Solutions to Exam 2 Practice Problems

1. Following the procedure from class notes: Set $N_1 = 77$, $N_2 = 66$ and $N_3 = 14$.

$N_1 \equiv 77 \equiv 5 \bmod 6$. $N_1^{-1} \equiv 5 \bmod 6$
$N_2 \equiv 66 \equiv 3 \bmod 7$. $N_2^{-1} \equiv 5 \bmod 7$
$N_3 \equiv 14 \equiv 3 \bmod 11$. $N_3^{-1} \equiv 4 \bmod 11$

Proposed Sol^{n}: $15 \cdot 77 \cdot 5 + 2 \cdot 66 \cdot 5 + 9 \cdot 14 \cdot 4 = 6939$.

Since Sol^{n}s to the system of Congruences are unique modulo $6 \cdot 7 \cdot 11 = 462$, and $6939 \equiv 9 \bmod 462$, 9 is also a sol^{n}.

Check: $9 \equiv 3 \bmod 6$ and $15 \equiv 3 \bmod 6$ $\Rightarrow 9 \equiv 15 \bmod 6$,

$9 \equiv 2 \bmod 7$ and $9 \equiv 9 \bmod 11$.

2. (a) One sol^{n}: $1512 = 2^3 \cdot 3^3 \cdot 7$

$\Rightarrow \phi(1512) = (2^3 - 2^2) \cdot (3^3 - 3^2) \cdot (7^1 - 7^0) = 4 \cdot 18 \cdot 6 = 432$

(b) Applying Euler's Product formula: $1512 \cdot (1 - \frac{1}{2})(1 - \frac{1}{3})(1 - \frac{1}{7})$

$= 1512 \cdot \frac{1}{2} \cdot \frac{2}{3} \cdot \frac{6}{7} = 432$, as required.

(c) $\phi(81 \cdot 77) = \phi(3^4 \cdot 7^1 \cdot 11^1) = (3^4 - 3^3)(7^1 - 7^0)(11^1 - 11^0) = 72 \cdot 6 \cdot 10 = 4320$

$\phi(81) = 3^4 - 3^3 = 72$ || $\phi(77) = (7^1 - 7^0)(11^1 - 11^0) = 60$ $\Rightarrow \phi(81) \cdot \phi(77) = 72 \cdot 60 = 4320$

3. $3451 \equiv 6 \bmod 13 \Rightarrow (3451)^{8,888,213} \equiv 6^{8,888,213} \bmod 13.$

On the other hand: $a^{12} \equiv 1 \bmod 13$ for all $a \in \mathbb{Z}$.

Since $8,888,213 = (12)\cdot(740,684) + 5$

$$6^{8,888,213} \equiv \left(6^{12}\right)^{(740,685)} \cdot 6^{5} \bmod 13$$

$$\equiv 1^{740,685} \cdot 6^{5} \bmod 13$$

$$\equiv 6^{5} \bmod 13$$

$$\equiv 7776 \bmod 13$$

$$\boxed{\equiv 2 \bmod 13}$$

4. We need to find the residues a modulo 19 such that

$$a^{9} \equiv 1 \bmod 19.$$

$1^9 \equiv 1 \bmod 19$
$2^9 \equiv -1 \bmod 19$
$3^9 \equiv -1 \bmod 19$
$4^9 \equiv 1 \bmod 19$
$5^9 \equiv +1 \bmod 19$
$6^9 \equiv 1$
$7^9 \equiv 1 \bmod 19$
$8^9 \equiv -1 \bmod 19$
$9^9 \equiv 1 \bmod 19$
$10^9 \equiv -1 \bmod 19$
$11^9 \equiv 1 \bmod 19$

CHECK:
$1 \equiv 1^2 \bmod 19$
$4 \equiv 2^2 \bmod 19$
$9 \equiv 3^2 \bmod 19$
$16 \equiv 4^2 \bmod 19$
$6 \equiv 5^2 \bmod 19$
$11 \equiv 7^2 \bmod 19$
$7 \equiv 8^2 \bmod 19$
$5 \equiv 9^2 \bmod 19$
~~$0 \equiv 10^2 \bmod 19$~~
$17 \equiv 6^2 \bmod 19$

$12^9 \equiv -1 \bmod 19$
$13^9 \equiv -1 \bmod 19$
$14^9 \equiv -1 \bmod 19$
$15^9 \equiv -1 \bmod 19$
$16^9 \equiv 1 \bmod 19$

$17 \equiv 1 \bmod 19$
$18 \equiv -1 \bmod 19$

Recall: There are $\frac{19-1}{2} = 9$ Squares

So These are The Squares mod 19

#5) $\left(\frac{6}{241}\right) = \left(\frac{2}{241}\right)\cdot\left(\frac{3}{241}\right) = 1\cdot\left(\frac{3}{241}\right)$, since $241 \equiv 1 \bmod 8 \equiv (-1)^{\frac{241^2-1}{8}}\cdot\left(\frac{241}{3}\right)$

$= 1\cdot\left(\frac{1}{3}\right) = 1\cdot 1 = 1$

$\left(\frac{1000001}{17}\right) = \left(\frac{10}{17}\right) = \left(\frac{2}{17}\right)\cdot\left(\frac{5}{17}\right) = 1\cdot(-1)^{\frac{2\cdot 8}{8}}\left(\frac{17}{5}\right)$, since $17 \equiv 1 \bmod 8 = \left(\frac{2}{5}\right) = -1$ since $5 \equiv 5 \bmod 8$

$\left(\frac{-46}{101}\right) = \left(\frac{-1}{101}\right)\left(\frac{2}{101}\right)^4\cdot\left(\frac{3}{101}\right) = (-1)^{50}\cdot 1\cdot\left(\frac{3}{101}\right) = (-1)^{50\cdot 1}\left(\frac{101}{3}\right) = \left(\frac{2}{3}\right) = -1$

#6) $\frac{p}{2} = \frac{31}{2} = 15.5$.

$\frac{p-1}{2} = 15$

1st: 5, 10, 15, 20, 25, 30, 35, 40, 45, 50, 55, 60, 65, 70, 75

5, 10, 15, [illegible], [illegible], [illegible], +4, +9, +14, [illegible], -12, -7, -2, 3, 8, 13

5, 10, 15, -11, -6, -1

negative terms is 6

$\therefore \left(\frac{5}{31}\right) = (-1)^6 = 1$

check: $\left(\frac{5}{31}\right) = 1\cdot\left(\frac{31}{5}\right) = \left(\frac{1}{5}\right) = 1$.

#7) (a) Modulo 7: $f(x)$ becomes $3x^2$ which has 0 as a root mod 7

(b) modulo 19: $f(x)$ becomes $x^2 - 7x + 1$. The discriminant:

$(-7)^2 - 4 = 49 - 4 = 45 \equiv 7 \bmod 19$. From #4 we know

$7 \equiv 8^2 \bmod 19$.

We want "$\frac{-b \pm \sqrt{b^2-4ac}}{2a}$" $= \frac{7 \pm 8}{2} = \frac{15}{2}$ or $\frac{-1}{2} \bmod 19$

But $2^{-1} \equiv 10 \bmod 19$ $\therefore$ $\frac{15}{2} \equiv 150 \equiv 17 \bmod 19$, $\frac{-1}{2} \equiv \frac{18}{2} = 180 \equiv 9 \bmod 19$.

Basic Roots: 17 and 9. Check $f(17) \equiv 17^2 - 119 + 1 \equiv 18 + 1 \equiv 0 \bmod 19$.

$f(9) \equiv 9^2 - 63 + 1 \equiv 19 \equiv 0 \bmod 19$

Thus: $\{17 + 19n \mid n \in \mathbb{Z}\} \cup \{9 + 19\cdot r \mid r \in \mathbb{Z}\}$ gives the full set of Roots modulo 19.