Section 4.4

Ex 6.

a) $a=2, m=17$, $17=2\cdot 8+1$ so $1=17-8\cdot 2$

so -8 is ~~the~~ an inverse

Ex. 20.

$x\equiv 2 \pmod 3$, $x\equiv 1 \pmod 4$, $x \equiv 3 \pmod 5$

Let $m=3\times 4\times 5=60$, $M_1=m/3=20$, $M_2=m/4=15$, $M_3=m/5=12$

We see that:

-1 is an inverse of $M_1 = 20 \bmod 3$ since $20\cdot(-1)\equiv 2 \pmod 3$

-1 is an inverse of $M_2 = 15 \bmod 4$ since $15\cdot(-1)\equiv \cancel{7}\ 1 \pmod 4$

-2 is an inverse of $M_3 = 12 \bmod 5$ since $12\cdot(-2)\equiv 1 \pmod 5$

Hence: $x = a_1M_1y_1 + a_2M_2y_2 + a_3M_3y_3$

$= 2\times 20\times(-1) + 1\times 15\times(-1) + 3\times 12\times(-2)$

$= -107 \equiv 53 \pmod{60}$

$\therefore$ the solution is $60k+53$ $(k\in\mathbb{Z})$

Ex. 22

$x\equiv 3 \pmod 6$, $x\equiv 4 \pmod 7$, using back substitution

From the first congruence equation : we know: $x=6t+3$ $(t\in\mathbb{Z})$ we can get substitute it to the second congruence equation

$6t+3\equiv 4 \pmod 7 \Rightarrow t\equiv 6 \pmod 7$

then we know: $t=7u+6$ $(u\in\mathbb{Z})$

substitute this back: $x = 6(7u+6)+3$

$= 42u+39$

So we get the solution is:

$x\equiv 39 \pmod{42}$

Ex.34

Use Fermat's little Theorem to find $23^{1002} \bmod 41$

$$
\begin{aligned}
23^{1002} \bmod 41 &= \cancel{(23^{28})^{35} \cdot 23^{22} \bmod 41} \\
&= \cancel{1^{35} \cdot (23^{6})^{3} \cdot 23^{4}} \\
&= (23^{40})^{25} \cdot 23^{2} \bmod 41 \\
&= 529 \bmod 41 \\
&= 37 \bmod 41
\end{aligned}
$$

Section 4.5

Ex.6.

$x_1 = (4 \times 3 + 1) \bmod 7 = 6$

$x_2 = (4 \times 6 + 1) \bmod 7 = 4$

$x_3 = (4 \times 4 + 1) \bmod 7 = 3$

$\cancel{x_3}$ and then it starts repeate the number 3, 6, 4 ....

Ex18

a) 7555618873

$X_{11} = 7+5+5+5+6+1+8+8+7+3 \bmod 9$

$= 55 \bmod 9$

$= 1$