HW7

1. Find $\text{Ord}_5 3 \Rightarrow a^x \equiv 1 \pmod{n}$

$3^1 \equiv 3 \pmod 5$ $\quad 3^2 \equiv 4 \pmod 5$

$3^3 \equiv 2 \pmod 5$ $\quad 3^4 \equiv 1 \pmod 5$

$\text{Ord}_5 3 = 4$

2. Show 2 is a primitive root of 9

2 is $r$, 9 is $n$

$\text{Ord}_n r = \phi(n) \Rightarrow \text{ord}_9 2 = \phi(9)$

$2^1 \equiv 2^1 \pmod 9$ $\quad 2^2 \equiv 4 \pmod 9$ $\quad 2^3 \equiv 8 \pmod 9$

$2^4 \equiv 7 \pmod 9$ $\quad 2^5 \equiv 5 \pmod 9$ $\quad 2^6 \equiv 1 \pmod 9$

$\text{Ord}_9 2 = 6$ $\quad \phi(9) = \phi(3^2) = 9 - 3 = 6$

$6 = 6$

3. $\text{ord}_{37} b = \phi(37)$ because $\gcd(b, 37) = 1$

$\phi(37) = 36$

$\therefore \text{ord}_{37} b \neq 8$ because $\text{ord}_{37} b$ has to be multiple of 36

4. $\text{Ord}_n r = \varphi(n)$ if $\gcd(n,r)=1$

$b = r \quad n = 41$

$\text{Ord}_{41} b$

$b \equiv 1 \pmod{41}$

$\text{ord}_n(a^u) = \dfrac{t}{\gcd(t,u)}$ where $\text{ord}_n a = t$

$\text{ord}_{41} b = \varphi(41) = 40$ because 41 primitive root of b

so, $\text{ord}_{41}(b^{15}) = \dfrac{40}{\gcd(40,15)} = \dfrac{40}{5} = 8$

If primitive root then,

$\text{ord}_{41}(b^{15}) = \varphi(41)$

$8 \neq 41$

$\therefore$ $b^{15}$ not a primitive root of 41

also corollary 9.4.1

$n^u$ is a primitive root of $n \iff \gcd(u, \varphi(n)) = 1$

$b^{15}$ is a primitive root of 41 $\iff \gcd(15, 40) = 1$
$= 8$

$\not\iff$

$b^{15}$ is not primitive root

5. $\text{ord}_{54}\, b = \phi(54) = \phi(2)\cdot\phi(3^3) = 1\cdot(3^3-3^2) = 18$

$\gcd(r, 18) = 1$ , $r = 5$

Number of incongruent roots is:

$$\phi(\phi(n)) = \phi(18) = \phi(3^2)\cdot\phi(2) = 2\cdot(3^2-3) = 6$$

6. Lagrange's theorem:

for polynomial $f(x) = a_n x^n + \dots + a_1 x + a_0$

there is <u>at most</u> $n$ incongruent roots mod $p$

$x^3 + 6 \Rightarrow$ At most 3 roots

Theorem 9.7

| | |
|---|---|
| $x = 0$ | $0^3 + 6 \equiv 6 \pmod 7$ |
| $x = 1$ | $1^3 + 6 \equiv 0 \pmod 7$ ✓ |
| $x = 2$ | $2^3 + 6 \equiv 0 \pmod 7$ ✓ |
| $x = 3$ | $3^3 + 6 \equiv 5 \pmod 7$ |
| $x = 4$ | $4^3 + 6 \equiv 0 \pmod 7$ ✓ |
| $x = 5$ | $5^3 + 6 \equiv 5 \pmod 7$ |
| $x = 6$ | $6^3 + 6 \equiv 5 \pmod 7$ |

Roots are $x = 1, 2, 4$

7.

$\phi(13) = 12$ ∴ $\phi(12) = \underline{4}$, 4 primitive roots

$12/2 = 6$
$12/3 = 4$

$2^6 \bmod 13 = 12$ ✓
$2^4 \bmod 13 = 3$

$3^6 \bmod 13 = 1$ ✗

$4^6 \bmod 13 = 1$ ✗

$5^6 \bmod 13 = 12$ ✗
$5^4 \bmod 13 = 1$

$6^6 \bmod 13 = 12$ ✓
$6^4 \bmod 13 = 9$

$7^6 \bmod 13 = 12$ ✓
$7^4 \bmod 13 = 9$

⋮

$11^6 \bmod 13 = 12$ ✓
$11^4 \bmod 13 = 3$

Found our 4 primitive roots so we can stop
$\{2, 6, 7, 11\}$

8.

Direct Proof

N.T.S. $m = \text{ord}_n b$

$$b^m \equiv 1 \pmod{n}$$

We know $n = b^m - 1$

then,

$$b^m - 1 \equiv n \pmod{n}$$

$$\Rightarrow \quad b^m \equiv n + 1 \pmod{n}$$

$$\Rightarrow \quad b^m \equiv 1 \pmod{n}$$

$$\therefore \quad m = \text{ord}_n b$$