7. $1^1, 2^2, 3^3, \dots,$ mod p

periodic w/ smallest

period $p(p-1)$.

Pf: $f(k) = k^k \bmod p$.

$f(k)$ periodic means

$f(k+T) \equiv f(k) \bmod p$

for some T $\forall k$.

↑ period

$f(k+2T) = f(k+T+T)$

$= f(k+T) = f(k)$

5. Let p be a prime such that $q = \frac{1}{2}(p-1)$ is also prime. Suppose that g is an integer satisfying

$$g \not\equiv 0 \pmod{p} \quad \text{and} g \not\equiv \pm 1 \pmod{p} \quad \text{and} g^q \not\equiv 1 \pmod{p}.$$

Prove that g is a primitive root modulo p.

if $f(k+T) \equiv f(k) \quad \forall k$

$\Rightarrow$ smallest period divides T

first show

$f(k) \equiv f(k+p(p-1))$

$f(k+p(p-1)) = (k+p(p-1))^{k+p(p-1)}$

$\equiv k^{k+p(p-1)} \equiv k^k (k^p)^{p-1}$

Fermat

$\equiv f(k) \cdot k^{p-1} \overset{\text{Fermat}}{\equiv} f(k).$

$\Rightarrow p(p-1)$ is a period.

minimality of $p(p-1)$

- first, claim that p divides the smallest period, T

Suppose not. $\Rightarrow T \not\equiv 0 \mod p$

$$f(k+T) = (k+T)^{k+T} \mod p$$

$$= f(k) \quad \forall k$$

$$- k^k$$

Set $k=p$

$$f(k+T) = (p+T)^{p+T} \equiv T^{p+T} \not\equiv 0$$

$$= p^p \equiv 0^1 \equiv 0$$

$f(k) \Rightarrow T = np$

Some n.

WTS $n = p-1$

$f(k) = f(k+T)$

$\iff k^k = (k+np)^{k+np}$

$= k^{k+np}$

$= k^k \; k^{np}$

$\iff k^{np} = 1$

$\shortparallel$

$(k^p)^n$

$\shortparallel$ Fermat

$k^n \equiv 1$

need $k^n \equiv 1 \mod p \quad \forall k$

$\iff n = p-1$

$\implies T = p(p-1)$. $\boxtimes$

5. Let p be a prime such that $q = \frac{1}{2}(p-1)$ is also prime. Suppose that g is an integer satisfying

$$g \not\equiv 0 \pmod p \quad \text{and} g \not\equiv \pm 1 \pmod p \quad \text{and} g^q \not\equiv 1 \pmod p.$$

Prove that g is a primitive root modulo p.

$p = 2q + 1$

$\mathrm{ord}(g) \mid p - 1 = 2q$

$\Rightarrow \mathrm{ord}(g) = 1, 2, q, 2q$

since q is prime.

so WTS $\mathrm{ord}(g) = 2q$

- $\mathrm{ord}(g) \neq 1$ since $g \not\equiv \pm 1 \mod p$
- $\mathrm{ord}(g) \neq 2$. since only -1 has order 2 & $g \not\equiv -1 \mod p$.
- $\mathrm{ord}(g) \neq q$ since $g^q \not\equiv 1 \mod p$

$\Rightarrow \mathrm{ord}(g) = 2q \Rightarrow g$ is p.r. ☐

p odd. show

a order 2 $\iff a = -1$.

Pf: if a has order 2

$\Rightarrow a^2 = 1$

$\iff a^2 - 1 \equiv 0$

$\iff (a-1)(a+1) \equiv 0 \mod p$

since there are no zero divisors mod p,

$a - 1 \equiv 0$ or $a + 1 \equiv 0$

$\Rightarrow a = \pm 1$.