

Selected Solution

Sect 3.3, #8: Find all integral solutions or show there are none to the system of congruences:

$$\begin{aligned}x &\equiv 7 \pmod{9} \\x &\equiv 13 \pmod{23} \\x &\equiv 1 \pmod{2}\end{aligned}$$

Method 1: Since $x \equiv 7 \pmod{9}$, we know that $x = 7 + 9k_1$ for some integer k_1 . We plug this into the second equation to get $7 + 9k_1 \equiv 13 \pmod{23}$. This can be reduced to $9k_1 \equiv 6 \pmod{23}$. We can solve this by using the Euclidean algorithm:

$$\begin{aligned}A : 23k_1 &\equiv 23 \pmod{23} \\B : 9k_1 &\equiv 6 \pmod{23} \\C = A - 2B : 5k_1 &\equiv 11 \pmod{23} \\D = B - C : 4k_1 &\equiv -5 \pmod{23} \\E = C - D : k_1 &\equiv 16 \pmod{23}\end{aligned}$$

So we know that $k_1 = 16 + 23k_2$ for some integer k_2 .

Plugging this into our x equation gives $x = 7 + 9(16 + 23k_2) = 151 + 207k_2$. We use this in the third equation to get $151 + 207k_2 \equiv 1 \pmod{2}$, which is equivalent to $k_2 \equiv 0 \pmod{2}$. This shows that $k_2 = 2k_3$ for some integer k_3 .

Therefore, $x = 151 + 207(2k_3) = 151 + 414k_3$ for some integer k_3 .

Method 2: We will solve the first two congruences simultaneously. We will use the Euclidean algorithm to find a solution to $9x_1 + 23y_1 = 1$:

$$\begin{aligned}23 &= 9(2) + 5 \\9 &= 5(1) + 4 \\5 &= 4(1) + 1 \implies 9(-5) + 23(2) = 1\end{aligned}$$

From this, we see that the multiplicative inverse of 9 is -5 modulo 23 and the multiplicative inverse of 23 is 2 modulo 9. Then we have

$$x \equiv 7 \cdot (23 \cdot 2) + 13 \cdot (9 \cdot (-5)) \pmod{9 \cdot 23} \implies x \equiv -263 \pmod{207} \equiv 151 \pmod{207}.$$

We now solve this congruence with the third congruence in the original statement. We can quickly see that a solution to $207x_2 + 2y_2 = 1$ is $x_2 = 1$ and $y_2 = -103$. Then we have

$$x \equiv 151 \cdot (2 \cdot -103) + 1 \cdot (207 \cdot 1) \pmod{207 \cdot 2} \implies x \equiv -30899 \pmod{414} \equiv 151 \pmod{414}.$$

Therefore, $x = 151 + 414k$ for some integer k .

Comments:

- Even when you are doing computations, it is important that your presentation is neat and organized.
- My personal preference is for the first method when working by hand as it does not require you to be able to work with large numbers. However, with the second method it is easier to quickly write out the solution once you have the multiplicative inverses. Notice that both methods use the Euclidean algorithm as the main tool (“systematic” methods).
- If you notice that both sides of equation B of the first method are divisible by 3 and that $(3, 23) = 1$, you can divide out the 3 to get $3k_1 \equiv 2 \pmod{23}$. Then if you notice that $2 \equiv -21 \pmod{23}$, you can quickly see that $k_1 \equiv -7 \pmod{23} \equiv 16 \pmod{23}$. The “unsystematic” method is valid, but you must still show some work (see page 69). It is not sufficient to just write $9k_1 \equiv 6 \pmod{23} \implies k_1 \equiv 16 \pmod{23}$.

Web Problem #1: Given an integer n , write out its base-10 expansion as $a_k a_{k-1} \dots a_0$. Show that n is divisible by 11 if and only if

$$(a_0 + a_2 + a_4 + \dots) - (a_1 + a_3 + a_5 + \dots)$$

is divisible by 11.

Proof: Notice that $10 \equiv -1 \pmod{10}$, so that $10^k \equiv (-1)^k \pmod{10}$. Then we can write

$$\begin{aligned} n &= 10^k \cdot a_k + 10^{k-1} \cdot a_{k-1} \dots + 10 \cdot a_1 + a_0 \\ &\equiv (-1)^k a_k + (-1)^{k-1} a_{k-1} + \dots + (-1) a_1 + a_0 \pmod{11} \\ &\equiv (a_0 + a_2 + a_4 + \dots) - (a_1 + a_3 + a_5 + \dots) \pmod{11} \end{aligned}$$

Therefore, both expressions are equivalent modulo 11 so that one is divisible by 11 if and only if the other is divisible by 11.

Comment: There is nothing wrong with the proof I gave in class. This proof turns out to be simpler and demonstrates the use of congruences for proving divisibility.

Web Problem #2b: Find the remainder when 89^{45} is divided by 43 without using Fermat’s Little Theorem.

Proof: We will use the method of successive squares. First notice that $89 \equiv 3 \pmod{43}$ so that we need to compute 3^{45} . We write out 45 as a binary expansion:

$$45 = 32 + 8 + 4 + 1 = 2^5 + 2^3 + 2^2 + 2^0.$$

We now start with 3 and successively square it modulo 43:

$$\begin{aligned}
 3 &= 3^{2^0} \equiv 3 \pmod{43} \\
 3^2 &= 3^{2^1} \equiv 9 \pmod{43} \\
 (3^2)^2 &= 3^{2^2} \equiv 81 \pmod{43} \equiv -5 \pmod{43} \\
 \left((3^2)^2\right)^2 &= 3^{2^3} \equiv 25 \pmod{43} \\
 \left(\left((3^2)^2\right)^2\right)^2 &= 3^{2^4} \equiv 625 \pmod{43} \equiv -20 \pmod{43} \\
 \left(\left(\left((3^2)^2\right)^2\right)^2\right)^2 &= 3^{2^5} \equiv 400 \pmod{43} \equiv 13 \pmod{43}
 \end{aligned}$$

Then we have

$$\begin{aligned}
 89^{45} &\equiv 3^{45} \pmod{43} \\
 &\equiv 3^{2^5} \cdot 3^{2^3} \cdot 3^{2^2} \cdot 3^{2^0} \pmod{43} \\
 &\equiv 13 \cdot 25 \cdot (-5) \cdot 3 \pmod{43} \\
 &\equiv 39 \cdot (-125) \pmod{43} \\
 &\equiv (-4) \cdot 4 \pmod{43} \\
 &\equiv -16 \pmod{43} \\
 &\equiv 27 \pmod{43}
 \end{aligned}$$

Comment: I believe the point of this problem was to compute the residue by hand without performing calculations with very large numbers. If you did this computation with numbers larger than 1000, you may want to do it again for practice.

Web Problem #3: Show that if n is composite and $n > 4$, then $(n-1)! \equiv 0 \pmod{n}$.

Proof: Since n is composite, we can write $n = ab$ with $1 < a \leq b < n$ (we can always order them in this way).

If $a \neq b$, then $1 < a < b < n$ and we see that both a and b appear in the product $(n-1)!$. Therefore, we have $(n-1)! = (ab)k'$ where k' is the product of all the integers between 1 and n except for a and b . This shows that $(n-1)! = nk$, so that $(n-1)! \equiv 0 \pmod{n}$.

If $a = b$, then $n = a^2$. Notice that $n > 4$ implies that $a > 2$. This means $1 < a < 2a < n$, so that $(n-1)! = (a \cdot 2a)k'$ where k' is the product of all the integers between 1 and n except for a and $2a$. Then we have $(n-1)! = 2nk$, which shows $(n-1)! \equiv 0 \pmod{n}$.