6.1) Wilson's + Converse of Wilson's 6.1 6.2

p is prime iff $(p-1)! \equiv -1 \mod p$

Fermat's Little theorem 6.3

sps p is prime and gcd $(a, p) = 1$

then $a^{p-1} \equiv 1 \mod p$

$a^p \equiv a \mod p$ 6.4

a^{p-2} is inverse of a mod p 6.5

ex $2^9 \equiv 512 \equiv 6 \mod 11$ is inverse of 2

since $2x \equiv 1 \mod 11$

$2^9 \cdot 2x \equiv 2^9 \mod 11$

$2^{10} \equiv 1$

6.2) FLIT tells us if n is prime and b is any integer, then $b^n \equiv b \bmod n$

So, $b^n \not\equiv b \bmod n$ then n is composite.

ex: $2^{63} \equiv 2^{66} \cdot 2^3 \equiv 8 \not\equiv 2 \bmod 63$

$\Rightarrow$ 63 is not prime.

Definition: $b > 0$, n is composite.

$b^{n-1} \equiv 1 \bmod n$ then n is Fermat Pseudoprime to the base b

Def: n is composite.

n is an absolute FP or Carmichael Prime if $\forall b$ w/ $\gcd(b, m) = 1$, $b^{m-1} \equiv 1 \bmod m$

Theorem: sps $m = p_1 p_2 \cdots p_r$ w/ $r \geq 3$

m is a CN when $p_i - 1 \mid m - 1$ $\forall i$

6.3) Euler's

Def: $\varphi(n)$ = # of pos int $\leq n$ and coprime to n

Reduced residue set:

For a modulus n, we define a

RRS mod n = a set of $\varphi(n)$ elts all coprime to n.

if $n = 10 \Rightarrow$ RRS $= \{1, 3, 7, 9\}$

$\equiv \{11, -7, 77, 9\}$

Thm: Sps $\{r_1, r_2, \ldots, r_{\varphi(n)}\}$ is a RRS mod n and $\gcd(a, n) = 1$

Then $\{ar_1, ar_2, \ldots, ar_{\varphi(n)}\}$ is also RRS mod n

Euler's Thm:

$$\gcd(a, n) = 1 \Rightarrow a^{\varphi(n)} \equiv 1 \bmod n$$

$$\varphi(p^k) = p^k - p^{k-1}$$

$$\varphi(p^k) = p^{k-1}(p-1)$$

$$\varphi(p^k) = p^k\left(1 - \frac{1}{p}\right)$$

7.1)

Def: Arithmetic function is a function that is defined for all positive integers.

Def: An arithmetic function f is called multiplicative if $f(mn) = f(m) \cdot f(n)$ when $\gcd(m, n) = 1$

Def: completely multiplicative if $f(m,n) = f(m) \cdot f(n)$ for all pos int m, n

φ is multiplicative

$$\varphi(n) = \prod_{i=1}^{j} \left(p_i^{k_i} - p_i^{k_i-1}\right)$$

$$\varphi(n) = \prod p_i^{k_i-1}(p_i - 1)$$

$$\varphi(n) = n \cdot \prod_{i=1}^{j} \left(1 - \frac{1}{p_i}\right)$$

ex: $\varphi(1000) = \varphi(2^3 \cdot 5^3) = 1000 \cdot \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{5}\right)$

7.2)

Def: $\sigma(n)$ = sum of all positir divisors of n

$\tau(n)$ = # of positive divisors of n

σ, τ are multiplicative

7.3) Perfect number: $\sigma(n) = 2n$

Deficient: $\sigma(n) < 2n$

Abundant: $\sigma(n) > 2n$

$n \in \mathbb{Z}^+$ is an even perfect number

iff $n = 2^{m-1}(2^m - 1)$ w/ $2^m - 1$ = prime

A prime of the form

$2^m - 1$ is a Mersenne Prime

Thm:

if $2^m - 1$ is prime, then m = prime

Thm:

if p = odd prime then divisors of $2^p - 1$ must have the form $2pk + 1$ w/ $k \in \mathbb{Z}^+$

9.1)

Order: $\gcd(a,n)=1$

$\text{ord}_n a$ = the smallest positive power of a which yields $1 \bmod n$

$$a^{\text{ord}_n a} \equiv 1 \mod n$$

if $a^b \equiv 1$ then $b \geq \text{ord}_n a$

Thm:

$$a^x \equiv 1 \mod n \text{ if } \text{ord}_n a \mid x$$

Cor:

$$\text{ord}_n a \mid \varphi(n)$$

Thm:

$$a^x \equiv a^y \mod n$$

iff $\text{ord}_n a \mid x-y$

iff $x \equiv y \mod \text{ord}_n a$

Primitive root: $\gcd(r,n)=1$

def: r is PR mod n if $\operatorname{ord}_n r = \varphi(n)$

Thm: if r = PR mod n
then $\{r^1, r^2, \dots, r^{\varphi(n)}\}$ = reduced residue set mod n

Thm:

$$\operatorname{ord}_n(a^k) = \frac{\operatorname{ord}_n a}{\gcd(\operatorname{ord}_n a, k)}$$

(a) $\operatorname{ord}_n(a^k) = \operatorname{ord}_n a$ if $\gcd(\operatorname{ord}_n a, k) = 1$

note: if r = PR mod n then
r^k = also PR if $\gcd(\varphi(n), k) = 1$
$\Rightarrow \varphi(\varphi(n))$ PR's mod n

9.4)

Def: Sps $r = pR \bmod n$

$\text{ind}_r a$ = unique exp x b/w $1, \varphi(n)$ s.t $r^x \equiv a \bmod n$

ex: $r = 3 \bmod 14$

$3^1 \equiv 3 \Rightarrow \text{ind}_3 3 = 1$

$3^2 \equiv 9 \Rightarrow \text{ind}_3 9 = 2$

$$r^{\text{ind}_r a} \equiv a \bmod n$$

$a \equiv b \bmod n$

iff $\text{ind}_r a = \text{ind}_r b$

iff $\text{ind}_r a \equiv \text{ind}_r b \bmod \varphi(n)$

$\text{ind}_r xy \equiv \text{ind}_r x + \text{ind}_r y \bmod \varphi(n)$

$\text{ind}_r(x^k) \equiv k \cdot \text{ind}_r x \bmod \varphi(n)$

$\text{ind}_r 1 \equiv 0 \bmod \varphi(n)$ since $r^{\varphi(n)} \equiv 1$