Math 135 — Alexander Maguire
Assignment 8 — 20396195

1) Find solutions to: $\begin{matrix} 15x \equiv 4 \pmod{26} \\ 24x \equiv 6 \pmod{63} \end{matrix}$.

We must find an arbitrary solution to the first congruency, which through a small amount of brute forcing yields $x=2$, so $x \equiv 2 \pmod{26}$, and now for the second congruency (with substantially more brute forcing): $x=16$. The solution to the following simultaneous congruencies is the same as our original question:

$\begin{matrix} x \equiv 2 \pmod{26} \\ x \equiv 16 \pmod{63} \end{matrix}$. We can now construct a linear equation from the first one, and solve it:

$\begin{matrix} 26y + 2 \equiv 16 \pmod{63} \\ 26y \equiv 14 \pmod{63} \end{matrix}$. With more brute forcing, we learn that $y=49$ is a solution, so $y \equiv 49 \pmod{63}$, therefore $y = 49 + 63z$. Substituting this back into $x = 2 + 26y$, we obtain $x = 1276 + 1638z$, ie $x \equiv 1276 \pmod{1638}$.

2) Given $\begin{matrix} n \equiv 1 \pmod{5} \\ n \equiv 0 \pmod{7} \\ n \equiv 6 \pmod{11} \\ n \equiv 5 \pmod{12} \end{matrix}$, solve for n.

$n \equiv 2261 \pmod{4620}$

3) RTS: $21 | (3n^7 + 7n^3 + 11n)$.

To prove $21 | (3n^7 + 7n^3 + 11n)$ we need prove only $3 | (3n^7 + 7n^3 + 11n)$ and $7 | (3n^7 + 7n^3 + 11n)$. In the first case, we observe that $3 | 3n^7$ trivially, and that $7n^3 \equiv 7n \pmod{3}$. Thus we have $3 | 18n$, again, trivially true. Since 3 divides all of the terms, 3 must divide the entire polynomial.

In the second case, $7 | 7n^3$ trivially, $3n^7 \equiv 3n \pmod{n}$, and so $7 | 14n$. Again, 7 divides the entire polynomial . QED ❑ .

4)

$$\begin{aligned} 279 &\equiv 79 \pmod{100} \\ 279^2 &\equiv 41 \pmod{100} \\ 279^4 &\equiv 81 \pmod{100} \\ 279^8 &\equiv 61 \pmod{100} \\ 279^{16} &\equiv 21 \pmod{100} \\ 279^{32} &\equiv 41 \pmod{100} \\ 279^{64} &\equiv 81 \pmod{100} \\ 279^{128} &\equiv 61 \pmod{100} \\ 279^{256} &\equiv 21 \pmod{100} \\ 279^{512} &\equiv 41 \pmod{100} \end{aligned}$$

$$279^{669} \equiv 279^{512} 279^{128} 279^{16} 279^{8} 279^{4} 279 \pmod{100}$$

$$279^{669} \equiv 19 \pmod{100}$$

5) RTS: $\phi(m) = \phi(2m)$ iff *m* is odd.

$\phi(ab) = \phi(a) \cdot \phi(b)$ when *a* and *b* are coprime. Because we know m is odd, it must be coprime to 2, and so $\phi(m) \cdot \phi(2) = \phi(2m)$. Since $\phi(2) = 1$, so $\phi(m) = \phi(2m)$, when .
QED. ❑