

Name:

**Problem 1:** Please solve the following set of simultaneous linear congruences:

$$x \equiv 1 \pmod{3}$$

$$x \equiv 2 \pmod{5}$$

$$x \equiv 3 \pmod{7}.$$

**Solution:** This problem is already in the correct form where each equation looks like  $x \equiv a_i \pmod{n_i}$  and all of the  $n_i$ s are pairwise relatively prime. Therefore we can say immediately that

$$a_1 = 1, \quad n_1 = 3, \quad \text{and} \quad N_1 = 35$$

$$a_2 = 2, \quad n_2 = 5 \quad \text{and} \quad N_2 = 21$$

$$a_3 = 3, \quad n_3 = 7 \quad \text{and} \quad N_3 = 15.$$

We just need to compute the  $x_i$ s and then we will be ready to put the solution together.

To compute  $x_1$ , we must find an integer such that  $x_1 N_1 \equiv 1 \pmod{n_1}$ , or, plugging in our values,  $35x_1 \equiv 1 \pmod{3}$ . Since  $35 \equiv 2 \pmod{3}$ , this is the same as solving  $2x_1 \equiv 1 \pmod{3}$ . By trying  $x_1 = 0, 1, 2$  (which are the only distinct values that  $x_1$  can take modulo 3) we see that  $x_1 = 2$ .

We now compute  $x_2$ . We solve  $x_2 N_2 \equiv 1 \pmod{n_2}$  or  $21x_2 \equiv 1 \pmod{5}$ . Since  $21 \equiv 1 \pmod{5}$ , this is just  $x_2 \equiv 1 \pmod{5}$ , and we can take  $x_2 = 1$ .

Finally we find  $x_3$ . The equation  $x_3 N_3 \equiv 1 \pmod{n_3}$  here is  $15x_3 \equiv 1 \pmod{7}$ . Since  $15 \equiv 1 \pmod{7}$ , the equation is just  $x_3 \equiv 1 \pmod{7}$  and we can take  $x_3 = 1$ .

Now the solution of this simultaneous set of congruences is

$$\begin{aligned} x &\equiv a_1 x_1 N_1 + a_2 x_2 N_2 + a_3 x_3 N_3 \pmod{n_1 n_2 n_3} \\ &\equiv 1 \cdot 2 \cdot 35 + 2 \cdot 1 \cdot 21 + 3 \cdot 1 \cdot 15 \pmod{3 \cdot 5 \cdot 7} \\ &\equiv 70 + 42 + 45 \pmod{105} \\ &\equiv 157 \pmod{105} \\ &\equiv 52 \pmod{105}. \end{aligned}$$

We can quickly check our answer: Indeed  $52 \equiv 1 \pmod{3}$ ,  $52 \equiv 2 \pmod{5}$  and  $52 \equiv 3 \pmod{7}$ .