Math 445 HW#3 Solutions

10. If $p \mid q$ and $a \geq 1$, then $a^p - 1 \mid a^q - 1$.

For any $n \geq 1$, $x^n - 1 = (x-1)(x^{n-1} + \dots + x + 1) = (x-1)\sum_{k=0}^{n-1} x^k$

(This can be proved by induction
$x^{n+1} - 1 = (x^n - 1)x + (x-1) = (x-1)\left(\left(x\sum_{k=0}^{n-1} x^k\right) + 1\right) = (x-1)\sum_{k=0}^{n+1-1} x^k$.)

If $p \mid q$, then $q = pn$ for some $n \geq 1$, so

$a^q - 1 = a^{pn} - 1 = (a^p)^n - 1 = (a^p - 1)\sum_{k=0}^{n-1}(a^p)^k$ is a multiple of $a^p - 1$, so $a^p - 1 \mid a^q - 1$.

11. $(m,n) = 1$ $a^p \underset{m}{\equiv} 1$, $a^q \underset{n}{\equiv} 1$, then $a^{\left(\frac{pq}{(p,q)}\right)} \underset{mn}{\equiv} 1$.

Since $(p,q) \mid p$ and $(p,q) \mid q$, $\frac{p}{(p,q)}$ and $\frac{q}{(p,q)}$ are integers. Then

$a^{\frac{pq}{(p,q)}} = (a^p)^{\frac{q}{(p,q)}} \underset{m}{\equiv} 1^{\frac{q}{(p,q)}} \underset{m}{\equiv} 1$ so $\boxed{m \mid a^{\frac{pq}{(p,q)}} - 1}$, and

$a^{\frac{pq}{(p,q)}} = (a^q)^{\frac{p}{(p,q)}} \underset{n}{\equiv} 1^{\frac{p}{(p,q)}} \underset{n}{\equiv} 1$, so $\boxed{n \mid a^{\frac{pq}{(p,q)}} - 1}$. But since

$(m,n) = 1$, this implies that $mn \mid a^{\frac{pq}{(p,q)}} - 1$, i.e. $a^{\frac{pq}{(p,q)}} \underset{mn}{\equiv} 1$.

[oops, or just note that $p \mid \frac{pq}{(p,q)}$, so $a^p - 1 \mid a^{\frac{pq}{(p,q)}} - 1$, to get the two boxes ...]

12. If $(m,n) = 1$ (and $(10,m) = (10,n) = 1$) then

$$\mathrm{ord}_{mn}(10) = \frac{\mathrm{ord}_m(10) \cdot \mathrm{ord}_n(10)}{(\mathrm{ord}_m(10), \mathrm{ord}_n(10))}$$

For ease of notation, set $r = \mathrm{ord}_m(10)$, $s = \mathrm{ord}_n(10)$. Then r is smallest positive integer with $10^r \underset{m}{\equiv} 1$, and same for s: $10^s \underset{n}{\equiv} 1$. By problem 11, we then know that $10^{\frac{rs}{(r,s)}} \underset{mn}{\equiv} 1$, since

$(m,n)=1$. So $\text{ord}_{mn}(10) \Big| \frac{rs}{(r,s)}$. To show that $\text{ord}_{mn}(10) = \frac{rs}{(r,s)}$, we then need to show that $\frac{rs}{(r,s)} \Big| \text{ord}_{mn}(10)$, i.e. if $10^k \underset{mn}{\equiv} 1$, then $\frac{rs}{(r,s)} \Big| k$. But $10^k \underset{mn}{\equiv} 1 \iff mn \mid 10^k-1 \iff$ (since $(m,n)=1$) $m \mid 10^k-1$ and $n \mid 10^k-1$. [($\Longrightarrow$) is immediate, since $m,n \mid mn$; ($\Longleftarrow$) uses $(m,n)=1$.] But $m \mid 10^k-1 \iff r=\text{ord}_m(10) \mid k$, and $n \mid 10^k-1 \iff s=\text{ord}_n(10) \mid k$. So $10^k \underset{mn}{\equiv} 1 \iff r \mid k$ and $s \mid k$. But

$r \mid k$ and $s \mid k \Longrightarrow \frac{rs}{(r,s)} \Big| k$, set $k=ru$, $k=sv$, then writing $(r,s)=rx+sy$ we have $(r,s)u = rxu+syu = (ru)x+syu$
$=(sv)x+syu = s(vx+yu)$, so $u=\frac{s}{(r,s)}(vx+yu)$, so
$k=ru=\frac{rs}{(r,s)}(vx+yu)$, i.e. $\frac{rs}{(r,s)} \Big| k$. ///

13. $(3,n)=(10,n)=1 \Longrightarrow \text{ord}_{3n}(10)=\text{ord}_n(10)$.

Since $(3,n)=1$ and $\text{ord}_3(10)=1$ [$10^1=10 \underset{3}{\equiv} 1$], from problem 12 above we have

$$\text{ord}_{3n}(10) = \frac{\text{ord}_3(10)\cdot\text{ord}_n(10)}{(\text{ord}_3(10),\ \text{ord}_n(10))} = \frac{1\cdot\text{ord}_n(10)}{(1,\text{ord}_n(10))}$$
$$= \frac{1\cdot\text{ord}_n(10)}{1} = \text{ord}_n(10). \quad ///$$

14. For any n $\quad \mathrm{ord}_n(10) \mid \mathrm{ord}_{n^2}(10)$. Compute $\mathrm{ord}_{49}(10)$.

Set $r = \mathrm{ord}_n(10)$ so $10^k \underset{n}{\equiv} 1 \Rightarrow r \mid k$. Set $s = \mathrm{ord}_{n^2}(10)$, so $10^s \underset{n^2}{\equiv} 1$, i.e. $n^2 \mid 10^s - 1$. But since $n \mid n^2$, we have $n \mid 10^s - 1$ so $10^s \underset{n}{\equiv} 1$, so $r \mid s$. So $\mathrm{ord}_n(10) \mid \mathrm{ord}_{n^2}(10)$.

To compute $\mathrm{ord}_{49}(10)$, we have $(10, 49) = 1$ $\quad [1 = 5 \cdot 10 + (-1) \cdot 49$
so we know from Fermat's Little Theorem that $\phi(49) = \phi(7^2) = 7^1 \cdot (7-1) = 42$; we also know that $10^{\phi(49)} \underset{49}{\equiv} 1$. $\mathrm{ord}_7(10) = 6$ (since, e.g. $\frac{1}{7} = .\overline{142857}$ has period 6.). So $\mathrm{ord}_{49}(10) \mid \phi(49) = 42$. So $\mathrm{ord}_7(10) = 6 \mid \mathrm{ord}_{49}(10)$, and $\mathrm{ord}_{49}(10) \mid \phi(49) = 42$. So $\mathrm{ord}_{49}(10) = 6$ or 42 (the only multiples of 6 which divide 42.)

So we check: $\quad 10^2 = 100 \underset{49}{\equiv} 2$, so $10^6 = (10^2)^3 \underset{49}{\equiv} 2^3 = 8 \underset{49}{\not\equiv} 1$.

So since $\mathrm{ord}_{49}(10) \neq 6$, we must have $\mathrm{ord}_{49}(10) = 42$.