CS 70 Discrete Mathematics and Probability Theory
Summer 2021 DIS 2C

# 1 Modular Practice

Solve the following modular arithmetic equations for $x$ and $y$.

(a) $9x+5 \equiv 7 \pmod{11}$.

(b) Show that $3x+15 \equiv 4 \pmod{21}$ does not have a solution.

(c) The system of simultaneous equations $3x+2y \equiv 0 \pmod{7}$ and $2x+y \equiv 4 \pmod{7}$.

(d) $13^{2019} \equiv x \pmod{12}$.

(e) $7^{21} \equiv x \pmod{11}$.

**Solution:**

(a) Subtract 5 from both sides to get:

$$9x \equiv 2 \pmod{11}.$$

Now since $\gcd(9,11)=1$, 9 has a (unique) inverse mod 11, and since $9 \times 5 = 45 \equiv 1 \pmod{11}$ the inverse is 5. So multiply both sides by $9^{-1} \equiv 5 \pmod{11}$ to get:

$$x \equiv 10 \pmod{11}.$$

(b) Subtract 15 from both sides to get:

$$3x \equiv 10 \pmod{21}.$$

Now note that this implies $3x \equiv 1 \pmod{3}$, since 3 divides 21, and the latter equation has no solution, so the former cannot either.

We are using the fact that if $d \mid m$, then $x \equiv y \pmod{m}$ implies $x \equiv y \pmod{d}$ (but not necessarily the other way around). To see this, if $x \equiv y \pmod{m}$, then $m \mid x-y$ (by definition) and so $d \mid x-y$, and hence $x \equiv y \pmod{d}$.

(c) First, subtract the first equation from double the second equation to get:

$$2(2x+y)-(3x+2y) \equiv x \equiv 1 \pmod{7}.$$

Now plug into the second equation to get:

$$2+y \equiv 4 \pmod{7},$$

so the system has the solution $x \equiv 1 \pmod{7}$, $y \equiv 2 \pmod{7}$.

(d) 13 is always 1 mod 12, so 13 to any power mod 12 is 1.

$$13^{2019} \equiv 1^{2019} \equiv 1 \pmod{11}.$$

(e) We can use repeated squaring for this question.

$7^2 \equiv 5 \pmod{11}$

$7^4 \equiv (7^2)^2 \equiv 5^2 \equiv 3 \pmod{11}$

$7^8 \equiv (7^4)^2 \equiv 3^2 \equiv 9 \pmod{11}$

$7^{16} \equiv (7^8)^2 \equiv 9^2 \equiv 4 \pmod{11}$

$7^{21} \equiv (7^{16}) * (7^4) * 7 \equiv 4 * 3 * 7 \equiv 7 \pmod{11}$

A way to avoid repeated squaring for so many times is to use Fermat's Little Theorem (you will learn this very soon) to simplify the exponent. We can rewrite the exponent as $21 = (11-1) \times 2 + 1$ and then directly get $7^{21} \equiv 1^2 * 7 \equiv 7 \pmod{11}$

## 2 When/Why can we use CRT?

Let $a_1, \ldots, a_n, m_1, \ldots, m_n \in \mathbb{Z}$ where $m_i > 1$ and pairwise relatively prime. In lecture, you've constructed a solution to

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ &\vdots \\ x &\equiv a_n \pmod{m_n}. \end{aligned}$$

Let $m = m_1 \cdot m_2 \cdots m_n$.

1. Show the solution is unique modulo $m$. (Recall that a solution is unique modulo $m$ means given two solutions $x, x' \in \mathbb{Z}$, we must have $x \equiv x' \pmod{m}$.)
2. Suppose $m_i$'s are not pairwise relatively prime. Is it guaranteed that a solution exists? Prove or give a counterexample.
3. Suppose $m_i$'s are not pairwise relatively prime and a solution exists. Is it guaranteed that the solution is unique modulo $m$? Prove or give a counterexample.

**Solution:**

1. Suppose $x, x' \in \mathbb{Z}$ are two solutions to the system of linear congruences. For $1 \leq i \leq n$, we have $x \equiv x' \pmod{m_i}$. Then $m_i \mid x' - x$. Since $m_i$'s are pairwise relatively prime, we have $m \mid x' - x$. Hence $x \equiv x' \pmod{m}$.

2. No. For example, the system

$$x \equiv 1 \pmod 2$$
$$x \equiv 2 \pmod 4$$

doesn't have a solution, since the first congruence says $x$ is odd but the second says $x$ is even.

3. No. For example, consider

$$x \equiv 0 \pmod 4$$
$$x \equiv 0 \pmod 8$$

Then $x = 0$ is a solution. But $x = 8$ is also a solution, and $0 \not\equiv 8 \pmod{32}$.

## 3 Mechanical Chinese Remainder Theorem

In this problem, we will solve for $x$ such that

$$x \equiv 1 \pmod 2$$
$$x \equiv 2 \pmod 3$$
$$x \equiv 3 \pmod 5$$

(a) Find a number $0 \leq b_2 < 30$ such that $b_2 \equiv 1 \pmod 2$, $b_2 \equiv 0 \pmod 3$, and $b_2 \equiv 0 \pmod 5$.

(b) Find a number $0 \leq b_3 < 30$ such that $b_3 \equiv 0 \pmod 2$, $b_3 \equiv 1 \pmod 3$, and $b_3 \equiv 0 \pmod 5$.

(c) Find a number $0 \leq b_5 < 30$ such that $b_5 \equiv 0 \pmod 2$, $b_5 \equiv 0 \pmod 3$, and $b_5 \equiv 1 \pmod 5$.

(d) What is $x$ in terms of $b_2$, $b_3$, and $b_5$? Evaluate this to get a numerical value for $x$.

**Solution:**

(a) (Note that students can use Extended Euclid for bigger numbers like mod 11. ) In order to make sure that $b_2 \equiv 0 \pmod 3$, we just need to make $b_2$ a multiple of 3–so we can start with just $b_2 = 3$. However, we now need to make sure we satisfy $b_2 \equiv 1 \pmod 2$, so we multiply this by $3^{-1} \pmod 2$. Since $3 \equiv 1 \pmod 2$, this is just 1. Thus, we so far have $b_2 = 3 \cdot 1$. We now need to make sure $b_2$ is a multiple of 5 (ie, is equivalent to zero mod 5), so we multiply our current value for $b_2$ by 5. But now we again need to make sure that $b_2$ is still equivalent to 1 mod 2, so we multiply by $5^{-1} \pmod 2$, which will again just be 1. Finally, we get $b_2 = 3 \cdot 1 \cdot 5 \cdot 1 = 15$.

(b) Similar to the previous part, we make $b_3$ just be $2 \cdot (2^{-1} \pmod 3) \cdot 5 \cdot (5^{-1} \pmod 3)$. We have that $2^{-1} \equiv 2 \pmod 3$ and $5^{-1} \equiv 2^{-1} \equiv 2 \pmod 3$, so $b_3 = 2 \cdot 2 \cdot 5 \cdot 2 = 40$. Reducing this to a number modulo 30, we get $b_3 = 10$.

(c) As before, we get $b_5 = 2 \cdot (2^{-1} \pmod 5) \cdot 3 \cdot (3^{-1} \pmod 5)$. Plugging in $2^{-1} \equiv 3 \pmod 5$ and $3^{-1} \equiv 2 \pmod 5$, we get $b_5 = 2 \cdot 3 \cdot 3 \cdot 2 = 36$. Since we want a number modulo 30, we reduce this to $b_5 = 6$.

(d) We went through all the above steps to ensure that $b_2 \equiv 1 \pmod 2$ and has no remainder for $\pmod 3$ and $\pmod 5$, $b_3 \equiv 1 \pmod 3$ and has no remainder for $\pmod 2$ and $\pmod 5$, $b_5 \equiv 1 \pmod 5$ and has no remainder for $\pmod 2$ and $\pmod 3$. So by multiplying coefficients before $b_i$ and adding them together enables us to manipulate the remainders of x in terms of $\pmod 2$, $\pmod 3$, $\pmod 5$ separately without affecting the remainders of others. We can write $x = b_2 + 2b_3 + 3b_5$. This ensures that when we take $x$ modulo 2, we end up getting $x \equiv b_2 + 2b_3 + 3b_5 \equiv 1 + 2(0) + 3(0) \equiv 1 \pmod 2$ as we expected–and similar statements can be made for the other two moduli. Evaluating this numerically, we get that $x = 15 + 2(10) + 3(6) = 53$. Reducing this to a number mod 30, we get $x = 23$.