Zackery Field
ID: 23031734
CS 70, Summer 2013
Homework 2
Problem 5 [21 Points]

1. [21 Points] Application of modular arithmetic.

   (a) [3 Points] Evaluate $(3002 + 6002 * 9002)(mod 3)$.

$$\begin{aligned} 3002 + 6002 * 9002 \quad & mod 3 \\ 2 + 2 * 2 \quad & mod 3 \\ 6 \quad & mod 3 \\ 0 \quad & mod 3 \end{aligned}$$

   (b) [3 Points] Evaluate $(1002^3 - 2468 * 17 + 4)(mod 5)$.

$$\begin{aligned} 1002^3 - 2468 * 17 + 4 \quad & mod 5 \\ \prod_{i=0}^{n-1} (1002^{2^i})^{a_i} - 2468 * 17 + 4 \quad & mod 5 \\ (((1002^{2^1})^1) * ((1002^{2^0})^1)) - 2468 * 17 + 4 \quad & mod 5 \\ (((1002^{2^1})^1) * ((1002^{2^0})^1)) - 2468 * 17 + 4 \quad & mod 5 \\ 3 - 3 * 2 + 4 \quad & mod 5 \\ 1 \quad & mod 5 \end{aligned}$$

   (c) [3 Points] The numbers $\{0, 1, 2, \ldots, 19\}$are "representative" of the congruence classes mod 20. For each of these classes, determine whether it has an inverse in mod 20, and if so, state the inverse. If the equation congruence proposition is left in a form not specifying b, then there exists no inverse.

$$
\begin{aligned}
0 * b &\equiv 1 (mod 20) \\
1 * 1 &\equiv 1 (mod 20) \\
2 * b &\equiv 1 (mod 20) \\
3 * 7 &\equiv 1 (mod 20) \\
4 * b &\equiv 1 (mod 20) \\
5 * b &\equiv 1 (mod 20) \\
6 * b &\equiv 1 (mod 20) \\
7 * 3 &\equiv 1 (mod 20) \\
8 * b &\equiv 1 (mod 20) \\
9 * 9 &\equiv 1 (mod 20) \\
10 * b &\equiv 1 (mod 20) \\
11 * 11 &\equiv 1 (mod 20) \\
12 * b &\equiv 1 (mod 20) \\
13 * 17 &\equiv 1 (mod 20) \\
14 * b &\equiv 1 (mod 20) \\
15 * b &\equiv 1 (mod 20) \\
16 * b &\equiv 1 (mod 20) \\
17 * 13 &\equiv 1 (mod 20) \\
18 * b &\equiv 1 (mod 20) \\
19 * 19 &\equiv 1 (mod 20)
\end{aligned}
$$

(d) [3 Points] Evaluate $\frac{5-(19-3)}{7*9}(mod 20)$.

$$
\begin{aligned}
\frac{5-(19-3)}{7*9} & \quad (mod 20) \\
\frac{-11}{63} & \quad (mod 20) \\
-11 * (\frac{1}{63})^{-1} &\equiv 1 (mod 20)
\end{aligned}
$$

Discovering $(\frac{1}{63})^{-1}$through the extended Euclidean formula:

$$
\begin{aligned}
63 &= 3*20+3 \\
20 &= 6*3+2 \\
3 &= 2*1+1 \\
&\textit{Back} \\
1 &= 3-1*2 \\
&= 3-(20-6*3) \\
&= 3-(20+6(63-3(20)) \\
&= 63-20*3-20+6(63)-18(20) \\
&= (7)63-(22)20
\end{aligned}
$$

Continuing from the block abocve:

$$
\begin{aligned}
-11*7 &\equiv 1(mod 20) \\
3 &\equiv (mod 20)
\end{aligned}
$$

(e) [3 Points] Use extended Euclidean to find the inverse of 36 mod 55.

$$
\begin{aligned}
55 &= 1*36+19 \\
36 &= 1*19+17 \\
19 &= 1*17+2 \\
17 &= 8*2+1 \\
&\textit{Back} \\
1 &= 17-8*2 \\
&= 17-8*(19-17) \\
&= 17-8*(19-(36-19)) \\
&= (36-19)-8*((55-36)-(36-(55-36))) \\
&= (36-(55-36))-8*(55-36-36+55-36) \\
&= (2*36-55)-8*(-3*36+2*55) \\
&= (26)36-(17)55 \\
inverse &= 26
\end{aligned}
$$

(f) [3 Points] Describe the solutions to $17x \equiv 4(mod 20)$.

$$
\begin{aligned}
17x + 20y &= 4 \\
&\textit{Euclid} \\
20 &= 1 * 17 + 3 \\
17 &= 5 * 3 + 2 \\
3 &= 1 * 2 + 1 \\
&\textit{Back} \\
1 &= 3 - 2 \\
&= 3 - (17 - 5 * 3) \\
&= 3 - (17 - 5 * (20 - 17)) \\
&= 20 - 17 - 17 + 5 * 20 - 5 * 17 \\
&= (6)20 - (7)17
\end{aligned}
$$

$$
\begin{aligned}
17(-28) &\equiv 4(mod 20) \\
x &= -28(mod 20) \\
&= 12
\end{aligned}
$$

$x = 12$ is a general solution to $17x \equiv 4(mod 20)$. The general solution is described as $12 + 20k$, $k \in \mathbb{Z}$

(g) [3 Points]