Last time:

Thm: If \( m, n \) are positive integers, \((m, n) = 1\), and \( d \mid mn\), then \( \exists \) unique pos intger \( d_1, d_2 \) so that \( d = d_1 d_2 \), \( d_1 \mid m \) and \( d_2 \mid n \). Conversely, if \( d_1 \mid m, d_2 \mid n\), then \( d_1 d_2 \mid mn \).

Ex: \( m = 2 \cdot 17, \ n = 3^2 \)

Divisors of \( m \): 1, 2, 17, 2 \cdot 17

Divisors of \( n \): 1, 3, 3^2

Exactly the divisors of \( m \cdot n = 2 \cdot 17 \cdot 3^2 \)

Last time: we defined a notion of multiplicative funcns

\( f: \mathbb{Z}_{>0} \rightarrow \mathbb{C} \) is multiplicative if \( f(mn) = f(m) f(n) \)

whenever \( m, n \) are relatively prime.

Notation: If \( f: \mathbb{Z}_{>0} \rightarrow \mathbb{C} \) is a function.
**Notation:** If \( f : \mathbb{Z}_{>0} \to \mathbb{C} \) is a function, 
\[
\sum_{d | n} f(d) : \text{denotes the sum of } f(d) \text{ over all positive divisors of } n.
\]

**Ex:** \[
\sum_{d | n} f(d) = f(1) + f(2) + f(5) + f(10)
\]

**Thm:** If \( f \) is a multiplicative function, and 
\( g : \mathbb{Z}_{>0} \to \mathbb{C} \) defined by 
\[
g(n) = \sum_{d | n} f(d), \text{ then } g \text{ is multiplicative.}
\]

**Corollary:**

a) \( d(n) := \# \text{ of pos. int. divisors of } n \) is multiplicative

b) \( \sigma(n) := \sum \text{ of pos. int. divisors of } n \) is multiplicative.

**Pf of Cor:**

a) \( d(n) = \sum_{d | n} 1 \) and \( f(n) = 1 \) is multiplicative

b) \( \sigma(n) = \sum_{d | n} d \) and \( f(d) = d \) is multiplicative.

**Pf of Thm:** Suppose \( n, m \geq 0, \ (n,m) = 1 \). Want to prove: 
\[
g(m) g(n) = g(mn).
\]

Have: 
\[
g(m) g(n) = \left( \sum_{d | m} f(d) \right) \left( \sum_{d | n} f(d) \right)
\]
\[ = \sum_{d_1 \mid n, d_2 \mid n} f(d_1) f(d_2) \]

\[ \cdot d_1 \mid m, d_2 \mid n \text{ and } (n,m) = 1 \implies (d_1,d_2) = 1 \]

\[ \implies f(d_1) f(d_2) = f(d_1 d_2) \quad \text{b/c } f \text{ is multiplicative by assumption.} \]

\[ \implies g(m)g(n) = \sum_{d_1 \mid \text{lcm}(d_1,d_2)} f(d_1 d_2) \]

By previous theorem,

\[ = \sum_{d \mid mn} f(d) = g(mn) \]

So \( g(m)g(n) = g(mn) \) when \( (m,n) = 1 \).

Aside \( m = 3 \quad n = 3 \)

<table>
<thead>
<tr>
<th></th>
<th>1</th>
<th>2</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>9</td>
</tr>
</tbody>
</table>

\[ \text{Then Suppose } n = p_1^{a_1} \cdots p_k^{a_k}. \text{ Then} \]

\[ d(n) = (a_1+1)(a_2+1) \cdots (a_k+1) \]

\[ \sigma(n) = \frac{p_1^{a_1+1} - 1}{p_1 - 1} \cdots \frac{p_k^{a_k+1} - 1}{p_k - 1} \]
\[ \sigma(n) = \frac{p_1^{\alpha_1} - 1}{p_1 - 1} \cdot \ldots \cdot \frac{p_k^{\alpha_k} - 1}{p_k - 1} \]

\textbf{Pf:} Because \( d \) is multiplicative,

\[ d(n) = d(p_1^{\alpha_1}) \ldots d(p_k^{\alpha_k}) \]

\[ d(p^a) \] : The divisors of \( p^a \) are \( \{1, p, p^2, \ldots, p^a\} \]

\[ = 1, a + 1 \text{ terms} \]

\[ = (a_1 + 1)(a_2 + 1) \ldots (a_k + 1) \]

\[ \sigma(n) = \sigma(p_1^{\alpha_1}) \ldots \sigma(p_k^{\alpha_k}) \]

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

\[ \sigma(n) = \frac{p_1^{\alpha_1} - 1}{p_1 - 1} \cdot \ldots \cdot \frac{p_k^{\alpha_k} - 1}{p_k - 1} \]

\[ \text{Ex: } d(36) = d(2^2 \cdot 3^2) = (1+2)(1+2) = 9 \]

\[ \sigma(36) = \sigma(2^2) \sigma(3^2) = (1+2+4)(1+3+9) \]

\[ = 7 \cdot 13 = 91 \]

\[ \text{Defn: } \text{A positive integer } n \text{ is } \underline{\text{perfect}} \text{ if } \]

\[ \sum d = n. \text{ In other words, } n \text{ is } \underline{\text{perfect}} \]
\[ \sum d = n. \quad \text{In other words, } n \text{ is perfect if } \sigma(n) = 2n. \]

\[ \sum_{d \mid n} (Aside: \sigma(n) > n, \quad \sigma(n) - n = \tau(n) \text{ if } n \text{ is perfect}) \]

Ex: 6 is perfect \(6 = 1 + 2 + 3\)

28 is perfect \(\sigma(28) = \sigma(4) \sigma(7) = (1 + 2 + 4)(1 + 7)\)
\[ = 7 \cdot 8 = 56 = 2 \cdot 28. \]

Conjecture: Every perfect number is even.

Know: There are no odd perfect numbers < 10,000.

In fact, If \(p\) is prime and \(2^{p-1} - 1\) is also prime, then \(n = 2^{p-1} (2^p - 1)\) is perfect.

Ex: \(p = 2, \quad 2^1 - 1 = 3\) is also prime
\[ n = 2^{2-1} \cdot 3 = 6 \text{ is perfect} \]

\(p = 3, \quad 2^2 - 1 = 3\) is also prime
\[ n = 2 \cdot (2^3 - 1) = 4 \cdot 7 = 28 \text{ is perfect} \]

A Mersenne prime is a prime of the form \(2^p - 1\) with \(p\) a prime.

Euler: If \(n\) is even and perfect then \(n = 2^{p-1} (2^p - 1)\) with \(p\) prime and \(2^p - 1\) prime.
Linear Diophantine Equations

**Aim:** Find all $x, y$ integers so that

$$ax + by = c$$

where $a, b, c$ are fixed integers.

**Ex:** Find all integer solutions to $14x + 22y = 10$

**Thm:** Suppose $a, b \neq 0$ integers and $d = (a, b)$. If $d \nmid c$, then the eqn $ax + by = c$ has no integral solutions.

If $d \mid c$, then the eqn has infinitely many solutions.

If $x_0, y_0$ is one integral solution, then all solutions are given by

$$x = x_0 + \frac{b}{d} t, \quad t \in \mathbb{Z}$$

$$y = y_0 - \frac{a}{d} t$$