Math 221-001 201710
Assignment # 7 - Answers

1. Solve the following simultaneous congruences.

(a)
$$\begin{aligned} x &\equiv 46 \pmod{51} \\ x &\equiv 27 \pmod{52} \end{aligned}$$

Answer. The Chinese Remainder Theorem guarantees that the solution exists, because $\gcd(51, 52) = 1$, If x is a solution, the first congruence tells us that $x = 46 + 51k$, with $k \in \mathbb{Z}$. From the second congruence, we get that $46 + 51k = 27 + 52h$, with $h \in \mathbb{Z}$. This equation we can write as $19 = 52h + 51(-k)$. This is a Diophantine equation, and its solutions are $h = 19 + 51n$, $-k = -19 - 52n$, with $n \in \mathbb{Z}$ (recall that 51 and 52 are coprime). So the general solution is given by $x = 27 + 52(19 + 51n) = 1015 + 51 \times 52n = 1015 + 2652n$, $n \in \mathbb{Z}$.

(b)
$$\begin{aligned} 2x &\equiv 11 \pmod{13} \\ 3x &\equiv 7 \pmod{10} \\ 7x &\equiv 5 \pmod{8} \end{aligned}$$

Answer. Notice that in the three equations the coefficient is coprime with the modulus. This means that they are all invertible. We have $2 \times 7 \equiv 1 \pmod{13}$, $3 \times 7 \equiv 1 \pmod{10}$, $7 \times 7 \equiv 1 \pmod{8}$. So, multiplying the equations by 7, 3, and 7 respectively, we get the new system of equations (completely equivalent to the original)

$$\begin{aligned} x &\equiv 12 \pmod{13} \\ x &\equiv 9 \pmod{10} \\ x &\equiv 3 \pmod{8} \end{aligned}$$

The second equation is particularly easy because its solutions are the integers ending in 9. If we then go to the third equation and try multiples of 8 plus 3, we quickly find that 59 is a solution to both equations. The least common multiple between $8 (= 2^3)$ and $10 (= 2 \times 5)$ is $2^3 \times 5 = 40$. So any solution of the second and third equations is of the form $59 + 40n$, $n \in \mathbb{Z}$ (the Chinese Remainder Theorem guarantees that we are not missing any solutions). To find which of these are also solutions of the first equation, use again a Diophantine equation: solutions of the first equation are of the form $12 + 13k$. So we want to find n, k with $12 + 13k = 59 + 40n$. That is, we need to solve the equation $47 = 13k + 40(-n)$. As $3 \times 13 = 39$, we have $1 = (-3) \times 13 + 40$, so $47 = (-141)13 + 47 \times 40$. So our general solution will be $k = -141 + 40m$, $-n = 47 - 13m$. From here we get $x = 12 + 13k = 12 + 13(-141 + 40m) = -1821 + 520m$, $m \in \mathbb{Z}$. The solutions won't change if we add multiples of 520, so we can also write the general solution as $259 + 520m$ (note that $259 = 4 \times 520 + (-1821)$).

2. Find all integers in the range 1000-4000 satisfying the simultaneous congruences:

$$\begin{aligned} x &\equiv 2 \pmod 7 \\ x &\equiv 5 \pmod{11} \\ x &\equiv 11 \pmod{17} \end{aligned}$$

Answer. The first two congruences can be easily solved together, because a quick glance shows that 16 is a solution. Then the general solution for first and second together is $x = 16+77n$ ($77 = 7\times 11$). Now we need to find which of those solutions are also solutions of the third congruence. For that we must have $16+77n = 11+17k$. This leads us to consider the equation $5 = 17k + 77(-n)$. Since 17 and 77 are coprime, the equation has solutions. Using the Euclidean Algorithm:

1	0	77	
0	1	17	4
1	−4	9	1
−1	5	8	1
2	−9	1	

we find that $1 = (-9)\times 17 + 2\times 77$, so $5 = (-45)\times 17 + 10\times 77$. So in general $k = -45+77m$, $-n = 10-17m$. Then the solution of the triple multiple congruence must be $x = 11 + 17(-45 + 77m) = -754 + 1309m$, $m \in \mathbb{Z}$. To get a nicer looking answer we can add 1309 to get $x = 555 + 1309m$, $m \in \mathbb{Z}$.

The question asks only for the values between 1000 and 4000. So we need

$$555 + 1309m \geq 1000, \quad \text{i.e.} \quad m \geq (1000 - 555)/1309 \simeq 0.34,$$

so $m \geq 1$. We also need

$$555 + 1309m \leq 4000, \quad \text{i.e.} \quad m \leq (4000 - 555)/1309 \simeq 2.63$$

so $m \leq 2$. We have shown that the only values of m that produce solutions in our range are $m = 1$ and $m = 2$. So the integers we are looking for are

$$555 + 1309 = 1864, \quad 555 + 2\times 1309 = 3173.$$

3. Prove that $21|(3n^7 + 7n^3 + 11n)$ for every integer n.

   Answer. By Fermat's Little Theorem, $[n^7]_7 = [n]_7$. This means that $n^7 - n = 7k$ for a certain integer k. Multiplying by 3, we get that $3n^7 - 3n = 3\times 7k = 21k$, so $[3n^7]_{21} = [3n]_{21}$. Similarly, $[n^3]_3 = [n]_3$, and we conclude that $[7n^3]_{21} = [7n]_{21}$. Using this information, we have

$$\begin{aligned} [3n^7 + 7n^3 + 11n]_{21} &= [3n^7]_{21} + [7n^3]_{21} + [11n]_{21} \\ &= [3n]_{21} + [7n]_{21} + [11n]_{21} \\ &= [3n + 7n + 11n]_{21} = [21n]_{21} = [0]. \end{aligned}$$

4. Let $\phi(m)$ be the Euler phi-function. Show that

(a) $\phi(m) = \phi(2m)$ if and only if m is odd.

Answer. Suppose first that m is odd. Then 2 and m are coprime, since $m = 2k + 1$ for some $k \in \mathbb{Z}$, and so $1 = m + (-k)2$. Then

$$\phi(2m) = \phi(2)\phi(m) = 1\phi(m) = \phi(m).$$

If m is even, then m has prime decomposition $m = 2^{r_1}p_2^{r_2}\cdots p_k^{r_k}$. Then

$$\phi(m) = m(1-1/2)(1-1/p_2)\cdots(1-1/p_k) \neq 2m(1-1/2)(1-1/p_2) = \phi(2m).$$

This shows that if $\phi(m) = \phi(2m)$, then m cannot be even, i.e. it is odd.

(b) $\phi(m) = m - 1$ if and only if m is prime.

Answer. If m is prime, then every number in $\{1, 2, \ldots, m-1\}$ is coprime with m: so $\phi(m) = m - 1$. Conversely, if $\phi(m) = m - 1$, this means that every number in the list $\{1, 2, \ldots, m-1\}$ has to be coprime with m (because there are precisely $m - 1$ numbers in the list, so there is no room for other numbers that would eventually be not coprime with m). In other words, the only numbers between 1 and m that divide m have to be 1 and m, implying that m is prime.

5. Find the remainder when $2^{(2^{100})}$ is divided by 29.

Answer. By Euler–Fermat, we have $2^{28} \equiv 1 \pmod{29}$. So we want to write $2^{100} = 28n + r$. To find r, we need to solve the congruence

$$r \equiv 2^{100} \pmod{28}.$$

As $28 = 4 \times 7$ and $(4, 7 = 1$, this congruence is equivalent to

$$\begin{cases} r \equiv 2^{100} \pmod 4 \\ r \equiv 2^{100} \pmod 7 \end{cases}$$

For the first congruence, since $2^2 \equiv 0 \pmod 4$, we get $r \equiv 0 \pmod 4$. For the second congruence, $2^3 \equiv 1 \pmod 7$, so $2^{100} = 2 \times 2^{99} \equiv 2 \pmod 7$. In other words, we need to solve

$$\begin{cases} r \equiv 0 \pmod 4 \\ r \equiv 2 \pmod 7 \end{cases}$$

So $r = 4a = 2 + 7b$, which leads us to $2 = 4a - 7b$. This is easily satisfied with $a = 4$, $b = 2$. Then, in general, $a = 4 + 7n$, and so $r = 4a = 16 + 28n$, i.e. $r \equiv 16 \pmod{28}$. Back to the original equation,

$$2^{2^{100}} = 2^{28n+16} = (2^{28})^n 2^{16} \equiv 2^{16} \pmod{29}$$

$$= 2^5 2^5 2^5 2 = \equiv 3 \times 3 \times 3 \times 2 = 27 \times 2 \pmod{29}$$

$$\equiv -2 \times 2 = -4 \equiv 25 \pmod{29}.$$