4. Given the congruence $x^3 \equiv a \pmod{p}$, where $p \geq 5$ is a prime and $(a, p) = 1$, prove the following:

(a) If $p \equiv 1 \pmod{6}$, then the congruence has either no solutions or three incongruent solutions modulo p. ✓

(b) If $p \equiv 5 \pmod{6}$, then the congruence has a unique solution modulo p.

a) $x^3 \equiv a \bmod p$ $\qquad a \neq 0$ by hypothesis.

Let g be a p.r. mod p.

$x = g^y$ for some y, $a = g^b$ some b

$\Rightarrow g^{3y} \equiv g^b \bmod p$ $\qquad g$ is p.r.

$\Leftrightarrow 3y \equiv b \bmod \operatorname{ord}(g) = p-1$

if this has no solns, neither does $x^3 \equiv a \bmod p$

$p \equiv 1 \bmod 6 \Rightarrow p-1 \equiv 0 \bmod 6$

$\Rightarrow 6 \mid p-1 \Rightarrow 3 \mid p-1$

then $3y \equiv b \bmod p-1$ not always soluable.

$\Rightarrow 3y - b = k(p-1)$ for some k

$\Rightarrow 3y - k(p-1) = b \quad (*)$

3 divides LHS $\qquad$ maybe 3 doesn't divide

$(*)$ has solns iff $3 \mid b$

$ax + by = c$ has solns iff $(a,b) \mid c$

if $3y \equiv b \mod p-1$ <u>does</u> have solns

$\Rightarrow y \equiv b/3 \mod \frac{p-1}{3}$

$\Rightarrow$ One Solution for $y \mod \frac{p-1}{3}$. call it y_0

$\Rightarrow$ three solutions for $y \mod p-1$.

$0, \frac{p-1}{3}, 2\frac{p-1}{3}$ are distinct mod $p-1$.

$y_0, \; y_0 + \frac{p-1}{3}, \; y_0 + 2\frac{p-1}{3}$

$y_0 + \cancel{3\frac{p-1}{3}} \equiv y_0 \mod p-1$

$\Rightarrow 3$ solns.

b) $3y \equiv a \mod p-1$

if $p \equiv 5 \mod 6 \Rightarrow p-1 \equiv 4 \mod 6$

$\Rightarrow \gcd(3, p-1) = 1$

since $p-1 \equiv 4 \mod 6$

$\Rightarrow p-1 = 6k+4$ some k

$\Rightarrow p-1 \equiv 1 \mod 3$

Since the only divisors of 3 are 1 & 3,

$(3, p-1) = 1$

3 invertible mod $p-1$

$\Rightarrow 3y \equiv b \mod p-1$ has unique soln

$\boxtimes$

5. Suppose that g is a primitive root modulo p, where p is an odd prime.

(a) Let n be the order of g modulo p^2. Prove that $p-1 \mid n$.

(b) Since g is a primitive root modulo p, we have $g^{p-1} = 1 + up$ for some $u \in \mathbb{Z}$. Suppose that $p \nmid u$. Use the binomial theorem to prove that

$$g^{t(p-1)} \equiv 1 \mod p^2 \iff p \mid t$$

(c) Explain why g is a primitive root modulo p^2.

a) $n = \mathrm{ord}_{p^2}(g) \Rightarrow g^n \equiv 1 \mod p^2$

$\Rightarrow g^n \equiv 1 \mod p$

$\Rightarrow \mathrm{ord}_p(g) \mid n \Rightarrow p-1 \mid n$ $\boxtimes$

b) $g^{p-1} = 1+up$ $\quad p \nmid u$

$g^{t(p-1)} = (g^{p-1})^t = (1+up)^t$ divisible by p^2

$= \sum_{k=0}^{t} \binom{t}{k} (up)^t = 1 + tup + \underline{\qquad}$

$\equiv 1 + tup \equiv 1 \mod p^2$

$\Rightarrow tup \equiv 0 \mod p^2$

$p \nmid u \Rightarrow p \mid t$

Conversely, if $p \mid t \Rightarrow t = kp$

$$\Rightarrow g^{t(p-1)} = g^{p(p-1)k} = \left(g^{p(p-1)}\right)^k$$

$$\equiv 1^k \mod p^2 \equiv 1 \mod p^2.$$

$\uparrow$ Euler: $\varphi(p^2) = p(p-1)$.

$\forall (a, p^2) = 1 \Rightarrow a^{\varphi(p^2)} \equiv 1 \mod p^2$

c) part (a) $\Rightarrow (p-1) \mid n$

$g^n \equiv 1 \mod p^2$

by part (b), $p \mid n$

$\Rightarrow p(p-1) \mid n$ but $n \mid p(p-1)$ by Lagrange

$\Rightarrow n = p(p-1) \Rightarrow g$ is a p.r.

$\boxtimes$