# Lecture 11.1

Last time:

- $n = x^2 + y^2$ if and only $n$ is of the form $n = d^2 p_1 \cdots p_r$ for distinct primes $p_i = 2$ or $p_i \equiv 1 \pmod 4$.

- $c$ is the hypotenuse in a primitive Pythagorean triple $(a,b,c)$ if and only if $c$ is a product of primes $p \equiv 1 \pmod 4$.

---

## Sums of Divisors

**Def** The divisor sum function $\sigma$ is

$$\sigma(n) = \sum_{d \mid n} d.$$

**Ex**

$\sigma(1) = 1$

$\sigma(2) = 1 + 2 = 3$

$\sigma(3) = 1 + 3 = 4$

$\sigma(4) = 1 + 2 + 4 = 7$

$\sigma(5) = 1 + 5 = 6$

$\sigma(6) = 1 + 2 + 3 + 6 = 12$

$\sigma(7) = 1 + 7 = 8$

$\sigma(8) = 1 + 2 + 4 + 8 = 15$

$$\sigma(9) = 1 + 3 + 9 = 13$$

Do you observe any patterns?

$\boxed{\text{Lemma}}$ If $p$ is prime, $\sigma(p) = p + 1$.

Pf: The only divisors of $p$ are $1$ and $p$. $\square$

$\boxed{\text{Theorem}}$ Let $\sigma$ be the divisor sum function.

(a) For any prime $p$ and $k \in \mathbb{N}$,

$$\sigma(p^k) = 1 + p + \ldots + p^k = \frac{p^{k+1} - 1}{p - 1}.$$

(b) If $\gcd(a,b)=1$, then

$$\sigma(ab)=\sigma(a)\sigma(b).$$

Exercise 1: Prove the Theorem!

These properties look just like the properties for $\phi(n)$ we proved earlier.

The relation between these functions goes even deeper...

Q: What happens when we apply $\phi(n)$

to the individual terms in

$$\sigma(n) = d_1 + d_2 + \dots + d_r \ ?$$

$\boxed{\text{Ex}}$ $\sigma(2) = 1 + 2 = 3$

vs. $\phi(1) + \phi(2) = 1 + 1 = 2$

$\sigma(3) = 1 + 3 = 4$

vs. $\phi(1) + \phi(3) = 1 + 2 = 3$

$\phi(4) = 1 + 2 + 4$ (we don't need the sum)

vs. $\phi(1) + \phi(2) + \phi(4) = 1 + 1 + 2 = 4$

$\phi(5) = 1 + 5$

vs. $\phi(1) + \phi(5)$

vs. $\phi(1) + \phi(5) = 1 + 4 = 5$

$$\phi(6) = 1 + 2 + 3 + 6$$

vs. $\phi(1) + \phi(2) + \phi(3) + \phi(6) = 6$

It appears that $\sum_{d \mid n} \phi(d) = n$. Why?

Define a new function $F(n)$ by

$$F(n) = \sum_{d \mid n} \phi(d).$$

**Lemma** For $p$ prime, $k \geq 1$,

$$F(p^k) = p^k.$$

Pf: We have $\sigma(p^k) = \sum_{j=0}^{k} p^j$ and

for each $j$,

$$\phi(p^j) = p^{j-1}(p-1) = p^j - p^{j-1}.$$

Then

$$F(p^k) = \sum_{d \mid p^k} \phi(d) = \sum_{j=0}^{k} \phi(p^j)$$

$$= \sum_{j=0}^{k} (p^j - p^{j-1})$$

$$= 1 + (p-1) + (p^2-p) + \dots + (p^k - p^{k-1})$$

$$= p^k. \quad \square$$

$\boxed{\text{Lemma}}$ If $\gcd(a,b) = 1$, $F(ab) = F(a)F(b)$.

Pf: Write $\sigma(a) = d_1 + \dots + d_r$

and $\sigma(b) = e_1 + \dots + e_s$.

Since $\gcd(a,b) = 1$, each pair $d_i, e_j$ is relatively prime, which means the divisors of $ab$ are all the $d_i e_j$.

Then
$$F(ab) = \sum_{d \mid ab} \phi(d)$$

$$= \sum_{\substack{1 \leq i \leq r \\ 1 \leq j \leq s}} \phi(d_i e_j)$$

$$= \sum_{\substack{1 \leq i \leq r \\ 1 \leq j \leq s}} \phi(d_i)\,\phi(e_j)$$

while on the other hand,

$$F(a)F(b) = \left(\sum_{i=1}^{r} \phi(d_i)\right)\left(\sum_{j=1}^{s} \phi(e_j)\right)$$

$$= \sum_{i,j} \phi(d_i)\,\phi(e_j)$$

by extended FOIL. □

$\boxed{\text{Def}}$ An arithmetic function is a function $f : \mathbb{N} \longrightarrow \mathbb{C}$, that is, an assignment of a complex number $f(n)$ to each $n \in \mathbb{N}$. An arithmetic

$f(n)$ to each $n \in \mathbb{N}$. An arithmetic

function $f$ is **(weakly) multiplicative**

if for any relatively prime $a, b \in \mathbb{N}$,

$f(ab) = f(a)f(b)$.

**Ex** We already knew $\phi(n)$ is a multiplicative function.

**Ex** We just proved $\sigma(n)$ and

$$F(n) = \sum_{d \mid n} \phi(n)$$

are multiplicative functions.

Remark: If $f$ is multiplicative, then the values of $f$ are completely determined by $f(p^k)$ for all primes $p$ and powers $k$.

$\boxed{\text{Ex}}$

$$F(100) = F(2^2 \cdot 5^2)$$
$$= F(2^2)F(5^2)$$
$$= 2^2 \cdot 5^2 = 100.$$

In fact, there was nothing special about $n = 100$ here.

$\boxed{\text{Theorem}}$ For any $n \in \mathbb{N}$, $F(n) = n$.

That is, $\displaystyle\sum_{d \mid n} \phi(d) = n$.

Exercise 2: Prove the Theorem!

Remark: For an odd prime $p$, the quadratic residue symbol $\left(\frac{n}{p}\right)$ appears to behave like a multiplicative function:

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$$

for <u>any</u> $a, b$, as long as they're both relatively prime to $p$.

If we extend the definition of $\left(\frac{\cdot}{p}\right)$ by

old version

$$\left(\frac{n}{p}\right) = \begin{cases} \left(\frac{n}{p}\right), & \gcd(n,p) = 1 \\ 0, & \gcd(n,p) > 1 \end{cases}$$

then this new $\left(\frac{\cdot}{p}\right)$ is a multiplicative function.

---

## Primitive Roots

Recall that the order of $a$ mod $n$

is the smallest $k \geq 1$ such that

$$a^k \equiv 1 \pmod{n}.$$

By a homework problem, if $k$ is the order of $a$ mod $n$, then $k \mid \phi(n)$.

When $n = p$ is prime, this means that $k \mid (p-1)$.

$\boxed{\text{Def}}$ A **primitive root** mod $p$ is an integer $a$ whose order mod $p$ is $p-1$.

Q: Do primitive roots always exist? And if so, how many are there?

Here's a table of orders mod $p$ for $p = 5, 7$ and $11$.

| $p=5$ |
|---|
| $1^1 \equiv 1 \pmod{5}$ |
| $2^4 \equiv 1 \pmod{5}$ |
| $3^4 \equiv 1 \pmod{5}$ |
| $4^2 \equiv 1 \pmod{5}$ |

| $p=7$ |
|---|
| $1^1 \equiv 1 \pmod{7}$ |
| $2^3 \equiv 1 \pmod{7}$ |
| $3^6 \equiv 1 \pmod{7}$ |
| $4^3 \equiv 1 \pmod{7}$ |
| $5^6 \equiv 1 \pmod{7}$ |
| $6^2 \equiv 1 \pmod{7}$ |

| $p=11$ |
|---|
| $1^1 \equiv 1 \pmod{11}$ |
| $2^{10} \equiv 1 \pmod{11}$ |
| $3^5 \equiv 1 \pmod{11}$ |
| $4^5 \equiv 1 \pmod{11}$ |
| $5^5 \equiv 1 \pmod{11}$ |
| $6^{10} \equiv 1 \pmod{11}$ |
| $7^{10} \equiv 1 \pmod{11}$ |
| $8^{10} \equiv 1 \pmod{11}$ |
| $9^5 \equiv 1 \pmod{11}$ |
| $10^2 \equiv 1 \pmod{11}$ |

2 and 3 are primitive

3 and 5 are primitive

2, 6, 7 and 8 are all prim.

roots roots roots

Here's some more data:

| $p$ | # primitive roots mod $p$ |
| --- | --- |
| 5 | 2 |
| 7 | 2 |
| 11 | 4 |
| 13 | 4 |
| 17 | 8 |
| 19 | 6 |
| 23 | 10 |
| 29 | 12 |
| 31 | 8 |
| 37 | 12 |

Next time: the pattern.