7.2:

Def: The sum of divisors function, denoted $\sigma(n)$, is defined by $\sigma(n) = \sum d$, for $n \in \mathbb{Z}^+$. This is an Arithmetic function.

Eg: $\sigma(15) = 1 + 5 = 6$.

In general, $\sigma(p) = 1 + p$.

Def: The number of divisors function, denoted $\tau(n)$, is defined by $\tau(n) = \text{number of positive divisors of } n$, $n \in \mathbb{Z}^+$.

Eg: $\tau(5) = 2$, in general $\tau(p) = 2$ for $p$ a prime.

$\tau(n) = \sum_{d|n} 1$

Eg: $n = 12$: $\sigma(12) = \sum_{d|12} d = 1 + 2 + 3 + 4 + 6 + 12 = 28$

$\tau(12) = \sum_{d|12} 1 = 6$

Theorem: If $f$ is a multiplicative function, then the summary function of $F$, denoted $\mathbb{F}$, given by $\mathbb{F}(n) = \sum_{d|n} f(d)$ is also multiplicative.
Proof. Need to show that $F(mn) = F(m) \cdot F(n)$, for $m, n \in \mathbb{Z}^+$ such that $(m, n) = 1$.

$$F(m \cdot n) = \sum_{d \mid mn} f(d) \cdot \text{Since } d \mid mn, \text{ we have } d = d_1d_2, \text{ where } d_1 \mid m \text{ and } d_2 \mid n.$$ 

Hence $F(mn) = \sum_{d \mid mn} f(d) = \sum_{d_1 \mid m} f(d_1)f(d_2), \text{ since } f\text{ is multiplicative and } (d_1, d_2) = 1$ because $(m, n) = 1$.

$$\sum_{d_1 \mid m} f(d_1)f(d_2) = \sum_{d_1 \mid m} \sum_{d_2 \mid n} f(d_1)$$

$$= F(m) \cdot F(n). \quad \square$$

Example: $n = 15, \quad 15 = 5 \times 3$.

$$F(15) = f(1) + f(3) + f(5) + f(15)$$

$$= f(1,1) + f(3,1) + f(5,1) + f(15,1)$$

$$= f(1) \cdot f(1) + f(3) \cdot f(1) + f(5) \cdot f(1) + f(15) \cdot f(1)$$

$$= (f(1) + f(5)) \cdot (f(1) + f(3))$$

$$= F(5) \cdot F(3).$$
Corollary: The functions \( \sigma \) and \( \varphi \) are multiplicative.

Let \( f(n) = n \) and \( g(n) = 1 \). Clearly \( f \) and \( g \) are arithmetic and multiplicative.

Note that \( \sigma(n) = \sum_{d|n} d = \sum_{d|n} f(d) \) and

\[
\tau(n) = \sum_{d|n} 1 = \sum_{d|n} g(d).
\]

Thus \( \sigma \) is the sum function of \( f \) and \( \tau \) is the sum function of \( g \), hence \( \sigma \) and \( \tau \) are multiplicative.

\[\text{Lemma: Let } p \text{ be a prime and } a \in \mathbb{Z}^+. \text{ Then}\]

\[\sigma(p^a) = 1 + p + p^2 + \ldots + p^a = \frac{p^{a+1} - 1}{p-1} \]

\[\tau(p^a) = a + 1.\]

Proof: The divisors of \( p^a \) are \( 1, p, p^2, \ldots, p^{a-1}, p^a \).

Hence \( \tau(p^a) = a + 1 \). Also \( \sigma(p^a) = 1 + p + p^2 + \ldots + p^a \)

\[= \frac{p^{a+1} - 1}{p-1} \]

\[\text{Example: } p = 7, \ a = 3, \ \sigma(7^3) = \frac{7^4 - 1}{7-1} = 912 \]

\[\tau(7^3) = 4.\]
\[ \sigma(n), \ n = 10! \]

Note that a prime \( p \mid 10! \iff p < 10, \)

so \( p = 2, 3, 5, 7. \)

\[ 10! = 2^8 \cdot 3^4 \cdot 5^2 \cdot 7 \]

\[ \sigma(10!) = \sigma(2^8) \cdot \sigma(3^4) \cdot \sigma(5^2) \cdot \sigma(7) \]

\[ = \left( \frac{2^{9-1}}{2-1} \right) \left( \frac{3^{5-1}}{3-1} \right) \left( \frac{5^{3-1}}{5-1} \right) \left( \frac{7^{2-1}}{7-1} \right) \]

\[ = 511 \times 242 \times \frac{124}{4} \times \frac{48}{6} \]

---

\[ \text{Q: For which positive integers } n \text{ is the sum of divisors odd?} \]

\[ \text{A: Let } n \in \mathbb{Z}^+, \ n = p_1^{d_1} p_2^{d_2} \ldots p_s^{d_s}, \ \text{p_i's primes.} \]

\[ \text{Need to find } n \text{ for which } \tau(n) \text{ is odd. Have} \]

\[ \tau(n) = \tau(p_1^{d_1}) \cdot \tau(p_2^{d_2}) \ldots \tau(p_s^{d_s}) \]

\[ = (d_1 + 1)(d_2 + 1) \ldots (d_s + 1). \]

For \( \tau(n) \) to be odd, each factor \((d_i + 1)\) must be odd, hence \( d_i \)'s must be even. Hence \( n \) has to be a square, i.e. a perfect square, with \( d_i = 2b_i \)

\[ 2^{b_1} b_1 \, 2^{b_2} b_2 \, \ldots \, 2^{b_s} b_s \]
Q: For which positive integers \( n \) is the sum of divisors odd?

A. Let \( n \in \mathbb{Z}^+ \), \( n = p_1^{d_1} p_2^{d_2} \cdots p_k^{d_k} \), \( p_i \)'s prime.

We know \( \sigma(n) = \sigma(p_1^{d_1}) \sigma(p_2^{d_2}) \cdots \sigma(p_k^{d_k}) \).

Want \( \sigma(n) = \text{odd} \)

\[ \sigma(n) = (1+p_1+p_1^2+\ldots+p_1^{d_1}) (1+p_2+p_2^2+\ldots+p_k^{d_k}) \]

For \( \sigma(n) \) to be odd, each factor in the product should be odd. Consider any factor, say for \( p_1 \). Then

\[ (1+p_1+p_1^2+\ldots+p_1^{d_1}) \] has \( d_1+1 \) terms in the sum.

Each power of \( p_1 \) is odd if \( p_1 \) is odd. Hence for

\[ (1+p_1+p_1^2+\ldots+p_1^{d_1}) \] to be odd, \( d_1 \) must be even.

If \( p_1 \) is even, then \( p_1 = 2 \), and we have

\[ (1+2+2^2+\ldots+2^{d_1}) \] which is always an odd number.

Hence we see that \( n = 2^t t \), where \( (2, t) = 1 \) and \( t \) is a perfect square since for odd primes \( p_i \) in the prime factorization,

the exponent \( d_j \) must be even.
3.3 Perfect Numbers and Mersenne Primes

**Definition:** A positive integer \( n \) such that \( \sigma(n) = 2n \) is called a perfect number.

For example, \( n = 6, \quad \sigma(6) = 1 + 2 + 3 + 6 = 12 \).

**Theorem:** A positive integer \( n \) is perfect if and only if \( n = 2^{k-1}(2^k - 1) \) for \( k \in \mathbb{Z}^+, \ k \geq 2 \) and such that \( 2^k - 1 \) is prime.

**Proof:** Let \( n \) be an even perfect number. Writing \( n = 2^n \cdot t, \ s, t \in \mathbb{Z}^+, \ t \) odd. Then

\[ \sigma(n) = \sigma(2^n) \cdot \sigma(t) = (2^{n+1} - 1) \cdot \sigma(t) = 2^{n+1} \cdot t \]

Note \( (2^{n+1}, 2^{n+1} - 1) = 1 \). Hence (*) implies

\[ 2^{n+1} \mid \sigma(t), \text{ so } 2^{n+1} \cdot q = \sigma(t) \]

Hence \( \sigma(n) = (2^{n+1} - 1) \cdot 2^t \cdot q = 2^{n+1} \cdot t \)

\[ \Rightarrow (2^{n+1} - 1) \cdot q = t \quad (**) \]

\[ \Rightarrow q \mid t \text{ and } q \neq t. \]

Add \( q \) to both sides of (**) to get

\[ t + q = 2^{n+1} \cdot q - q + q = 2^{n+1} \cdot q = \sigma(t) \]

Let us show that \( q = 1 \).
If \( q \neq 1 \), then there are at least three distinct positive divisors of \( t \), namely 1, 1, and \( t \).

Hence \( \sigma(t) \geq t + q + 1 \) \( \Rightarrow \sigma(t) - t = q + 1 \).

Hence \( q = 1 \) and we have \( t = 2^{s+1} - 1 \) and \( \sigma(t) = t + 1 \). This forces \( t \) to be a prime.

Hence \( N = 2^b (2^{s+1} - 1) \) (\( k = s+1 \) in the theorem).

\[ \Leftarrow \text{ Let } N = 2^k (2^b - 1), \quad \text{for } k \geq 2 \text{ and } (2^b - 1) \text{ is a prime.} \]

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

\[ = \left( 2^{k+1} - 1 \right) \cdot 2^k - 2^b - 1 + 1 \]

\[ = 2^k (2^b - 1) = 2N \]

\( \Rightarrow \) \( N \) is perfect.

Consequence: To find even perfect numbers, we must find primes that are of the form \( 2^m - 1 \).

Theorem: If \( m \) is a positive integer and \( 2^m - 1 \) is a prime, then \( m \) is a prime.
Find all positive integers \( n \) such that \( \phi(n) = 6 \).

**Proof:** Suppose \( m \) is not a prime and \( 2^m - 1 \) is a prime. Let \( m = ab \), \( 1 < a < m, 1 < b < m \).

As \( 2^m - 1 \) is prime, we must have \( m > 1 \).

We have

\[
(2^m - 1) = (2^a - 1)(2 + 2^a + \ldots + 2^{a-1})
\]

Both the factors on the right are \( > 1 \). Hence \( (2^m - 1) \) is composite if \( m \) is not prime.

\( \Rightarrow \) Thus for \( (2^m - 1) \) to be a prime, \( m \) has to be prime.

**Definition:** If \( m \) is a positive integer, then \( M_m = 2^m - 1 \) is called the \( M \) - Mersenne number.

If \( p \) is a prime and \( M_p = 2^p - 1 \) is also prime, then \( M_p \) is called a Mersenne prime.

\( \Rightarrow \) \( M_7 = 2^7 - 1 = 127 \) (prime); \( M_5 = 2^5 - 1 = 31 \) (prime);

\( M_{11} = 2^{11} - 1 = 2047 = 23 \times 89 \), \( M_{23} = 2^{23} - 1 = 47 \times 17 \times 8 \times 487 \).
Theorem: If $p$ is an odd prime, then any divisor of the Mersenne number $M_p = 2^p - 1$ is of the form $2kp + 1$ for $k \in \mathbb{Z}^+$. 

Proof: Let $q$ be a prime such that $q \mid M_p = 2^p - 1$. Since $q$ is odd, by FLT, $2^{q-1} \equiv 1 \pmod{q} \Rightarrow a^q - 1$. Also, know that $(2^p, 2^q - 1) = (p, q - 1) = 2^p$. Hence $p \mid q - 1 \Rightarrow q - 1 = mp$. Since $q - 1 \mid p$. Hence $p \mid q - 1 \Rightarrow q - 1 = mp$. As $q$ is odd, $(q - 1)$ is even, hence $m$ is even as $p$ is odd. Therefore, $m = 2k$, $k \in \mathbb{Z}^+$ 

$\Rightarrow q = mp + 1 \Rightarrow q = 2kp + 1$.

Any divisor of $M_p$ is a product of prime divisors of $M_p$, and each prime divisor is of the form $2kp + 1$. Hence the product $M_p$ is also of this form.

Example: $M_{13} = 2^{13} - 1 = 8191$, $\sqrt{8191} \approx 90.5$. Any prime divisor of $M_{13}$ has to be of the form $26k + 1$. Possible candidates are 53, 79 but $53$ do not divide $M_{12} \Rightarrow M_{12}$ is a prime.
We have special tests for Mersenne numbers to decide whether a Mersenne number is a prime. Using these, it has been possible to determine whether extremely large Mersenne numbers are prime.
There are special primality tests for Mersenne numbers, using which it has been possible to determine whether extremely large Mersenne numbers are primes.

**Example: Lucas-Lehmer Test**

**Theorem:** Let \( p \) be a prime and let \( M_p = 2^p - 1 \) denote the \( p \)th Mersenne number. Define a sequence of integers recursively by \( \gamma_1 = 4 \), and for \( k \geq 2 \)

\[
\gamma_k = \gamma_{k-1}^2 - 2 \mod M_p, \quad 0 \leq \gamma_k < M_p.
\]

Then \( M_p \) is prime \( \iff \gamma_{p-2} \equiv 0 \mod M_p \).

**Example:** \( M_5 = 31 \).

\[
\begin{align*}
\gamma_1 &= 4, \quad \gamma_2 = 4^2 - 2 \equiv 14 \mod 31, \\
\gamma_3 &= 14^2 - 2 \equiv 8 \mod 31, \\
\gamma_4 &= 8^2 - 2 \equiv 62 \mod 31, \\
\gamma_5 &= 62, \quad 62 \equiv 0 \mod 31.
\end{align*}
\]

Hence \( M_5 \) is a prime.

**Remark:** Let \( p \) be a prime and \( M_p \) the \( p \)th Mersenne number. It is possible to determine whether \( M_p \) is prime in \( \leq C p^3 \) bit operations.

(Largest prime: \( M_{7,420,912} \) has 23,249,425 digits.)
(2020) $82,589,933$
$2^7 - 1$ $24,862,048$ digits.

**Question:** Are there odd perfect numbers?

**Answer:** Unknown!

**Ex:** Find all positive solutions to the equation

$$\phi(n) = 12.$$ 

Let $n = p_1^{t_1} p_2^{t_2} \cdots p_k^{t_k}$

$$\phi(n) = p_1^{t_1-1}(p_1-1) \cdot p_2^{t_2-1}(p_2-1) \cdots p_k^{t_k-1}(p_k-1)$$

$11^2$

$12$

$2^1$

$2 \times 3$

The only primes $p_i$ in $n$ must be such that

$(p_i - 1) | 112$. So note that the only primes

possible dividing $n$ are $2, 3, 5, 7$.

$$n = 2^a \cdot 3^b \cdot 5^c \cdot 7^d \quad 0 \leq a, b, c, d.$$ 

$$12 = \phi(n) = 2(1) 	imes 3(2) \cdot 5(4) \cdot 7(6)$$

**Case 1:** Assume $d = 1$; then $c = 0$, and following possibilities:

- $a = 1$ and $b = 1 \implies n = 28, 42, 21.$
- $a = 0$ and $b = 1 \implies 42, 14, 42.$
Cryptosystem \rightarrow \mathcal{K} \rightarrow \text{key space}
\xrightarrow{f} \mathcal{C} \rightarrow \text{finite set of possible ciphertext messages.}

For each \( k \in \mathcal{K} \), there is an encryption function \( E_k \) and a decryption function corresponding to \( E_k \), say \( D_k \) s.t. \( D_k E_k(x) = x \) for every plain text message \( x \).

\underline{Caesar Cipher:}

\[
\begin{array}{cccccccc}
A & B & C & D & E & F & G \\
0 & 1 & 2 & 3 & 4 & 5 & 6 \\
C & 3 & 4 & 5 & 6 & 7 & 8 & 9
\end{array}
\]

Based on modular arithmetic:

\( P = \text{plain text} \); \( C = \text{cipher text} \).

Transformation: \( C = P + 3 \pmod{26} \)

Procedure: Start with the plain text; group it into groups of 5 letters, apply the transformation, write the corresponding cipher text.

Note: \( P = C - 3 \pmod{26} \)
Case 2: Assume \( c = 1 \): Conclude that \( 5 \times n \).

Case 3: Assume \( d = 0, b = 2 \).
Only possibility lead is \( n = 2^2 \times 3^2 = 36 \).
\( a = 2 \).

Case 4: Assume \( d = 0, b = 1 \).
Conclude this case cannot occur.

Case 5: Assume \( d = 0, b = 0 \); Conclude \( n = 2^a \).
\[ \Rightarrow \quad 12 = 2^{a-1} \quad \Rightarrow \quad \leq . \]

Check: \( n = 2^8, 42, 21, 36 \) all have \( \phi(n) = 2 \).

8.1 CRYPTOLOGY : Study devoted to secrecy systems.

CRYPTOGRAPHY : Designing and implementing secrecy systems.

Cryptanalysis : Breaking secrecy systems.

\[ P = \text{Plain text} \quad \xrightarrow{\text{transformation}} \quad C = \text{Cipher text} \]

\[ \begin{align*}
\text{(Encryption)} & \quad C \\
\text{(Decipher)} & \quad \text{(Decipher)} \\
P & \quad \text{(Decipher)} \\
\end{align*} \quad \text{key: A particular step in the transformation} \]
Example: GOOD MORNING
6:14 14 3 12 14 17 13 8 13 6
15 20 16 11 16 9
3 key
J R R G P R U Q L Q J 26
Cipher Text: JRRGP RUQLQJ
GOOD MORNING

Decryption: L F D P H L V D Z L F R Q I X H U H G
15 3 15 7 11 21 3 25 11 5 17 16 19 23 7 20 7 6
C - 3 (26)
8 2 0 12 4 8 18 0 22 8 2 14 13 16 20 4 17 4 3
Plain text: I CAME ISAW I CONQUERED