \equiv 1 \pmod{N} \) \( \Rightarrow \) \( x_0 \equiv \pm 1 \pmod{N} \).

Then, if \( N \) is prime, we conclude \( x \equiv \pm 1 \pmod{N} \).

Since \( x^2 = \left(b^{\frac{N-1}{4}}\right)^2 = b^{\frac{N-1}{2}} \equiv 1 \pmod{N} \).

Hence, if \( b^{\frac{N-1}{2}} \not\equiv \pm 1 \pmod{N} \) then \( N \) is composite.

If \( b^{\frac{N-1}{2}} \equiv 1 \pmod{N} \) and \( N-1 \) is divisible by 4,
we repeat with \( y = b^{\frac{N-1}{4}} \).

Again, \( y^2 = \left(b^{\frac{N-1}{4}}\right)^2 = b^{\frac{N-1}{2}} \equiv 1 \pmod{N} \) \( \Rightarrow \) \( y \equiv \pm 1 \pmod{N} \) if \( N \) is prime. Thus \( b^{\frac{N-1}{4}} \not\equiv \pm 1 \Rightarrow N \) composite.

If it fails we can repeat as long as \( \frac{N-1}{2^k} \)
is an integer and \( b^{\frac{N-1}{2^k}} \equiv 1 \pmod{N} \).
Example: We know that \( N = 561 \) is the smallest Carmichael number.

Then \( 5^{560} \equiv 1 \pmod{561} \) \( \forall b \in \mathbb{Z} \), \((b, 561) = 1\).

- Take \( b = 5 \). We have \( 5^{280} \equiv 67 \not\equiv \pm 1 \pmod{561} \).
- Take \( b = 2 \). We have \( 2^{140} \equiv 1 \pmod{561} \).

But \( 2^0 \equiv 67 \not\equiv 1 \pmod{561} \).

So, depending on the base we may need a different number of steps in Miller's test.

**Def:** Let \( N \in \mathbb{Z}_+ \). Write \( N - 1 = 2^s t \), where \( s > 0 \), odd.

We say that \( N \) passes Miller's test for base \( b \) if either \( b^t \equiv 1 \pmod{N} \) or \( b^{2^j t} \equiv -1 \pmod{N} \) for some \( j \) in \( 0 \leq j \leq s - 1 \).

Example: Let \( N = 2047 = 2^3 \cdot 89 \).

Then \( 2^{2046} = (2^2)^{1023} \equiv 1 \pmod{2047} \).

So \( N \) is a pseudoprime in base \( 2 \).

Moreover, \( \frac{N - 1}{2} = 1023 \) and \( 2^{1023} \equiv (2^{11})^{93} \equiv 1 \pmod{2047} \).

So \( 2047 \) fools Miller's test in the notation of the previous definition. We have \( \ell = 1023 \) and \( b^\ell \equiv 1 \pmod{N} \).
Q: CAN A COMPOSITE NUMBER PASS MILLER'S TEST IN ALL BASES?

THM: IF \( N \) IS POSITIVE, ODD AND COMPOSITE THEN \( N \) FOOLS MT FOR AT MOST \( \frac{N-1}{2^k} \) BASES \( b \) S.T. \( 1 \leq b \leq N-1 \).

Rabin's Probability Test

Let \( N \in \mathbb{Z}_2 \). Pick \( b_1, \ldots, b_k \in \mathbb{Z}_2 \)
S. T. \( 1 < b_i \leq N-1 \).

IF \( N \) IS COMPOSITE THE PROBABILITY THAT IT PASSES MT FOR ALL \( b_i \) IS LESS THAN \( \frac{1}{4^k} \).
Euler's \( \phi \) Function and Euler's Theorem

**THM (FLT):** Let \( p \) be prime and \( a \in \mathbb{Z} \) coprime to \( p \). Then \( a^{p-1} \equiv 1 \pmod{p} \)

**Q:** If instead of \( p \) we use a modulus \( M \) which is not prime, what is the smallest power \( a^x \) guaranteed to be congruent to 1 \( \pmod{M} \) ?

We will see that the answer is given by Euler's Theorem. First, we need to introduce the following function.

**DEF:** Let \( N \in \mathbb{Z}_{>0} \). The Euler \( \phi \)-function is given by

\[
\phi(N) = \# \{ x \in \mathbb{Z} : 1 \leq x \leq N \text{ AND } (x,N) = 1 \}
\]

i.e., it counts the number of integers coprime to \( N \) between 1 and \( N \).

**Ex:** \( \phi(1) = 1 \), \( \phi(2) = 1 \), \( \phi(3) = 2 \) because 1, 2 are coprime to 3.
\[ \phi(6) = 2 \text{ since from } 1, 2, 3, 4, 5, 6 \]
only 1, 5 are coprime to 6.

\[ \phi(p) = \# \{ x \in \mathbb{Z} : 1 \leq x \leq p , \ (x,p) = 1 \} = p - 1 \]

**Theorem (Euler):**

Let \( a, M \in \mathbb{Z} \) with \( M > 0 \) and \( (a, M) = 1 \).

Then \( a^{\phi(M)} \equiv 1 \pmod{M} \)

**Corollary:** Let \( M = p \) be prime.

Then \( \phi(p) = p - 1 \) and \( a^{p-1} \equiv 1 \pmod{p} \)

In other words, FLT is true.

**Proof of Euler's Theorem:** Let \( M = \mathbb{Z} \) \((a, M) = 1\).

By definition of \( \phi(M) \) there are \( \phi(M) \) integers in \([1, M]\) coprime to \( M \).

We write \( a_1, a_2, \ldots, a_{\phi(M)} \) to denote them.

Consider the integers

\( (1) \ a \cdot a_1, a \cdot a_2, \ldots, a \cdot a_{\phi(M)} \)
CLAIM: The integers in \((A)\) are all distinct \(\mod M\), satisfy \((a \cdot a_i, M) = 1\) and are not congruent to zero \(\mod M\).

From the claim it follows
\[
(a \cdot a_1)(a \cdot a_2) \cdots (a \cdot a_{\phi(n)}) \\
\equiv a_1 \cdots a_{\phi(n)} \pmod{M}
\]
\[
\Rightarrow a^{(a_1 a_2 \cdots a_{\phi(n)})} \equiv a_1 a_2 \cdots a_{\phi(n)} \pmod{M}
\]

Since \((a_1 a_2 \cdots a_{\phi(n)}, M) = 1\) there is an inverse \(X\) of \(a_1 a_2 \cdots a_{\phi(n)}\). Multiplying the previous congruence by \(X\) gives
\[
a^{\phi(n)} \equiv 1 \pmod{M}
\]

Proof of claim:

Suppose \((a \cdot a_i, M) > 1\) for some \(i\).
\[
\Rightarrow\text{ prime } p \mid a \cdot a_i \text{ and } p \mid M \\
\Rightarrow (p \mid a \text{ or } p \mid a_i) \text{ and } p \mid M \\
\Rightarrow (p \mid a \text{ and } p \mid M) \text{ or } (p \mid a_i \text{ and } p \mid M)
\]
\[ (a, m) > 1 \quad \text{and} \quad (a_i, m) > 1 \quad \text{xxx}
\]

Then \( (a, a_i, m) = 1 \) \( \Rightarrow \) \( a a_i \neq 0 \pmod{m} \)

(Otherwise \( M \mid a a_i \))

Suppose \( a a_i \equiv a a_j \pmod{M} \)

Since \( (a_i, M) = 1 \), \( \hat{a_i} \) exists \( \Rightarrow \) Hence

\[
\hat{a_i} (a a_i) = \hat{a_i} (a a_j) \Rightarrow a_i \equiv a_j \pmod{M}
\]

Because \( 0 \leq a_i, a_j \leq m - 1 \)

We conclude \( a_i = a_j \)

\[ \blacksquare \]

**DEF**: A set of integers with \( \phi(m) \) elements which are co-prime to \( M \) and no two of them are congruent \( \mod M \) is a reduced residue system \( \mod M \).

**Corollary (of claim)**: Let \( a \in \mathbb{Z} \), \( (a, m) = 1 \)

If \( \{ a_1, a_2, \ldots, a_{\phi(m)} \} \) is a \( \mathbb{Z}/m \)-set \( \mod M \)

Then \( \{ a + a_1, a + a_2, \ldots, a + a_{\phi(m)} \} \) also is
**Theorem (Formula for \( \phi \)):**

Let \( N = p_1^{a_1} \cdots p_k^{a_k} \), \( a_k \geq 1 \)

Then,

\[
\phi(N) = N \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_k}\right)
\]

\[
= \prod_{j=1}^{k} \frac{a_j - 1}{p_j - 1}
\]

**Example:** \( \phi(100) = \phi(2^2 \cdot 5^2) = 100 \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{5}\right) = 40 \)

**Example:** Compute the last decimal digits of \( 3^{50} \).

Writing in base 10: \( 3^{50} = a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + \cdots + a_1 \cdot 10 + a_0 \)

The last two digits are \( a_1 a_0 \) so we need to compute \( 3^{50} \pmod{100} \)

We have \( 3^{40} = \phi(100) \equiv 1 \pmod{100} \) by Euler's Theorem.

So \( 3^{50} = 3^{40} \cdot 3^{10} \equiv 1 \cdot 3^{10} \)

\[
\equiv 3 \cdot 3 \cdot 3 \equiv (-1)^2 \cdot 9 \equiv 49 \pmod{100}
\]
THEM (Formula for $\phi$)

Let $N = p_1^{a_1} \cdots p_k^{a_k}$, $a_k \geq 1$, $p_i$ distinct

Then,

$$\phi(N) = N \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_k}\right) = \prod_{j=1}^{k} p_j^{a_j-1} (p_j - 1)$$

Example: Find all $N \in \mathbb{Z}_+$ s.t. $\phi(N) = 1$

We have

$$\phi(N) = \prod_{j=1}^{k} p_j^{a_j-1} (p_j - 1) = 1$$

$\Rightarrow p_i - 1 | 1 \Rightarrow p_i = 2 \quad \forall p_i | N$

Then, if $N \neq 1$ we have $N = 2^{a}$, $a \geq 1$

and $\phi(N) = 2^{a-1} (2-1) = 1 \Rightarrow a = 1$

$\Rightarrow \boxed{N = 2}$ is a solution

Since $\phi(1) = 1$ then $\boxed{N = 1}$ is another solution
Example: Solve $\phi(N) = 3$

Let $N = p_1^{a_1} \cdots p_k^{a_k}$. Then $p_i \cdot 1 \mid 3 \quad \forall p_i \mid N$

$\Rightarrow p_i \cdot 1 = 1 \quad \text{or} \quad p_i - 1 = 3$

$\Rightarrow p_i = 2 \quad \text{or} \quad p_i = 4$

Since 4 is not prime we have $N = 2^a$, $a \geq 0$.

- If $a = 0 \Rightarrow N = 1$ is not a solution $\phi(1) = 1 \neq 3$
- If $a \geq 1 \Rightarrow \phi(N) = 2^{a-1} (2-1) = 3$ \quad XXX

So there are no solutions.

Example: Solve $\phi(N) = 8$

- Let $N = p_1^{a_1} \cdots p_k^{a_k}$.
- If some $p_i > 9 \Rightarrow \phi(N) \geq p_i - 1 > 8$, a contradiction
  So $p_i \leq 9$
- If $7 \mid N \Rightarrow (7-1) = 6 \mid \phi(N) = 8$, impossible
  So $p_i \neq 7 \quad \forall i$
- Thus $N = 2^a \cdot 3^b \cdot 5^c$
- If $b \geq 2 \Rightarrow 3^{b-1} \mid \phi(N) = 8$, impossible, so $b = 0, 1$.
- If $c \geq 2 \Rightarrow 5^{c-1} \mid \phi(N) = 8$, impossible, so $c = 0, 1$. 
We now divide into cases according to \( b \) and \( c \)

1. \( b = c = 0 \Rightarrow N = 2^a \quad \Rightarrow \quad \phi(N) = 2^{a-1} \)
\[ \Rightarrow a = 4 \quad \Rightarrow \quad N = 16 \]

* The case \( a = 0 \Rightarrow N = 1 \) which is no solution \( \phi(1) \neq 8 \).

2. \( b = 0, c = 1 \Rightarrow N = 2^a \cdot 5 \quad \Rightarrow \quad \phi(N) = 2^a \cdot 4 = 8 \)
\[ \Rightarrow a = 2 \quad \Rightarrow \quad N = 20 \]

* The case \( a = 0 \Rightarrow N = 5 \Rightarrow \phi(N) = 4 \neq 8 \), no solution

3. \( b = 1, c = 0 \Rightarrow N = 2^a \cdot 3 \quad \Rightarrow \quad \phi(N) = 2^a \cdot 2 = 8 \)
\[ \Rightarrow a = 3 \quad \Rightarrow \quad N = 24 \quad ; \quad a = 0 \Rightarrow N = 3 \), no sol.

4. \( b = c = 1 \Rightarrow N = 2^a \cdot 3 \cdot 5 \quad \Rightarrow \quad \phi(N) = 2^a \cdot 2 \cdot 4 = 8 \)
\[ \Rightarrow a = 1 \quad \Rightarrow \quad N = 30 \]

\[ a = 0 \Rightarrow N = 15 \Rightarrow \phi(N) = (3-2)(5-1) = 8 \]

\[ \text{so} \quad N = 15 \quad \text{is also a solution} \]
ARITHMETIC FUNCTIONS

DEF: A function whose domain is \( \mathbb{Z}_{\geq 0} \) is called an arithmetic function.

Examples:
1) \( f(N) = 1 \) \( \forall N \in \mathbb{Z}_{\geq 0} \)
2) \( f(N) = N \) \( \forall N \in \mathbb{Z}_{\geq 0} \)
3) \( \phi(N) \) (the Euler \( \phi \)-function)
4) \( \tau(N) = \text{"number of positive divisors of } N \"
5) \( \sigma(N) = \text{"sum of positive divisors of } N \"

Example: Take \( N = 6 \).

Its positive divisors are \( \{1, 2, 3, 6\} \).

Thus \( \tau(6) = 4 \) and \( \sigma(6) = 1 + 2 + 3 + 6 = 12 \).

DEF: An arithmetic function \( f \) is called multiplicative if \( f(N_1 \cdot N_2) = f(N_1)f(N_2) \) whenever \( (N_1, N_2) = 1 \). We say it is completely multiplicative if \( f(N_1N_2) = f(N_1)f(N_2) \) \( \forall N_1, N_2 \).
**THM:** The function $\phi(n)$ is multiplicative.

**Proof:** Let $N_1, N_2 > 0$ be coprime.

Let us write all the integers up to $N_1 \cdot N_2$ as follows:

\[
\begin{array}{cccccc}
1 & N_1 + 1 & 2N_1 + 1 & \cdots & (N_2 - 1)N_1 + 1 \\
2 & N_1 + 2 & 2N_1 + 2 & \cdots & (N_2 - 1)N_1 + 2 \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
R & N_1 + R & 2N_1 + R & \cdots & (N_2 - 1)N_1 + R \\
N_1 & 2N_1 & 3N_1 & \cdots & N_1 \cdot N_2
\end{array}
\]

Let $R > 0$ satisfy $1 \leq R \leq N_1$ and $(R, N_1) = d > 1$. Then all the numbers in the $R$-th row are divisible by $d$. Then they are not coprime to $N_1 \cdot N_2$. Then all the numbers coprime to $N_1 \cdot N_2$ are in the $\phi(N_1)$ rows where $(R, N_1) = 1$. 

\[\phi(n) = \prod_{p | n} \left(1 - \frac{1}{p}\right)\]

\[\phi(1 \cdot N_2) = \phi(N_2) \cdot \phi(1) = \phi(N_2)\]

By definition $\phi(n)$ is the number of positive integers up to $n$ which are coprime to $n$.
Suppose \((12, N_1) = 1\)

Then the numbers in the 12-th row are coprime to \(N_1\).

Therefore, a number in the 12-th row is coprime to \(N_1 N_2\) if and only if it is coprime to \(N_2\).

So we want to count the numbers in the 12-th row that are coprime to \(N_2\).

The \(N_2\) elements in the 12-th row are all distinct mod \(N_2\). Indeed, suppose

\[ k \cdot N_1 + 12 \equiv k' \cdot N_1 + 12 \pmod{N_2} \]

implies

\[ k \cdot N_1 \equiv k' \cdot N_1 \pmod{N_2} \]

since \((N_1, N_2) = 1\), \(N_1^{-1}\) exists mod \(N_2\)

Giving \( k \equiv k' \pmod{N_2} \)

\[ \Rightarrow k = k' \] since \(0 \leq k, k' \leq N_2 - 1\)

So, mod \(N_2\), the 12-th row contains the integers \(1, 2, \ldots, N_2\) in some order, hence exactly \(\phi(N_2)\) elements of row 12 are coprime to \(N_2\).
Because there are \( \phi(N_2) \) rows each with \( \phi(N_2) \) elements (coprime to \( N_2 \), hence coprime to \( N_1N_2 \)), we conclude \( \phi(N_1 \cdot N_2) = \phi(N_1) \cdot \phi(N_2) \).
The following gives a method to produce multiplicative functions.

**THM:** Let $f$ be an arithmetic function. Define the arithmetic function $F$ by

$$F(N) = \sum_{\substack{d \mid N \quad d > 0}} f(d) \quad \forall N \in \mathbb{Z}_{>0}$$

If $f$ is multiplicative then $F$ is multiplicative.

**THM:** $\sigma(N)$ and $\tau(N)$ are multiplicative.

**Proof:** We can write $\tau(N) = \sum_{\substack{d \mid N \quad d > 0}} 1$

And $\sigma(N) = \sum_{\substack{d \mid N \quad d > 0}} d$

Since $f(N) = 1$ and $f(N) = N$ are multiplicative, the result follows by the previous THM.
Theorem: Let \( f \) be an arithmetic function.

Define the AF \( F \) by

\[
F(N) = \sum_{d \mid N \atop d > 0} f(d) \quad \forall N \in \mathbb{Z}_{\geq 0}
\]

If \( f \) is multiplicative then \( F \) is multiplicative.

Corollary: \( \sigma(N) \) and \( \tau(N) \) are multiplicative.

Proof: Let \( N_1, N_2 \in \mathbb{Z}_{\geq 0} \) be coprime.

Want: \( F(N_1N_2) = F(N_1)F(N_2) \)

By definition \( F(N_1N_2) = \sum_{d \mid N_1N_2 \atop d > 0} f(d) \)

Claim: From \( (N_1, N_2) = 1 \) it follows that each divisor \( d \)

of \( N_1N_2 \) can be written as \( d = d_1 \cdot d_2 \) where

\( (d_1, d_2) = 1 \), \( d_1 \mid N_1 \) and \( d_2 \mid N_2 \). Also, each

such product is a divisor of \( N_1N_2 \).
\text{CLAIM} \implies F(N_1 \cdot N_2) = \sum_{d \mid \text{LCM}(N_1,N_2)} f(d) = \\
= \sum_{d_1 \mid N_1, d_2 \mid N_2} f(d_1, d_2) = \sum_{d_1 \mid N_1, d_1 > 0} f(d_1) \cdot f(d_2) \quad \text{\textit{f is multiplicative}} \\
= \left( \sum_{d_1 \mid N_1, d_1 > 0} f(d_1) \right) \left( \sum_{d_2 \mid N_2, d_2 > 0} f(d_2) \right) = F(N_1) \cdot F(N_2) \quad \square
Formulas for $\phi$, $\sigma$, $\tau$

Let $N = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$, $p_i$ distinct primes.

Let $f$ be $\phi$, $\sigma$ or $\tau$. Then

$$f(N) = f(p_1^{a_1}) f(p_2^{a_2}) \cdots f(p_k^{a_k})$$

Because we have seen these are multiplicative.

Thus to find a formula it is enough to have a formula for $f(p_i^{a_i})$ and take product.

**Lemma:** $\phi(p^a) = p^a - p^{a-1} = p^a (1 - \frac{1}{p})$

**Proof:** (Note $\phi(p) = p-1$ is a special case.)

Note $(N, p^a) = 1 \iff (N, p) = 1 \iff p \mid N$

Then $\phi(p^a) = \# \{ x \in \mathbb{Z} : 1 \leq x \leq p^a, (N, p^a) = 1 \}$

The positive multiples of $p$ which are $\leq p^a$ are the numbers of the form $kp$ for $1 \leq k \leq p^{a-1}$.

In particular, there are $p^{a-1}$ of them.

Thus $\phi(p^a) = p^a - p^{a-1}$.
**THM:** \( \phi(N) = N \prod_{p \mid N} \left( 1 - \frac{1}{p} \right) \)

**Proof:** \( \phi(N) = \phi(p_1^{a_1}) \cdots \phi(p_k^{a_k}) \)
\[
= p_1^{a_1} \left( 1 - \frac{1}{p_1} \right) \cdots p_k^{a_k} \left( 1 - \frac{1}{p_k} \right) = \prod_{i=1}^{k} \left( 1 - \frac{1}{p_i} \right) \]
\[
= N \prod_{i=1}^{k} \left( 1 - \frac{1}{p_i} \right) \]

**THM:** Let \( N = p_1^{a_1} \cdots p_k^{a_k} \), \( a_k > 1 \), \( p_i \) distinct primes

Then,
\[
\tau(N) = \prod_{i=1}^{k} (a_i + 1) \quad \sigma(N) = \prod_{i=1}^{k} \left( \frac{p_i^{a_i+1} - 1}{p_i - 1} \right) \]

**Proof:** It is enough to compute \( \sigma(p^a) \) and \( \tau(p^a) \)

- The positive divisors of \( p^a \) are \( \{1, p, p^2, \ldots, p^a\} \)
- In particular, \( p^a \) has \( a+1 \) positive divisors so \( \tau(p^a) = a+1 \)
- \( \sigma(p^a) = 1 + p + p^2 + \ldots + p^a = \frac{p^{a+1} - 1}{p - 1} \) by the formula

**Example:** \( N = 100 = 2^2 \cdot 5^2 \)
\[
\sigma(N) = \frac{2^3 - 1}{2 - 1} \cdot \frac{5^3 - 1}{5 - 1} = 7 \cdot 31 = 217
\]
\[
\tau(N) = (2+1)(2+1) = 9
\]
**Theorem:** Let $N \in \mathbb{Z}_{>0}$. Then \( \sum_{d|N} \phi(d) = N \)

**Proof:** \( F(N) = \sum_{d|N} \phi(d) \) is multiplicative because \( \phi \) is multiplicative.

Then \( F(N) = F(p_1^{a_1}) \cdots F(p_k^{a_k}) \), where \( N = p_1^{a_1} \cdots p_k^{a_k} \).

We have \( F(p) = \sum_{0 \leq i \leq \alpha} \phi(p^i) = 1 + (p-1) + (p^2 - p) + \cdots + (p^\alpha - p^{\alpha-1}) = p^\alpha \)

Therefore, \( F(N) = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k} = N \) \( \Box \)

**Example:** \( N = 12 \)

Positive divisors: \( 1, 2, 3, 4, 6, 12 \)

\( \phi(1) = \phi(2) = 1 \), \( \phi(3) = \phi(4) = \phi(6) = 2 \)

\( \phi(12) = 4 \).

Now \( F(12) = 1 + 1 + 2 + 2 + 2 + 4 = 6 + 6 = 12 \).

As expected.
**Perfect Numbers**

**Def:** An integer \( N > 0 \) is called **perfect** if \( \sigma(N) = 2N \)

**Ex:** \( N = 6 \) has positive divisors \( \{1, 2, 3, 6\} \)

\[ \sigma(6) = 1 + 2 + 3 + 6 = 12 = 2 \cdot 6 \]

**Ex:** \( N = 28 \) has positive divisors \( \{1, 2, 4, 7, 14, 28\} \)

\[ \sigma(28) = 1 + 2 + 4 + 7 + 14 + 28 = 28 + 28 = 2 \cdot 28 \]

**Def:** We call the integer \( M_N = 2^N - 1 \) the \( N \)-th **Mersenne Number**. If \( M_N \) is prime, we say it is a **Mersenne Prime**.

**Thm:** If \( M_N \) is prime then \( N \) is prime.

**Proof:** Suppose \( N = a \cdot b \) with \( 1 < a, b < N \), so \( N \) is composite.

We have

\[ 2^N - 1 = 2 - 1 = (2 - 1)(2 + 2 + 2 + \ldots + 2 + 1) \]

with both factors > 1. Thus \( M_N \) is not prime. \( \square \)
Example: \[ 2^5 - 1 = 31 \text{ is prime} \]
\[ 2^7 - 1 = 127 \text{ is prime} \]
\[ 2^{11} - 1 = 2047 = 23 \cdot 89 \text{ not prime} \]

There is a 1-1 correspondence between \textit{Mersenne primes} and \textit{even perfect numbers}.

**THEorem:** \textit{Let } \( N \in \mathbb{N} \), \textit{then } \( N \) \textit{is an even perfect number if and only if } \( N = 2^p (2^p - 1) \) \textit{where } \( 2^p - 1 \) \textit{is a prime.}

**Proof:** \( \iff \) \textit{Let } \( 2^p - 1 \) \textit{be a prime } \( \Rightarrow \) \textit{ } \( 2^p \) \textit{is a prime}

By previous Theorem

Write \( N = 2^p (2^p - 1) \) which is even. Compute

\[
\sigma(N) = \sigma(2^p (2^p - 1)) = \sigma(2^p) \sigma(2^p - 1) = \sigma(2^p) \cdot \sigma(2^p - 1)
\]

\[ \sigma \text{ is multiplicative} \]

\[ (2^p - 1, 2^p - 1) = 1 \]

\[
= \left( \frac{2^p - 1}{2 - 1} \right) \cdot 2^p = \left( \frac{2^p - 1}{2^p - 1} \cdot 2^p \right) = 2^p \]

Because \( 2^p - 1 \) is prime we have

\[ \sigma(2^p - 1) = 2^p + 1 = 2^p \]

(Or apply the formula)

\[
N = 2^p - 1
\]
Let $N$ be an even perfect number.

Write $N = 2^a \cdot b^c$, $a, b, c \in \mathbb{Z}_{>0}$, $b$ odd, $a \geq 1$.

We have

$$\sigma(N) = \sigma(2^a) \cdot \sigma(b^c) = \left( \frac{2^{a+1} - 1}{2 - 1} \right) \sigma(b) = \left( \frac{2^{a+1} - 1}{2 - 1} \right) \sigma(b)$$

by multiplicative formula.

Since $N$ is perfect, $\sigma(N) = 2N = 2 \cdot (2^a \cdot b) = 2^{a+1} \cdot b$.

$$\Rightarrow \left( 2^{a+1} - 1 \right) \sigma(b) = 2^{a+1} \cdot b \quad (\star)$$

$$\Rightarrow 2^{a+1} \mid \sigma(b) \iff \sigma(b) = 2^{a+1} \cdot c \quad (\star \star)$$

Replacing in $(\star)$ gives

$$\left( 2^{a+1} - 1 \right) 2^a \cdot c = 2^{a+1} \cdot b$$

$$\Rightarrow \left( 2^{a+1} - 1 \right) c = b \quad (\Delta).$$

CLAIM: $c = 1$ then $b = 2^{a+1} - 1$ and $(\star \star)$ gives

$$\sigma(b) = 2^{a+1} = b + 1 \Rightarrow b \text{ is prime.}$$

Therefore, $N = 2^a \cdot b = 2^a \left( 2^{a+1} - 1 \right)$ with $2^{a+1} - 1$ is prime, as desired.

We now prove the claim.

Suppose $c > 1$. From $(\Delta)$ we see that $b$ has at least the positive divisors $1, c, b^c$.

Thus $\sigma(b) > 1 + b + c$, but from $(\star \star)$

$$\sigma(b) = 2^a \cdot c = \left( \frac{2^{a+1} - 1}{2 - 1} \right) c + c = b + c,$$ a contradiction.
THEM: Let $p$ be a prime.

THEN any divisor of $M_p = 2^p - 1$ is of the form $2p^i k + 1$

PROOF: Since the product of two numbers $9_1 9_2 \equiv 1 \pmod{2p}$
is $9_1 9_2 \equiv 1 \pmod{2p}$ it is enough to prove the theorem forprime divisors.

Let $q \mid M_p$ be prime. By FLT we have
\[ 2^{q-1} \equiv 1 \pmod{q} \Rightarrow q \mid 2^{q-1} - 1 \]
\[ \Rightarrow q \mid (2^{p-1}, 2^{q-1}) = 2^{(p, q-1)} - 1 \neq 1 \]

CLAIM (x): $(N^{p-1}, N^{q-1}) = N^{(p, q-1)} - 1$ (Lemma 4.3 in the book)
\[ \Rightarrow (p, q-1) 
eq 1 \Rightarrow p \mid q-1 \text{ since } p \text{ is prime} \]
\[ \Rightarrow q-1 = p \cdot k' \text{ with } k' = 2k \text{ since } q \text{ is odd (} M_p \text{ is odd)} \]
\[ \Rightarrow q = 1 + 2kp \]

EX: Is $M_{23} = 2^{23} - 1 = 8388607$ a prime?

By the theorem we only need to test divisibility by primes of the form $q = 46k + 1$.

The smallest is 47 and dividing $M_{23}$ by it gives $M_{23} = 47 \times 178481$. 