133 **Quiz 6.** Name: ______________________________

1. (5 points) Prove that the odd prime divisors of the number n^2+1 are of the form $4k+1$ (use Wilson's theorem, by first converting "p divides n^2+1" into a congruence equation).

suppose $p | n^2+1$ and p is odd

then $n^2 \equiv -1 \bmod p \Rightarrow x^2 \equiv -1 \bmod p$ has a solution $x = n$

$\Rightarrow p \equiv 1 \bmod 4$ (if $p \equiv 3 \bmod 4$, $x^2 \equiv -1 \bmod p$ has no solutions).

Eg $7^2+1 = 50 = 2 \cdot 5 \cdot 5$ $\quad 5 \equiv 1 \bmod 4$

2. (3 points) Solve the congruence (you need not simplify the answer) $x^2+1 \equiv 0 \pmod{53}$.

$x = \left(\frac{53-1}{2}\right)! \equiv 26!$ or $x \equiv -26!$ mod 53.

3. Let $n = 2p$ odd prime show that $n = 2p$ divides $a^{n-1} - a$ by showing that both 2 and p divide $a^{n-1} - a$.

$n - 1 > 1$

Show

$2 | a^{n-1} - a$

if $2|a$ then $2|a^{n-1}$

$\Rightarrow 2|a^{n-1} - a$

if $2 \nmid a$, $a \equiv 1 \bmod 2$

$a^{n-1} \equiv 1 \bmod 2 \Rightarrow a^{n-1} - a \equiv 0 \bmod 2$

Show

$p | a^{n-1} - a$

case 1 : $p|a$ then $p|a^{n-1} \Rightarrow p|a^{n-1} - a$.

case 2 : if $p \nmid a$ then $a^{p-1} \equiv 1 \bmod p$

$\Rightarrow a^{2p-2} \equiv 1 \bmod p$

$\Rightarrow a^{2p-1} \equiv a \bmod p$ but $2p-1 = n-1$.

4. (4 points) Determine $\tau(300)$, $\sigma(300)$ (the number of divisors of 300 and the sum of divisors of 300).

$300 = 2^2 \cdot 3 \cdot 5^2$

$\Rightarrow \tau(300) = (2+1)(1+1)(2+1)$

$$\sigma(300) = \frac{2^3-1}{2-1} \frac{3^2-1}{3-1} \frac{5^3-1}{5-1} = 7 \cdot \cancel{\frac{8}{2}}^{4} \cdot \cancel{\frac{24}{4}}^{6}$$

$= 28 \cdot 6$

$= \underline{168}$.