Math 445 H.W. #4 Solutions

15. How many solutions? $\quad 17-1 = p-1 = 16$

(a) $x^{12} \underset{17}{\equiv} 16 \pmod{17}$ $\quad (12,16) = 4$

Check: $16^{(16/4)} \underset{17}{\equiv} (-1)^4 \underset{17}{\equiv} 1$ So eqn has $\underline{4}$ solutions.

(b) $x^{48} \equiv 9 \pmod{17}$ $\quad (48,16) = 16$

Check: $9^{16/16} = 9^1 = 9 \underset{17}{\not\equiv} 1$ So eqn has $\underline{0}$ solutions

(c) $x^{20} \equiv 13 \pmod{17}$ $\quad (20,16) = (5\cdot 4, 4\cdot 4) = 4$

Check: $13^{(16/4)} = 13^4 \underset{17}{\equiv} (169)^2 \underset{17}{\equiv} (-1)^2 \underset{17}{\equiv} 1$

So eqn. has $\underline{4}$ solutions

(d) $x^{11} \equiv 9 \pmod{17}$ $\quad (11,16) = 1$

Check: $9^{(16/1)} = 9^{16} \underset{17}{\equiv} 1$ by Fermat's Little theorem.

So eqn has $\underline{1}$ solution.

16. p prime, $p \equiv 3 \pmod 4$ then $x^4 \underset{p}{\equiv} a$ has a solution $\Longleftrightarrow x^2 \underset{p}{\equiv} a$ does.

$x^4 \underset{p}{\equiv} a$ has a solution $\Longleftrightarrow a^{\frac{p-1}{(p-1,4)}} \underset{p}{\equiv} 1$

$x^2 \underset{p}{\equiv} a$ has a solution $\Longleftrightarrow a^{\frac{p-1}{(p-1,2)}} \underset{p}{\equiv} 1$.

But $p \underset{4}{\equiv} 3 \Longrightarrow p = 4n+3$ for some n, so $p-1 = 4n+2 = 2(2n+1)$

So $(p-1,2) = 2$ (i.e. $2 \mid p-1$) and $(p-1,4) = 2$, since otherwise $(p-1,4) = 4$, i.e. $4 \mid p-1 = 2(2n+1)$, a contradiction.

So $(p-1,2)=(p-1,4)$, so $a^{\frac{p-1}{(p-1,4)}} \underset{p}{\equiv} 1 \iff a^{\frac{p-1}{(p-1,2)}} \underset{p}{\equiv} 1$.

This implies our conclusion. //

17. p prime $\operatorname{ord}_p(a)=3$, then $a^2+a+1 \underset{p}{\equiv} 0$ and $\operatorname{ord}_p(a+1)=6$.

$\operatorname{ord}_p(a)=3 \implies a^3 \underset{p}{\equiv} 1$ so $p \mid a^3-1=(a-1)(a^2+a+1)$.

But ~~[illegible]~~ $p \nmid (a-1)$, since otherwise $a^1 \underset{p}{\equiv} a \underset{p}{\equiv} 1$ so $\operatorname{ord}_p(a)=1$.

So since p is prime, $p \mid a^2+a+1$, i.e. $a^2+a+1 \underset{p}{\equiv} 0$.

This implies that $a+1 \underset{p}{\equiv} -a^2$, so $(a+1)^6 \underset{p}{\equiv} (-a^2)^6 \underset{p}{\equiv} (-1)^6 a^{12} \underset{p}{\equiv} a^{12} \equiv 1$

since $3 \mid 12$. So $\operatorname{ord}_p(a+1) \mid 6$, so $\operatorname{ord}_p(a+1)=1,2,3$ or 6.

But $(a+1)^1 \underset{p}{\equiv} (a+1) \underset{p}{\equiv} 1 \implies a \underset{p}{\equiv} 0$, so a would have no order;

$1 \underset{p}{\equiv} (a+1)^2 \underset{p}{\equiv} (-a^2)^2 \underset{p}{\equiv} a^4 \underset{p}{\equiv} a \implies a \underset{p}{\equiv} 1$, so a would have order 1;

$1 \underset{p}{\equiv} (a+1)^3 \underset{p}{\equiv} (-a^2)^3 \underset{p}{\equiv} (-1)^3 a^6 \underset{p}{\equiv} (-1)(a^3)^2 \underset{p}{\equiv} (-1) \implies$ ~~[illegible]~~ $1+1 \underset{p}{\equiv} 0$

$\implies p \mid 2 \implies p=2$, but then $a \underset{p}{\equiv} 0$ or 1 so again does not have

order 3. So $(a+1)^k \not\underset{p}{\equiv} 1$ for $0<k<6$, so $\operatorname{ord}_p(a+1)=6$. //

18. If $a \geq 2$ then $(a^m-1, a^n+1) \mid 2$ if m is odd.

Set $d=(a^m-1, a^n+1)$, so $d \mid a^m-1$, $d \mid a^n+1$, ie

$a^m \underset{d}{\equiv} 1$, $a^n \underset{d}{\equiv} -1$. $\quad a^m \underset{d}{\equiv} 1 \implies \operatorname{ord}_d(a) \mid m$, which is

odd. Only odd numbers divide odd numbers, so $\operatorname{ord}_d(a)$ is odd.

$a^n \underset{d}{\equiv} -1 \implies a^{2n} \underset{d}{\equiv} (a^n)^2 \equiv (-1)^2 \equiv 1$, so $\operatorname{ord}_d(a) \mid 2n$. But

$\mathrm{ord}_d(a)$ odd $\Rightarrow$ $(\mathrm{ord}_d(a), 2) = 1$ $\Rightarrow$ $\mathrm{ord}_d(a) \mid n$ so $a^n \underset{d}{\equiv} 1$. But since $a^n \underset{d}{\equiv} -1$, we then have $1 \underset{d}{\equiv} -1$, so $d \mid 1-(-1) = 2$. So $d \mid 2$, as desired.

19. p odd prime, $\mathrm{ord}_p(a) = \mathrm{ord}_p(b) = p-1$, then $\mathrm{ord}_p(ab) < p-1$.

Since p is odd, $p-1 = 2d$ for some d. Since

$$a^{p-1} \underset{p}{\equiv} a^{2d} \underset{p}{\equiv} (a^d)^2 \underset{p}{\equiv} 1$$ and p is prime, $a^d \underset{p}{\equiv} \pm 1$.

Since a is a primitive root, $a^d \underset{p}{\not\equiv} 1$, so $a^d \underset{p}{\equiv} -1$.

For the same reason, $b^d \underset{p}{\equiv} (-1)$. Then

$$(ab)^d \underset{p}{\equiv} a^d b^d \underset{p}{\equiv} (-1)(-1) \underset{p}{\equiv} 1.$$

So $\mathrm{ord}_p(ab) \mid d = \frac{p-1}{2} < p-1$, so ab is not ~~a~~ a primitive root of 1 mod p. ◾