Solutions to Homework 3

§1.3 #14. *Prove that if* $x^2 \equiv n \pmod{65}$ *has a solution, then so does* $x^2 \equiv -n \pmod{65}$.

Observe that

$$8^2 = 64 \equiv -1 \pmod{65}.$$

Thus if $x^2 \equiv n \pmod{65}$ then $(8x)^2 = 64x^2 \equiv -n \pmod{65}$.

§1.3 #21.

a. $x \equiv 1 \pmod 3$ *and* $x \equiv 1 \pmod 5$.

We can just eyeball this one: $x \equiv 1 \pmod{15}$.

b. $x \equiv 1 \pmod 4$ *and* $x \equiv 7 \pmod{13}$.

We can write $1 = 1 \cdot 13 - 3 \cdot 4$, so the formula in Theorem 3.7 gives

$$x \equiv 1 \cdot 1 \cdot 13 - 7 \cdot 3 \cdot 4 \equiv -71 \pmod{52},$$

but it would be nicer to say

$$x \equiv 33 \pmod{52}.$$

c. $x \equiv 3 \pmod 4$ *and* $x \equiv 4 \pmod 5$ *and* $x \equiv 3 \pmod 7$.

First we solve the first pair of congruences. We could rewrite them as $x \equiv -1 \pmod 4$ and $x \equiv -1 \pmod 5$, so we can eyeball the solution as $x \equiv -1 \pmod{20}$. Or we could just apply the formula: write $1 = 5 - 4$, so $x \equiv 3 \cdot 5 - 4 \cdot 4 \equiv -1 \pmod{20}$.

Next we solve $x \equiv -1 \pmod{20}$ and $x \equiv 3 \pmod 7$. Write $1 = 3 \cdot 7 - 20$, so

$$x \equiv (-1) \cdot 3 \cdot 7 - 3 \cdot 20 \equiv -81 \pmod{140},$$

but it would be nicer to say

$$x \equiv 59 \pmod{140}.$$

d. $19x \equiv 1 \pmod{140}$.

We could just write $1 = 59 \cdot 19 - 8 \cdot 140$, so $59 \cdot 19 \equiv 1 \pmod{140}$, so multplying through by 59 we get $x \equiv 59 \pmod{140}$.

But if we want to follow the hint and use the Chinese Remainder Theorem, we could observe that $140 = 4 \cdot 5 \cdot 7$, so if $19x \equiv 1 \pmod{140}$ then

$$3x \equiv 1 \pmod{4} \qquad 4x \equiv 1 \pmod{5} \qquad 5x \equiv 1 \pmod{7}.$$

Solving each of these we find that

$$x \equiv 3 \pmod{4} \qquad x \equiv 4 \pmod{5} \qquad x \equiv 3 \pmod{7}.$$

In part c we saw that the solution to this is $x \equiv 59 \pmod{140}$.

e. $x \equiv 3 \pmod{9}$ *and* $x \equiv 18 \pmod{24}$.

The greatest common divisor of 9 and 24 is 3, and their least common multiple is 72. We see that $3 \equiv 18 \pmod{3}$, so the problem can be solved. We can write $3 - 18 = (-5) \cdot 3$ and $3 = 3 \cdot 9 - 24$, so the formula in Theorem 3.8 gives

$$x \equiv (-5) \cdot (-24) + 18 \equiv 138 \pmod{72},$$

but it would be nicer to say

$$x \equiv 66 \pmod{72}.$$

f. $x \equiv 4 \pmod{105}$ *and* $x \equiv 29 \pmod{80}$.

The greatest common divisor of 105 and 80 is 5, and their least common multiple is 1680. We see that $4 \equiv 29 \pmod{5}$, so the problem can be solved. We can write $4 - 29 = (-5) \cdot 5$ and $5 = 4 \cdot 80 - 3 \cdot 105$, so the formula in Theorem 3.8 gives

$$x \equiv (-5) \cdot 4 \cdot 80 + 29 \equiv -1571 \pmod{1680},$$

but it would be nicer to say

$$x \equiv 109 \pmod{1680}.$$

g. $x \equiv 11 \pmod{142}$ *and* $x \equiv 25 \pmod{86}$.

The greatest common divisor of 142 and 86 is 2, and their least common multiple is 6106. We see that $11 \equiv 25 \pmod 2$, so the problem can be solved. We can write $11-25 = (-7)\cdot 2$ and $2 = 20\cdot 142 - 33\cdot 86$, so the formula in Theorem 3.8 gives

$$x \equiv (-7)\cdot(-33)\cdot 86 + 25 \equiv 19891 \pmod{6106},$$

but it would be nicer to say

$$x \equiv 1573 \pmod{6106}.$$

§1.3 #23. *If a is selected at random from 1, 2, …, 11, and b is selected at random from 1, 2, …, 12, what is the probability that $ax \equiv b \pmod{12}$ has at least one solution?*

From what we proved in lecture, and what you read at the top of page 26, we know that the equation $ax \equiv b \pmod{12}$ has a solution if and only if b is a multiple of $\gcd(a, 12)$. The values of a and b for which this is true are indicated with $\times$:

	$b=1$	2	3	4	5	6	7	8	9	10	11	12
$a=1$	$\times$	$\times$	$\times$	$\times$	$\times$	$\times$	$\times$	$\times$	$\times$	$\times$	$\times$	$\times$
2		$\times$		$\times$		$\times$		$\times$		$\times$		$\times$
3			$\times$			$\times$			$\times$			$\times$
4				$\times$				$\times$				$\times$
5	$\times$	$\times$	$\times$	$\times$	$\times$	$\times$	$\times$	$\times$	$\times$	$\times$	$\times$	$\times$
6						$\times$						$\times$
7	$\times$	$\times$	$\times$	$\times$	$\times$	$\times$	$\times$	$\times$	$\times$	$\times$	$\times$	$\times$
8				$\times$				$\times$				$\times$
9			$\times$			$\times$			$\times$			$\times$
10		$\times$		$\times$		$\times$		$\times$		$\times$		$\times$
11	$\times$	$\times$	$\times$	$\times$	$\times$	$\times$	$\times$	$\times$	$\times$	$\times$	$\times$	$\times$

Counting up the rows, we find $12+6+4+3+12+2+12+3+4+6+12 = 76$ values of a and b for which the equation can be solved, out of $11\cdot 12 = 132$ possible values, so the probability is

$$76/132 \approx 57.6\%.$$