Math 135 Alexander Maguire
Assignment 7 20396195

1) RTS: $641 | (2^{2^5}+1)$.
This is the same as showing $2^{2^5}+1 \equiv 641 (mod\, 641)$, which of course is the same as $2^{32} mod\, 641 + 1\, mod\, 641 = 0$. Trivially, $1\, mod\, 641 = 1$ and we observe that $2^{32} = (2^{16})^2$.
We can now expand this upwards modulo 641 to get our answer $2^8 = 256$.
$2^{16} = 256^2 = 65536\, mod\, 641 = 154$, and finally $2^{32} \equiv 154^2 \equiv 23716 \equiv 640 (mod\, 641)$. Nice!
❑

2) Find $26^{7^9} (mod\, 11)$. We can use Fermat's Little Theorem to determine that $26^{10} \equiv 1 (mod\, 11)$, as 11 is prime and coprime to 26. Because $7^9 = 40353607$, we can rewrite it as $10 \cdot 4035360 + 7$, and thus $26^{7^9} = 26^{10^{4035360}} 26^7$. Because congruency is maintained through multiplication, $26^{10^{4035360}} \equiv 1 (mod\, 11)$ implying $26^{7^9} \equiv 1 \cdot 26^7 (mod\, 11)$.
Now we can transform 26 into a congruency class in $\mathbb{Z}_{11}$, $[26] = [4]$.
$[4^7] = [4^3][4^4] = [9][256] = [9][3] = [27] = [5]$, therefore $26^{7^9} \equiv 5 (mod\, 11)$.

3) $p-1 = qs + r$
a) RTS $a^r \equiv 1 (mod\, p)$ from $a^{p-1} \equiv 1 (mod\, p)$.
$a^{p-1} \equiv 1 (mod\, p)$
$a^{qs+r} \equiv 1 (mod\, p)$
$a^{qs} a^r \equiv 1 (mod\, p)$
but $a^s \equiv 1 (mod\, p)$, so any multiple of *s* (including qs) is also congruent to 1, so $1 \cdot a^r \equiv 1 (mod\, p)$, and thus $a^r \equiv 1 (mod\, p)$. ❑
b) Since $a^s \equiv 1 (mod\, p)$ and *s* is the smallest positive integer, and $0 \leqslant r \leq s$, *r* must be 0.
c) Because $r = 0$, $p-1 = qs + 0$, and $1 \cdot a^r \equiv 1 (mod\, p)$, $s | (p-1)$ must be true.
d) As we have seen above, $p-1 = qs$, and that $s | (p-1)$, $p-1 = s$, so the smallest positive integer *s* for $8^s \equiv 1 (mod\, 17)$ must be 16.

4) Solve $\begin{matrix}[7][x]+[12][y]=[6] \\ [6][x]+[11][y]=[13]\end{matrix}$ in $\mathbb{Z}_{20}$:

$$[7][x]+[12][y]=[6]$$
$$[21][x]+[36][y]=[18]$$
$$[x]+[16][y]=[18]$$
$$[x]=[18]-[16][y]$$
$$[6]([18]-[16][y])+[11][y]=[13]$$
$$[8]-[16][y]+[11][y]=[13]$$
$$[27][y]=[-5]$$
$$[7][y]=[15]$$
$$[y]=[45]$$
$$[y]=[5]$$

now solve for x:
$$[7][x]+[12][5]=[6]$$
$$[7][x]+[60]=[6]$$
$$[x]=[18]$$

5) Solve $\begin{matrix}[8][x]+[3][y]=[9] \\ [6][x]+[5][y]=[2]\end{matrix}$ in $\mathbb{Z}_{12}$:

$$\begin{gathered}[8][x]+[3][y]=[9] \\ [32][x]+[12][y]=[36] \\ [8][x]=[0] \\ [x]=[0]\end{gathered}$$

now solve for y:

$$\begin{gathered}[6][0]+[5][y]=[2] \\ [25][y]=[10] \\ [y]=[10]\end{gathered}$$