Math 445 Homework 4 solutions

13. Show that if $n|m$, and $(10, m) = 1$, then the period of the decimal expansion of $1/n$ divides the period of the decimal expansion of $1/m$.

Translating this into the language of orders, if $n|m$ and $(10, m) = 1$, then we wish to show that $\text{ord}_n(10)|\text{ord}_m(10)$. Setting $s = \text{ord}_m(10)$, it is enough to show that $10^s \equiv 1 \pmod{n}$, since we know that $\text{ord}_n(10)$ divides any such exponent. But by definition, $10^s \equiv 1 \pmod{m}$, so $m|10^s - 1$, so $10^s - 1 = mx$ for some x . But since $n|m$, $m = ny$ for some y, so $10^s - 1 = mx = (ny)x = n(xy)$, so $n|10^s - 1$, so $10^s \equiv 1 \pmod{n}$, as desired.

14. Show that for every $n \geq 2$, $\text{ord}_{3^n}(10) = 3^{n-2}$.

(Hint: induction! This is not entirely unlike what we did for 7^n....)
[N.B.: Consequently, the period of the decimal expansion of $1/3^n$ is 3^{n-2} .]

We show first that for every $n \geq 2$, $10^{3^{n-2}} = 1 + k3^n$ for some k with $(k, 3) = 1$. We proceeed by induction. For $n = 2$, $10^{3^{2-2}} = 10^{3^0} = 10^1 = 10 = 1 + 1 \cdot 3^2$, so $k = 1$ and $(1, 3) = 1$. Now suppose that $10^{3^{n-2}} = 1 + k3^n$ for some k with $(k, 3) = 1$. Then

$$\begin{aligned}
10^{3^{(n+1)-2}} &= 10^{3^{n-2} \cdot 3} = (10^{3^{n-2}})^3 = (1 + k3^n)^3 \\
&= 1 + 3(1)^2(k3^n) + 3(1)(k3^n)^2 + (k3^n)^3 \\
&= 1 + k3^{n+1} + k^2 3^{2n+1} + k^3 3^{3n} \\
&= 1 + (k + k^2 3^n + k^3 3^{2n-1})3^{n+1}
\end{aligned}$$

with $k + k^2 3^n + k^3 3^{2n-1} \equiv k + k^2(0) + k^3(0) \equiv k \pmod{3}$ (since $n, 2n - 1 \geq 1$) . So $(k + k^2 3^n + k^3 3^{2n-1}, 3) = (k, 3) = 1$, so $10^{3^{(n+1)-2}} = 1 + K3^{n+1}$ with $(K, 3) = 1$, as desired. So by induction, for $n \geq 2$, $10^{3^{n-2}} = 1 + k3^n$ for some k with $(k, 3) = 1$.

Since $10^{3^{n-2}} = 1 + k3^n$, $10^{3^{n-2}} \equiv 1 \pmod{3^n}$, so $\text{ord}_{3^n}(10)|3^{n-2}$. So either $\text{ord}_{3^n}(10) = 3^{n-2}$ or $\text{ord}_{3^n}(10) = 3^m$ for some $m < n - 2$. But we know from above that $10^{3^m} - 1 = k3^{m+2}$ for some k with $(k, 3) = 1$. So if $\text{ord}_{3^n}(10) = 3^m$, then $3^n|10^{3^m} - 1$, so $10^{3^m} - 1 = s3^n$ for some s. But then $k3^{m+2} = s3^n$, so cancelling powers of 3, $k = s3^{n-(m+2)} = s3^{(n-2)-m} = s3^r$ for some $r \geq 1$. So $3|k$, so $(k, 3) = 3$, a contradiction. So $\text{ord}_{3^n}(10) = 3^{n-2}$, as desired.

15. Show that if $(3, n) = 1$ (and $(10, n) = 1$), then $\text{ord}_n(10) = \text{ord}_{3n}(10) = \text{ord}_{9n}(10)$.

By problem number 13, we know that $\text{ord}_n(10)|\text{ord}_{3n}(10)$ and $\text{ord}_{3n}(10)|\text{ord}_{9n}(10)$. In particular, $\text{ord}_n(10) \leq \text{ord}_{3n}(10)$ and $\text{ord}_{3n}(10) \leq \text{ord}_{9n}(10)$. To show that they are all equal, it suffices to show that $\text{ord}_{9n}(10) \leq \text{ord}_n(10)$; what we will if fact show is that $\text{ord}_{9n}(10)|\text{ord}_n(10)$.

$\text{ord}_n(10)$ is the smallest positive k for which $n|10^k - 1$, and so it is enough to show that if $n|10^k - 1$, then $9n|10^k - 1$. But $10 \equiv 1 \pmod{9}$, so $1)^k \equiv 1^k = 1 \pmod{9}$. so $9|10^k - 1$ for <u>every</u> $k \geq 1$. and since $(3, n) = 1$, 3 and n share no factors, so 9 and n share no factors (p prime and $p|9 = 3^2$, $p|n$, then $p|3$ and $p|n$, so $p|(3, n) = 1$), so $(9, n) = 1$.

But $n|10^k-1$, $9|10^k-1$, and $(9,n)=1$ together imply $9n|10^k-1$, as desired. So $\mathrm{ord}_{9n}(10)|\mathrm{ord}_n(10)$, and so

$$\mathrm{ord}_n(10)=\mathrm{ord}_{3n}(10)=\mathrm{ord}_{9n}(10), \text{ as desired.}$$

16. Find the primitive roots of 1 mod 31. (I.e., find all a, $1\le a\le 31$, with $\mathrm{ord}_{31}(a)=30$. (Hint: find one; then use one of our results to quickly find the others.)

To get started, we don't have much better than random chance? $\phi(31)=31-1=30=2\cdot3\cdot5$, so the possible orders of elements are 2,3,5,6,10,15, or 30. We could construct a primitive root in the course of our failures if we assemble exactly the data needed to use the proof of existence, i.e., numbers of orders 2, 3, and 5 precisely; their product will be a primitive root. But that seems unlikely to occur first...

Start with $a=2$; mod 31, $a^2=4$, $a^4=16$, $a^8=256=31{\cdot}8{+}8\equiv8$, $a^{16}\equiv64=31{\cdot}2{+}2\equiv2$. So $a^2=4\not\equiv1$, $a^3=4\cdot2=8\not\equiv1$, but $a^5=32\equiv1$, so 2 has order 5 mod 31.

Next try $a=3$; mod 31, $a^2=9$, $a^4=81=31\cdot3-12\equiv-12\equiv19$,
$a^8\equiv19^2=361=31\cdot11+20\equiv20$, and
$a^{16}\equiv20^2=400=31\cdot13-3\equiv-3\equiv28$.

So $a^2=9\not\equiv1$,
$a^3=9\cdot3=27\not\equiv1$,
$a^5=a^4\cdot a\equiv19\cdot3=57\equiv26\not\equiv1$,
$a^6=a^4\cdot a^2\equiv19\cdot9=171=31\cdot5+16\equiv16\not\equiv1$,
$a^{10}=a^8\cdot a^2\equiv20\cdot9=180=31\cdot6-6\equiv25\not\equiv1$,
$a^{15}=a^{10}a^5\equiv25\cdot26=650=31\cdot20+30\equiv30\equiv-1\not\equiv1$,
and just for sanity's sake, $a^{30}=a^{15}a^{15}\equiv(-1)^2=1$.
So 3 has order 30 mod 31, and so is a primitive root of 1 mod 31.

To find all other primitive roots of 1 mod 31, we can take all 3^k mod 31, for $(k,\phi(31))=(k,30)=1$. But the numbers coprime to $30=2\cdot3\cdot5$ are the numbers less than 30 that are not multiples of 2, 3, or 5, i.e., $k=1,7,11,13,17,19,23,29$ (since $30<6^2=36$, we should have expected all primes...). Note that we know this list is complete, since $\phi(\phi(31))=\phi(30)=\phi(2\cdot3\cdot5)=1\cdot2\cdot4=8$, so we should have 8 primitive roots. So we compute:

$3^1=3$, $3^7=3^43^3\equiv19\cdot27=540-27=31\cdot18-18-27\equiv-45\equiv-14\equiv17$,
$3^{11}=3^83^3\equiv20\cdot27=540=31\cdot18-18\equiv-18\equiv13$,
$3^{13}=3^{11}3^2\equiv13\cdot9=117=31\cdot4-7\equiv-7\equiv24$,
$3^{17}=3^{16}3\equiv-3\cdot3=-9\equiv22$,
$3^{19}=3^{17}3^2\equiv22\cdot9=198=31\cdot6+12\equiv12$,
$3^{23}=3^{19}3^4\equiv12\cdot19=240-12=31\cdot8-8-12\equiv-20\equiv11$,
and $3^{29}=3^{16}3^{13}\equiv28\cdot24\equiv(-3)\cdot(-7)=21$.

So the primitive roots of 1 mod 31 are: 3, 17, 13, 24, 22, 12, 11, and 21, or, in increasing order, 3, 11, 12, 13, 17, 21, 22, and 24. Who would have guessed....