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 (practice)

Solve for $x \in \mathbb{Z}$ where:

$$x \equiv 2 \pmod 3$$
$$x \equiv 3 \pmod 5$$
$$x \equiv 4 \pmod 7$$

(a) Find the multiplicative inverse of 5×7 modulo 3.

(b) What is the smallest $a \in \mathbb{Z}^+$ such that $5 \mid a$, $7 \mid a$, and $a \equiv 2 \pmod 3$?

(c) Find the multiplicative inverse of 3×7 modulo 5.

(d) What is the smallest $b \in \mathbb{Z}^+$ such that $3 \mid b$, $7 \mid b$, and $b \equiv 3 \pmod 5$?

(e) Find the multiplicative inverse of 3×5 modulo 7.

(f) What is the smallest $c \in \mathbb{Z}^+$ such that $3 \mid c$, $5 \mid c$, and $c \equiv 4 \pmod 7$?

(g) Write down the set of solutions for the system of equations.

Solution:

(a) 2

(b) $5 \times 7 \times ((5 \times 7)^{-1} \times 2 \pmod 3) = 5 \times 7 \times (2 \times 2 \pmod 3) = 35$

(c) 1

(d) $3 \times 7 \times (3 \times 7)^{-1} \times 3 = 3 \times 7 \times 1 \times 3 = 63$

(e) 1

(f) $3 \times 5 \times (3 \times 5)^{-1} \times 4 = 3 \times 5 \times 1 \times 4 = 60$

(g) $x \equiv 35 + 63 + 60 \pmod{3 \cdot 5 \cdot 7}$, so $x \equiv 158 \equiv 53 \pmod{105}$.