Math 255 - Spring 2017
Review Homework Solutions

All problems that are not covered here are covered either in Answers to selected suggested problems 1 (posted on March 1), Answers to selected suggested problems 2 (posted on April 12) or Solutions to suggested problems (posted at the bottom with the final exam material). Please note that some full solutions are sketched out by hand at the end of Answers to selected suggested problems 1 and 2.

Section 3.1

5. (b) If $\gcd(a,b) = p$, then both a and b are divisible by p, but at least one of a or b is not divisible by p^2. Without loss of generality let that one be a, so $a = pN$, with $\gcd(p,N) = 1$, and $b = p^kM$, with $k \geq 1$ and $\gcd(p,M) = 1$. Furthermore since $\gcd(a,b) = p$, $\gcd(N,M) = 1$ since a and b have no further prime factors in common. Then $a^2 = p^2N^2$, $a^3 = p^3N^3$, and $b^2 = p^{2k}M^2$. Therefore $\gcd(a^2,b^2) = p^2$, $\gcd(a^2,b) = p$ if $k = 1$ or p^2 if $k \geq 2$, and $\gcd(a^3,b^2) = p^2$ if $k = 1$ or p^3 if $k \geq 2$.

Section 4.4

4. Only part (a) has numbers that are reasonable for the final exam.

   (a) We have $a_1 = 1$, $N_1 = 35$ and $x_1 = 2$, $a_2 = 2$, $N_2 = 21$ and $x_2 = 1$, and $a_3 = 3$, $N_3 = 15$ and $x_3 = 1$. Therefore the solution is $x \equiv 70 + 42 + 45 \equiv 157 \equiv 52 \pmod{105}$.

   (b) We have $a_1 = 5$, $N_1 = 899$ and $x_1 = 7$, $a_2 = 14$, $N_2 = 341$ and $x_2 = 4$, and $a_3 = 15$, $N_3 = 319$ and $x_3 = 7$. Therefore the solution is $x \equiv 31465 + 19096 + 33495 \equiv 84056 \equiv 4944 \pmod{9889}$.

   (c) We have $a_1 = 5$, $N_1 = 187$ and $x_1 = 1$, $a_2 = 4$, $N_2 = 102$ and $x_2 = 4$, and $a_3 = 3$, $N_3 = 66$ and $x_3 = 8$. Therefore the solution is $x \equiv 935+1632+1584 \equiv 4151 \equiv 785 \pmod{1122}$.

   (d) First we put the system in the correct form to apply the Chinese Remainder Theorem:

   $$x \equiv 3 \pmod{5}, \quad x \equiv 3 \equiv 1 \pmod{2},$$
   $$x \equiv 2 \pmod{7}, \quad x \equiv 81 \equiv 4 \pmod{11}$$

   (Note that instead of $x \equiv 1 \pmod{2}$, we could put either $x \equiv 1 \pmod{6}$ or $x \equiv 3 \pmod{6}$ or $x \equiv 5 \pmod{6}$ and solve three different Chinese Remainder problems.)
   We have $a_1 = 3$, $N_1 = 154$ and $x_1 = -1$, $a_2 = 1$, $N_2 = 385$ and $x_2 = 1$, $a_3 = 2$,

$N_3 = 110$ and $x_3 = 3$, and $a_4 = 4$, $N_4 = 70$ and $x_4 = 3$. Therefore the solution is $x \equiv -462 + 385 + 660 + 840 \equiv 1423 \equiv 653 \pmod{770}$.
(If we had solve the three Chinese Remainder Theorem problems we would have obtained $653, 1423$ and 2193 modulo 2310, which are the three lifts of the single solution modulo 770 that we obtained. In that sense, the two ways of seeing the problem really give the same solution.)

Section 6.1

19. Since both f and g are multiplicative, whenever $\gcd(m, n) = 1$, we have $f(mn) = f(m)f(n)$ and $g(mn) = g(m)g(n)$. Therefore if $\gcd(m, n) = 1$ we have

$$\begin{aligned} fg(mn) &= f(mn)g(mn) \quad \text{by definition of the function } fg \\ &= f(m)f(n)g(m)g(n) \quad \text{since } f \text{ and } g \text{ are multiplicative} \\ &= f(m)g(m)f(n)g(n) \quad \text{by commutativity of multiplication} \\ &= fg(m)fg(n) \quad \text{by definition of the function } fg \end{aligned}$$

and fg is multiplicative. Similarly

$$\begin{aligned} \frac{f}{g}(mn) &= \frac{f(mn)}{g(mn)} \quad \text{by definition of the function } \frac{f}{g} \\ &= \frac{f(m)f(n)}{g(m)g(n)} \quad \text{since } f \text{ and } g \text{ are multiplicative} \\ &= \frac{f(m)}{g(m)}\frac{f(n)}{g(n)} \quad \text{by commutativity of multiplication} \\ &= \frac{f}{g}(m)\frac{f}{g}(n) \quad \text{by definition of the function } \frac{f}{g} \end{aligned}$$

and $\frac{f}{g}$ is multiplicative as well, assuming that g does not take the value 0.

20. Note that this question requires the definition of τ and its formula in Theorem 6.2, which you are not responsible for. However, given a multiplicative function and a formula for this function (or perhaps after you have been asked to computed a closed formula for the function) you are responsible for being able to solve a problem similar to this problem. In other words, you should know how to show that a function is multiplicative and how to show that two multiplicative functions are equal.

    (a) Let $\gcd(m, n) = 1$. Write $m = p_1^{k_1} \dots p_r^{k_r}$ for the factorization of m into primes. Then $r = \omega(m)$. Similarly, if the factorization of n into primes is $n = q_1^{\ell_1} \dots q_s^{\ell_s}$, $\omega(n) = s$. If $\gcd(m, n) = 1$, then we have $p_i \neq q_j$ for all i and j (none of the primes in the two factorizations coincide). Therefore, the factorization of mn into distinct primes is $p_1^{k_1} \dots p_r^{k_r} q_1^{\ell_1} \dots q_s^{\ell_s}$, and $\omega(mn) = r + s$. (This is because the primes are distinct! Otherwise there would be collapsing. For example, $\omega(2) = 1$

and $\omega(6) = 2$ but $\omega(12) = 2$ since 2 and 6 share a prime factor that gets counted only once in 12.) Therefore

$$2^{\omega(mn)} = 2^{r+s} = 2^r 2^s = 2^{\omega(m)} \cdot 2^{\omega(n)}.$$

(b) We first argue that both $\tau(n^2)$ and $\sum_{d|n} 2^{\omega(d)}$ are multiplicative. For $\sum_{d|n} 2^{\omega(d)}$, we have by part (a) that $2^{\omega(n)}$ is multiplicative, and therefore $\sum_{d|n} 2^{\omega(d)}$ is multiplicative also by the Big Theorem (Theorem 6.4). For $\tau(n^2)$, we note that if $\gcd(m, n) = 1$, then $\gcd(m^2, n^2) = 1$ as well. Therefore

$$\tau((mn)^2) = \tau(m^2n^2) = \tau(m^2)\tau(n^2).$$

Now if two functions are multiplicative, as shown in the homework it suffices to show that they agree on prime powers to show that they always agree. Therefore let p be a prime and $k \geq 1$ be an integer. We have

$$\begin{aligned}\sum_{d|p^k} 2^{\omega(d)} &= \sum_{j=0}^{k} 2^{\omega(p^j)} \\ &= 1 + k \cdot 2 \quad \text{since } 2^{\omega(1)} = 2^0 = 1 \text{ and otherwise } 2^{\omega(p^j)} = 2 \\ &= 2k + 1 \\ &= \tau(p^{2k}) \quad \text{by Theorem 6.2} \\ &= \tau((p^k)^2),\end{aligned}$$

and this completes the proof.

Section 7.2

4. See solutions to Homework 7, problem 3.

Section 8.1

1. See Answers to selected suggested problems 2, but do not forget that to show that a number a has order k, the **most important thing** is to show that no positive integer less than k gives $a^\ell \equiv 1 \pmod{n}$.

Extra problems:

1. To check if 113 is prime, it suffices to check if it is divisible by a prime number that is strictly less than $\sqrt{113}$. Those primes are $2, 3, 5$ and 7. Since the last digits of 113 is 3, we see that it is not divisible by 2 or 5. The sum of the digits of 113 is 5, so 113 is not divisible by 3 either. Finally, $113 = 70 + 43 = 70 + 42 + 1 \equiv 1 \pmod{7}$, so 113 is not divisible by 7 either. Therefore 113 is prime.

2. Since the congruences are not of the form $x \equiv a_i \pmod{n_i}$, we must first write them in that form before applying the Chinese Remainder Theorem recipe. To do that, we will need $2^{-1} \pmod 3$, which is 2, $3^{-1} \pmod 4$, which is 3 and $3^{-1} \pmod 5$, which is 2. (All three of these inverses can either be found by using the Euclidean algorithm as in Exam 1, problem 1b), or by inspection since the modulus of the congruence is so small.)

   Therefore we have

$$\begin{aligned} 2x &\equiv 1 \pmod 3 \\ 2 \cdot 2x &\equiv 2 \cdot 1 \pmod 3 \\ x &\equiv 2 \pmod 3 \end{aligned}$$

   as well as

$$\begin{aligned} 3x &\equiv 2 \pmod 4 \\ 3 \cdot 3x &\equiv 3 \cdot 2 \pmod 4 \\ x &\equiv 2 \pmod 4 \end{aligned}$$

   and

$$\begin{aligned} 3x &\equiv 2 \pmod 5 \\ 2 \cdot 3x &\equiv 2 \cdot 2 \pmod 5 \\ x &\equiv 4 \pmod 5 \end{aligned}$$

   We apply the CRT algorithm to

$$\begin{aligned} x &\equiv 2 \pmod 3 \\ x &\equiv 2 \pmod 4 \\ x &\equiv 4 \pmod 5 \end{aligned}$$

   .

   $\underline{n_1 = 3}$ We have $a_1 = 2$ and $N_1 = 20$. To find x_1 we must solve $N_1 x_1 \equiv 1 \pmod 3$. Since $20 \equiv 2 \pmod 3$, we solve $2x_1 \equiv 1 \pmod 3$, and the solution is $x_1 = 2$.

   $\underline{n_2 = 4}$ We have $a_2 = 2$ and $N_2 = 15$. To find x_2 we must solve $N_2 x_2 \equiv 1 \pmod 4$. Since $15 \equiv 3 \pmod 4$, we solve $3x_2 \equiv 1 \pmod 4$, and the solution is $x_2 = 3$.

   $\underline{n_3 = 5}$ We have $a_3 = 4$ and $N_3 = 12$. To find x_3 we must solve $N_3 x_3 \equiv 1 \pmod 5$. Since $12 \equiv 2 \pmod 5$, we solve $2x_3 \equiv 1 \pmod 5$, and the solution is $x_3 = 3$.

   Putting it all together, the solution is

$$x \equiv 2 \cdot 20 \cdot 2 + 2 \cdot 15 \cdot 3 + 4 \cdot 12 \cdot 3 \equiv 80 + 90 + 144 \equiv 20 + 30 + 24 \equiv 74 \equiv 14 \pmod{60}.$$

3. (a) We have

$$\left(\frac{-157}{241}\right) = \left(\frac{-1}{241}\right) \cdot \left(\frac{157}{241}\right),$$

and we compute each symbol separately.
Since $241 \equiv 1 \pmod 4$, $\left(\frac{-1}{241}\right) = 1$.
For the other symbol we use Quadratic Reciprocity:

$$\left(\frac{157}{241}\right)\left(\frac{241}{157}\right) = (-1)^{(157-1)(241-1)/4} = (-1)^{78\cdot 120} = 1,$$

so $\left(\frac{157}{241}\right)$ and $\left(\frac{241}{157}\right)$ have the same sign.
Now

$$\left(\frac{241}{157}\right) = \left(\frac{84}{157}\right) = \left(\frac{4}{157}\right)\left(\frac{3}{157}\right)\left(\frac{7}{157}\right) = \left(\frac{3}{157}\right)\left(\frac{7}{157}\right),$$

since 4 is a square in the integers, so $\left(\frac{4}{157}\right) = 1$.
The two remaining Legendre symbols are again computed using Quadratic Reciprocity:

$$\left(\frac{3}{157}\right)\left(\frac{157}{3}\right) = (-1)^{(3-1)(157-1)/4} = (-1)^{1\cdot 78} = 1,$$

and

$$\left(\frac{157}{3}\right) = \left(\frac{1}{3}\right) = 1.$$

Therefore

$$\left(\frac{3}{157}\right) = 1.$$

Also,

$$\left(\frac{7}{157}\right)\left(\frac{157}{7}\right) = (-1)^{(7-1)(157-1)/4} = (-1)^{3\cdot 78} = 1,$$

and

$$\left(\frac{157}{7}\right) = \left(\frac{3}{7}\right).$$

This last symbol can be computed by hand since 7 is small, or by using Quadratic Reciprocity one last time:

$$\left(\frac{3}{7}\right)\left(\frac{7}{3}\right) = (-1)^{(3-1)(7-1)/4} = (-1)^{1\cdot 3} = -1,$$

and

$$\left(\frac{7}{3}\right) = \left(\frac{1}{3}\right) = 1.$$

Therefore

$$\left(\frac{3}{7}\right) = -1$$

and

$$\left(\frac{7}{157}\right) = -1.$$

Therefore we have

$$\left(\frac{241}{157}\right) = 1 \cdot -1 = -1,$$

so

$$\left(\frac{157}{241}\right) = -1$$

and in conclusion

$$\left(\frac{-157}{241}\right) = -1.$$

(b) We first factor 177 into primes:

$$\left(\frac{177}{179}\right) = \left(\frac{3}{179}\right)\left(\frac{59}{179}\right).$$

And now we can use Quadratic Reciprocity to compute each symbol. We have

$$\left(\frac{3}{179}\right)\left(\frac{179}{3}\right) = (-1)^{(3-1)(179-1)/4} = (-1)^{1\cdot 89} = -1$$

and

$$\left(\frac{179}{3}\right) = \left(\frac{2}{3}\right) = -1,$$

so

$$\left(\frac{3}{179}\right) = 1.$$

Also,

$$\left(\frac{59}{179}\right)\left(\frac{179}{59}\right) = (-1)^{(59-1)(179-1)/4} = (-1)^{29\cdot 89} = -1,$$

and

$$\left(\frac{179}{59}\right) = \left(\frac{2}{59}\right).$$

Since $59 \equiv 3 \pmod 8$, $\left(\frac{2}{59}\right) = -1$, and

$$\left(\frac{59}{179}\right) = 1.$$

Putting the two together,

$$\left(\frac{177}{179}\right) = 1 \cdot 1 = 1.$$

4. (a) Here $n = 64 = 2^6$. Therefore we solve $x^2 \equiv 17 \equiv 1 \pmod{8}$ and lift from there, using the $p = 2$ lifting technique.

Base case We solve $x^2 \equiv 17 \equiv 1 \pmod{8}$. This has solution $x \equiv 1 \pmod{8}$.

First lift: From modulo 8 to modulo 16 We recall the that the lifting step is peculiar when $p = 2$: We will "lower" our solution $x \equiv 1 \pmod{8}$ to $x \equiv 1 \pmod{4}$ and lift that directly to a solution modulo 16. The lifting equation is therefore

$$x_1 = 1 + 4y_0,$$

and we wish that

$$x_1^2 \equiv 17 \equiv 1 \pmod{16}.$$

We notice in fact that the lift with $y_0 = 0$ works, since $x \equiv 1 \pmod{16}$ is a solution to $x^2 \equiv 1 \pmod{16}$. (This is not the only possible lift, but we only need one to continue.)

Second lift: From modulo 16 to modulo 32 Again we "lower" our solution to $x \equiv 1 \pmod{8}$ and lift from there directly to a solution modulo 32. The lifting equation is

$$x_1 = 1 + 8y_0,$$

and we wish that

$$x_1^2 \equiv 17 \pmod{32}.$$

We have

$$\begin{aligned} x_1^2 &= (1 + 8y_0)^2 \\ &= 1 + 16y_0 + 64y_0^2 \\ &\equiv 1 + 16y_0 \pmod{32}. \end{aligned}$$

Therefore we want to solve

$$17 \equiv 1 + 16y_0 \pmod{32}.$$

It is perhaps easy to see that $y_0 = 1$ does the trick. (But it is not the only solution! Thankfully we only need one lift to continue.) Our lift is therefore $x_1 = 1 + 8y_0 = 9$.

Third lift: From modulo 32 to modulo 64 This time we "lower" our solution to $x \equiv 9 \pmod{16}$ and lift directly to a solution modulo 64. Note that this solution modulo 16 is not the same solution we had earlier. That is normal and this is why we did the step in the middle, to get $x \equiv 9 \pmod{16}$, which really is a solution to $x^2 \equiv 1 \pmod{16}$. The problem is that we had the "wrong" solution earlier, a solution that we couldn't use in our lifting equation. This is why we have to do this weird dance of taking a small step back at the lifting step.

Our lifting equation is

$$x_1 = 9 + 16y_0,$$

and we wish that

$$x_1^2 \equiv 17 \pmod{64}.$$

We have

$$\begin{aligned}x_1^2 &= (9+16y_0)^2\\ &= 81+288y_0+16^2y_0^2\\ &\equiv 17+32y_0 \pmod{64}\end{aligned}$$

Therefore we want to solve

$$17 \equiv 17+32y_0 \pmod{64},$$

which has as one of its solutions $y_0 = 0$ (again, this is not the unique solution but we only need one lift). Therefore the lift is $x_1 = 9$.

Give all solutions Now that we have one solution to $x^2 \equiv 17 \pmod{64}$, namely $x \equiv 9 \pmod{64}$, we can use our Theorem, which says that there are 4 solutions in total, and the other three are $x \equiv -9 \equiv 55 \pmod{64}$, $x \equiv 9+32 \equiv 41 \pmod{64}$ and $x \equiv -41 \equiv 23 \pmod{64}$. Therefore the 4 solutions are $9, 23, 41$ and $55 \pmod{64}$.

(b) In this problem $n = 81 = 3^4$. Therefore we start by solving $x^2 \equiv 34 \equiv 1 \pmod{3}$ and lift from there, using the p odd lifting technique.

Base case We solve $x^2 \equiv 34 \equiv 1 \pmod{3}$. This has solution $x \equiv 1 \pmod{3}$.

First lift: From modulo 3 to modulo 9 This is the normal, vanilla lifting from 3 to 9. Our lifting equation is

$$x_1 = 1+3y_0$$

and we wish that

$$x_1^2 \equiv 34 \equiv 7 \pmod{9}.$$

We have

$$\begin{aligned}x_1^2 &= (1+3y_0)^2\\ &= 1+6y_0+9y_0^2\\ &\equiv 1+6y_0 \pmod{9},\end{aligned}$$

so we must solve

$$7 \equiv 1+6y_0 \pmod{9}.$$

We see that one solution is $y_0 = 1$, and since we only need one solution our lift is $x_1 = 1+3 = 4$. (In this case, this is not the only solution $y_0 \pmod{9}$ to this equation, but this is the only possible lift. This is different than the situation above where there actually are two lifts for each solution.)

Second lift: From modulo 9 to modulo 27 Our lifting equation is

$$x_1 = 4 + 9y_0,$$

and we wish that

$$x_1^2 \equiv 34 \equiv 7 \pmod{27}.$$

We have

$$\begin{aligned} x_1^2 &= (4+9y_0)^2 \\ &= 16 + 72y_0 + 81y_0^2 \\ &\equiv 16 + 18y_0 \pmod{27}, \end{aligned}$$

so we must solve

$$7 \equiv 16 + 18y_0 \pmod{27}.$$

This doesn't have an obvious solution, so we solve it in the traditional way:

$$\begin{aligned} 7 &\equiv 16 + 18y_0 \pmod{27} \\ -9 &\equiv 18y_0 \pmod{27} \\ -1 &\equiv 2y_0 \pmod{3} \\ 2 &\equiv 2y_0 \pmod{3}, \end{aligned}$$

which has solution $y_0 = 1$. Therefore the lift is $x_1 = 4 + 9 = 13$.

Third lift: From modulo 27 to modulo 81 Our lifting equation is

$$x_1 = 13 + 27y_0$$

and we wish that

$$x_1^2 \equiv 34 \pmod{81}.$$

We have

$$\begin{aligned} x_1^2 &= (13+27y_0)^2 \\ &= 169 + 702y_0 + 27^2y_0^2 \\ &\equiv 7 + 54y_0 \pmod{81}, \end{aligned}$$

so we must solve

$$34 \equiv 7 + 54y_0 \pmod{81}.$$

Again the solution is not obvious

$$\begin{aligned} 34 &\equiv 7 + 54y_0 \pmod{81} \\ 27 &\equiv 54y_0 \pmod{81} \\ 1 &\equiv 2y_0 \pmod{3} \end{aligned}$$

and this has solution $y_0 = 2$. Therefore the lift is $x_1 = 13 + 27 \cdot 2 = 13 + 54 = 67$.

Give all solutions Since 81 is a power of an odd prime, there are two solutions and they are $x \equiv 67 \pmod{81}$ and $x \equiv -67 \equiv 14 \pmod{81}$. Therefore the solutions are $x \equiv 14$ and $67 \pmod{81}$.

(c) Here $n = 135 = 3^3 \cdot 5$. Therefore we must solve $x^2 \equiv 59 \equiv 5 \pmod{27}$ and $x^2 \equiv 1 \pmod{5}$.

First equation $x^2 \equiv 5 \pmod{27}$: We must start by solving $x^2 \equiv 5 \equiv 2 \pmod{3}$. This has no solution. Therefore $x^2 \equiv 5 \pmod{27}$ has no solution and $x^2 \equiv 59 \pmod{135}$ has no solution.

(d) For this equation it's easy to see that $x \equiv 5 \pmod{80}$ will be a solution, as well as $x \equiv -5 \equiv 75 \pmod{80}$. However, there might be more solutions that are harder to find; since 80 is not a power of a prime we don't have an easy result giving us all of the solutions in terms of these two solutions and it's faster and safer to just do all our steps.

Since $n = 80 = 2^4 \cdot 5$, we must solve $x^2 \equiv 25 \equiv 9 \pmod{16}$ and $x^2 \equiv 25 \equiv 0 \pmod{5}$.

First equation $x^2 \equiv 9 \pmod{16}$: It is easy to see the solution $x \equiv 3 \pmod{16}$. Since $16 = 2^4$, we know that there are exactly 4 solutions and they are $x \equiv 3 \pmod{16}$, $x \equiv -3 \equiv 13 \pmod{16}$, $x \equiv 3 + 8 \equiv 11 \pmod{16}$ and $x \equiv -3 + 8 \equiv 5 \pmod{16}$.

Second equation $x^2 \equiv 25 \equiv 0 \pmod{5}$: This has as its only solution $x \equiv 0 \pmod{5}$.

Therefore the equation $x^2 \equiv 25 \pmod{80}$ has 4 solutions, and they satisfy:

$$\begin{aligned}
x \equiv 3 \pmod{16} &\quad \text{and} \quad x \equiv 0 \pmod{5},\\
x \equiv 5 \pmod{16} &\quad \text{and} \quad x \equiv 0 \pmod{5},\\
x \equiv 11 \pmod{16} &\quad \text{and} \quad x \equiv 0 \pmod{5},\\
x \equiv 13 \pmod{16} &\quad \text{and} \quad x \equiv 0 \pmod{5},
\end{aligned}$$

respectively. Now it's time for some Chinese Remainder Theorem to figure out what those are modulo 80.

For each of these four CRT problems, we will have $N_1 = 5$ and x_1 will be the solution to $5x_1 \equiv 1 \pmod{16}$. So we find $5^{-1} \pmod{16}$. First we do division: $16 = 3 \cdot 5 + 1$. So $1 = 16 - 3 \cdot 5$ and $5^{-1} \equiv -3 \equiv 13 \pmod{16}$. We will use $x_1 = -3$ because it's a smaller number in absolute value. In all of the CRT problems we will also have $a_2 = 0$, so N_2 and x_2 won't matter.

With this done, it's not so bad to get all of the answers:

For the first solution, $a_1 = 3$, so

$$x \equiv 3 \cdot 5 \cdot (-3) + 0 \equiv -45 \equiv 35 \pmod{80}.$$

For the second solution, $a_1 = 5$, so

$$x \equiv 5 \cdot 5 \cdot (-3) + 0 \equiv -75 \equiv 5 \pmod{80}.$$

For the third solution, $a_1 = 11$, so

$$x \equiv 11 \cdot 5 \cdot (-3) + 0 \equiv -165 \equiv -5 \equiv 75 \pmod{80}.$$

For the last solution, $a_1 = 13$, so

$$x \equiv 13 \cdot 5 \cdot (-3) + 0 \equiv -195 \equiv -35 \equiv 45 \pmod{80}.$$

Therefore the four solutions are $x \equiv 5, 35, 45$ and $75 \pmod{80}$. We note that this is $x \equiv \pm 5 \pmod{40}$ but 40 is not a factor of 80 such that $x^2 \equiv 25 \pmod{40}$ has 2 solutions (the equation has four solutions, $5, 15, 25$ and $35 \pmod{40}$). Therefore the conjecture we made in the last problem of the suggested problems is false as stated.

(e) To solve $x^2 + 20x + 30 \equiv 0 \pmod{105}$, we use the quadratic formula:

$$x \equiv \frac{-b + \text{``}\sqrt{b^2 - 4ac}\text{''}}{2a} \equiv \frac{-20 + \text{``}\sqrt{20^2 - 4 \cdot 30}\text{''}}{2} \equiv \frac{-20 + \text{``}\sqrt{280}\text{''}}{2} \pmod{105}.$$

To compute "$\sqrt{280}$" we must find all solutions to $y^2 \equiv 280 \equiv 70 \pmod{105}$. Since $105 = 3 \cdot 5 \cdot 7$, we must solve $y^2 \equiv 70 \equiv 1 \pmod{3}$, $y^2 \equiv 70 \equiv 0 \pmod{5}$ and $y^2 \equiv 70 \equiv 0 \pmod{7}$.

These can all be solved by inspection. The first equation has solutions $y \equiv 1 \pmod{3}$ and $y \equiv 2 \pmod{3}$, the second equation has solution $y \equiv 0 \pmod{5}$ and the last equation has solution $y \equiv 0 \pmod{7}$. Therefore $y^2 \equiv 70 \pmod{105}$ has 2 solutions, and they satisfy

$$\begin{aligned} y &\equiv 1 \pmod{3}, \quad y \equiv 0 \pmod{5}, \quad \text{and} \quad y \equiv 0 \pmod{7}, \\ y &\equiv 2 \pmod{3}, \quad y \equiv 0 \pmod{5}, \quad \text{and} \quad y \equiv 0 \pmod{7}, \end{aligned}$$

respectively.

We use the Chinese Remainder Theorem to obtain the solution modulo 105. For both of the problems we will have $N_1 = 35$ and x_1 such that $35x_1 \equiv 1 \pmod{3}$, or $2x_1 \equiv 1 \pmod{3}$. The solution is $x_1 = 2$. Also for both of the problems we will have $a_2 = a_3 = 0$, so we will not need to worry about N_2, x_2, N_3 or x_3.

Now we get the answers, the first one has $a_1 = 1$, so

$$y \equiv 1 \cdot 35 \cdot 2 + 0 + 0 \equiv 70 \pmod{105}.$$

The second has $a_1 = 2$, so

$$y \equiv 2 \cdot 35 \cdot 2 + 0 + 0 \equiv 140 \equiv 35 \pmod{105}.$$

We now plug these into the quadratic formula. The first solution is

$$x \equiv \frac{-20 + 70}{2} \equiv \frac{50}{2} \equiv 25 \pmod{105}$$

and the second solution is

$$x \equiv \frac{-20+35}{2} \equiv \frac{15}{2} \pmod{105}.$$

To perform the division by 2 we must find $2^{-1} \pmod{105}$. Since $2 \cdot 53 = 106 \equiv 1 \pmod{105}$, $2^{-1} \equiv 53 \pmod{105}$. Therefore the second solution is

$$x \equiv 15 \cdot 53 \equiv 945 \equiv 60 \pmod{105}.$$

The two solutions are therefore $x \equiv 25 \pmod{105}$ and $x \equiv 60 \pmod{105}$.

Section 4.4

#4 a) $a_1 = 1$ $N_1 = 35$ $35x_1 \equiv 1 \bmod 3$

$2x_1 \equiv 1 \bmod 3$ $x_1 = 2$

$a_2 = 2$ $N_2 = 21$ $21x_2 \equiv 1 \bmod 5$

$x_2 \equiv 1 \bmod 5$ $x_2 = 1$

$a_3 = 3$ $N_3 = 15$ $15x_3 \equiv 1 \bmod 7$

$x_3 \equiv 1 \bmod 7$ $x_3 = 1$

b) $a_1 = 5$ $N_1 = 899$ $899x_1 \equiv 1 \bmod 11$

$8x_1 \equiv 1 \bmod 11$ $x_1 = 7$

$8 \cdot 7 \equiv 56 \equiv 1 \bmod 11$

$a_2 = 14$ $N_2 = 341$ $341x_2 \equiv 1 \bmod 29$

$22x_2 \equiv 1 \bmod 29$

$29 = 22 + 7$
$22 = 3 \cdot 7 + 1$

$1 = 22 - 3 \cdot 7$
$= 22 - 3(29 - 22)$
$= 4 \cdot 22 - 3 \cdot 29$

$x_2 = 4$

$a_3 = 15$ $N_3 = 319$ $319x_3 \equiv 1 \bmod 31$

$9x_3 \equiv 1 \bmod 31$

$31 = 3 \cdot 9 + 4$
$9 = 2 \cdot 4 + 1$

$1 = 9 - 2 \cdot 4$
$= 9 - 2(31 - 3 \cdot 9)$
$= 7 \cdot 9 - 2 \cdot 31$

$x_3 = 7$

c) $a_1=5$ $N_1=187$ $187x_1\equiv 1 \bmod 6$

$x_1\equiv 1 \bmod 6$ $x_1=1$

$a_2=4$ $N_2=102$ $102x_2\equiv 1 \bmod 11$

$3x_2\equiv 1 \bmod 11$

$3\cdot 4\equiv 12\equiv 1 \bmod 11$ $x_2=4$

$a_3=3$ $N_3=66$ $66x_3\equiv 1 \bmod 17$

$15x_3\equiv 1 \bmod 17$ $x_3=8$

$(-2)(-9)=18\equiv 1 \bmod 17$

$15\cdot 8\equiv 1 \bmod 17$

d) $a_1=3$ $N_1=154$ $154x_1\equiv 1 \bmod 5$ $x_1=-1$

$4x_1\equiv 1 \bmod 5$

$a_2=1$ $N_2=385$ $385x_2\equiv 1 \bmod 2$ $x_2=1$

$x_2\equiv 1 \bmod 2$

$a_3=2$ $N_3=110$ $110x_3\equiv 1 \bmod 7$

$5x_3\equiv 1 \bmod 7$

$x_3=3$

$7=5+2$ $1=5-2\cdot 2$

$5=2\cdot 2+1$ $=5-2\cdot(7-5)$

$=3\cdot 5-2\cdot 7$

$a_4=4$ $N_4=70$ $70x_4\equiv 1 \bmod 11$

$4x_4\equiv 1 \bmod 11$ $x_4=3$

$4\cdot 3=12\equiv 1 \bmod 11$