MATH 135 Fall 2020: Extra Practice 8

Warm-Up Exercises

WE01. Is 738645899999999324343123 divisible by 11?

Solution. We may simply apply Proposition 9 from the course notes: an integer is divisible by 11 if the difference of the sums of the even and odd digits is divisible by 11.

The even digits are $7+8+4+8+9+9+9+9+3+4+4+1+3 = 78$ and the odd digits are $3+6+5+9+9+9+9+2+2+3+3+2 = 62$. We have $78-62 = 16$ which is not divisible by 11.

Therefore, $11 \nmid 738645899999999324343123$. □

WE02. For each linear congruence, determine the complete solution, if a solution exists.

(a) $3x \equiv 11 \pmod{18}$

Solution. Notice that $\gcd(3, 18) = 3$ and $3 \nmid 11$. Therefore, by LCT, there are no solutions. □

(b) $4x \equiv 5 \pmod{21}$

Solution. Notice that $\gcd(4, 21) = 1$ and $1 \mid 5$. Therefore, LCT guarantees a set of solutions where $x \equiv x_0 \pmod{21}$ for some particular solution x_0.

By inspection, $21 + 4(-4) = 5$, so $4(-4) \equiv 5 \pmod{21}$.

Therefore, the set of solutions is $x \in [-4]_{21} = [17]_{21}$. □

WE03. Complete the addition and multiplication tables for $\mathbb{Z}_5$.

Solution. The elements of $\mathbb{Z}_5$ are $\{[0], [1], [2], [3], [4]\}$:

$+$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$
$[0]$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$
$[1]$	$[1]$	$[2]$	$[3]$	$[4]$	$[0]$
$[2]$	$[2]$	$[3]$	$[4]$	$[0]$	$[1]$
$[3]$	$[3]$	$[4]$	$[0]$	$[1]$	$[2]$
$[4]$	$[4]$	$[0]$	$[1]$	$[2]$	$[3]$

$\times$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$
$[0]$	$[0]$	$[0]$	$[0]$	$[0]$	$[0]$
$[1]$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$
$[2]$	$[0]$	$[2]$	$[4]$	$[1]$	$[3]$
$[3]$	$[0]$	$[3]$	$[1]$	$[4]$	$[2]$
$[4]$	$[0]$	$[4]$	$[3]$	$[2]$	$[1]$

□

WE04. What is the remainder when 14^{43} is divided by 41?

Solution. Since 41 is prime and $41 \nmid 14$, we may apply Fermat's Little Theorem.

$$14^{41-1} = 14^{40} \equiv 1 \pmod{41}$$

Now, simply apply modular arithmetic: $14^2 = 196 \equiv -9 \pmod{41}$, and $14^3 = 14 \cdot 14^2 \equiv 14 \cdot -9 \equiv -3 \pmod{41}$. Finally, $14^{40} \cdot 14^3 = 14^{43} \equiv 1 \cdot -3 \equiv 38 \pmod{41}$. Therefore, the remainder is 38. □

WE05. Solve

$$\begin{aligned} x &\equiv 7 \pmod{11} \\ x &\equiv 5 \pmod{12} \end{aligned}$$

Solution. We apply the Chinese Remainder Theorem since $\gcd(11, 12) = 1$. Solutions to the first equation are $x \equiv 7, 18, 29, 40, 51, 62, 73, 84, 95, 106, 117, 128 \pmod{132}$. Solutions to the second are $x \equiv 5, 17, 29, 41, 53, 65, 77, 89, 101, 113, 125 \pmod{132}$. The unique solution common to these is $x \equiv 29 \pmod{132}$. □

WE06. What is the smallest non-negative integer x such that $2000 \equiv x \pmod{37}$?

Solution. Simply reduce using the division algorithm, which guarantees a minimal non-negative remainder below 37: we have $2000 = 37(54) + 2$, so $2000 \equiv 2 \pmod{37}$. □

Recommended Problems

RP01. Is $27^{129} + 61^{40}$ divisible by 14? Justify your answer.

Solution. We simplify with $27 \equiv -1 \pmod{14}$ and $61 \equiv 5 \pmod{14}$:

$$\begin{aligned} 27^{129} + 61^{40} &\equiv (-1)^{128+1} + (5)^{40} \pmod{14} \\ &\equiv -1 + 5^{32+8} \pmod{14} \end{aligned}$$

Now, we can repeatedly square 5 to calculate 5^{32} and 5^8.

$$\begin{aligned} 5^2 &\equiv 25 \equiv 11 \pmod{14} \\ 5^4 &\equiv 121 \equiv 9 \pmod{14} \\ 5^8 &\equiv 81 \equiv 11 \pmod{14} \\ 5^{16} &\equiv 121 \equiv 9 \pmod{14} \\ 5^{32} &\equiv 81 \equiv 11 \pmod{14} \end{aligned}$$

Substituting back,

$$27^{129} + 61^{40} \equiv -1 + (11)(11) \equiv 120 \equiv 8 \pmod{14}$$

Therefore, the remainder is 8 by CTR, which is not 0, so $14 \nmid (27^{129} + 61^{40})$. □

RP02. Prove Congruence Power (CP): For all positive integers n and integers a and b, if $a \equiv b \pmod{m}$, then $a^n \equiv b^n \pmod{m}$.

Proof. Let a and b be integers congruent mod m. We prove by induction on n. Let $P(n)$ denote the statement that $a^n \equiv b^n \pmod{m}$.

The base case $P(1)$, $a^1 \equiv b^1 \pmod{m}$ follows from the hypothesis.

Now, let k be a positive integer. Suppose $P(k-1)$ holds, that is, $a^{k-1} \equiv b^{k-1} \pmod{m}$. Since $a \equiv b \pmod{m}$, we may write $a = b + pm$ for some integer p. By our inductive hypothesis, we write $a^{k-1} = b^{k-1} + qm$ for some integer q.

Multiplying these equations together,

$$\begin{aligned}(a)(a^{k-1}) &= (b+pm)(b^{k-1}+qm)\\ a^k &= b^k + b^{k-1}pm + bqm + pqm^2\\ a^k - b^k &= (b^{k-1}p + bq + pqm)m\end{aligned}$$

which, since $b^{k-1}p + bq + pqm$ is an integer, implies m divides $a^k - b^k$. By the definition of congruence, $a^k \equiv b^k \pmod{m}$, which is exactly $P(k)$.

Therefore, by induction, $P(n)$ is true for all positive integer n. □

RP03. What is the remainder when 3141^{2001} is divided by 17?

Solution. First, notice that $3141 \equiv 13 \pmod{17}$. We also have that $3141^2 \equiv 13^2 \equiv -1 \pmod{17}$. Therefore, $3141^{2001} \equiv 3141(3141^2)^{1000} \equiv 13(-1)^{1000} \equiv 13 \pmod{17}$. By CTR, the remainder is 13. □

RP04. Solve $49x^{177} + 37x^{26} + 3x^2 + x + 1 \equiv 0 \pmod{7}$.

Solution. First, notice that $49x^{177} \equiv 0 \pmod{7}$ for any integer x since $7 \mid 49$. Also, $37 \equiv 2 \pmod{7}$, so $37x^{26} \equiv 2x^{26} \equiv 2(x^2)^{13} \pmod{7}$ for any integer x. Additionally, by CFlT, $x^7 \equiv x \pmod{7}$ for any integer x, so $2x^{26} \equiv 2x^{7(3)+5} \equiv 2(x^7)^3(x^5) \equiv 2x^8 \equiv 2x^2 \pmod{7}$ for any integer x.

Now, simply test every value of x and find $5x^2 + x$:

$x \pmod 7$	0	1	2	3	4	5	6
$x^2 \pmod 7$	0	1	4	2	2	4	1
$5x^2 \pmod 7$	0	5	6	3	3	6	5
$5x^2 + x \pmod 7$	0	6	1	6	0	4	4

Now, since $-1 \equiv 6 \pmod{7}$, our solutions are $x \equiv 1, 3 \pmod{7}$. □

RP05. Solve

$$\begin{aligned}3x - 2 &\equiv 7 \pmod{11}\\ 5 &\equiv 4x - 1 \pmod{9}\end{aligned}$$

Solution. We can simplify these congruences by CAM to $3x \equiv 9 \pmod{11}$ and $4x \equiv 6 \pmod{9}$. Since 11 is prime, we can apply CD to the first congruence to get $x \equiv 3 \pmod{11}$. Then, $x = 11k + 3$ for some integer k. Substituting,

$$\begin{aligned}4(11k+3) &\equiv 6 \pmod{9}\\ 44k &\equiv -6 \pmod{9}\\ -k &\equiv -6 \pmod{9}\\ k &\equiv 6 \pmod{9}\end{aligned}$$

Therefore, $k = 9n + 6$ for an integer n, and $x = 11(9n+6) + 3 = 99n + 69$. Equivalently, by definition, $x \equiv 69 \pmod{99}$. □

RP06. The Chinese Remainder Theorem deals with the case where the moduli are coprime. We now investigate what happens if the moduli are not coprime.

(a) Consider the following two systems of linear congruences:

$$A: \begin{cases} n \equiv 2 & \pmod{12} \\ n \equiv 10 & \pmod{18} \end{cases} \qquad B: \begin{cases} n \equiv 5 & \pmod{12} \\ n \equiv 11 & \pmod{18} \end{cases}$$

Determine which one has solutions and which one has no solutions. For the one with solutions, give the complete solutions to the system. For the one with no solutions, explain why no solutions exist.

Solution. Consider system A. By definition, numbers n congruent to 10 modulo 18 are of the from $n = 10 + 18k$ for some integer k. Substituting into the first congruence, $10 + 18k \equiv 2 \pmod{12}$, that is, $6k \equiv 4 \pmod{12}$. However, since $\gcd(6, 12) = 6$ and $6 \nmid 4$, there are no valid values of k.

Consider system B. By definition, solutions to the second congruence are of the from $n = 11+18k$ for some integer k. Substituting, $11+18k \equiv 5 \pmod{12}$, that is, $6k \equiv 6 \pmod{12}$. Since $\gcd(6, 12) = 6$ and $6 \mid 6$, a solution exists. By inspection, $k = 1$ is a solution. By LCT, the set of all solutions is given by $\{k \in \mathbb{Z} : k \equiv 1 \pmod{2}\}$. Therefore, values for k are of the form $2m+1$ for some integer m. Backsubstituting, $n = 11 + 18(2m + 1) = 29 + 36m$. Equivalently, the solution set for all n is given by

$$\{n \in \mathbb{Z} : n \equiv 29 \pmod{36}\} \qquad \square$$

(b) Let a_1 and a_2 be integers, and let m_1 and m_2 be positive integers. Consider the following system of linear congruences:

$$S: \begin{cases} n \equiv a_1 & \pmod{m_1} \\ n \equiv a_2 & \pmod{m_2} \end{cases}$$

Using your observations in (a), complete the following two statements. The system S has a solution if and only if $\boxed{a_1 \equiv a_2 \pmod{\gcd(m_1, m_2)}}$. If n_0 is a solution to S, then the complete solution is $\boxed{n \equiv n_0 \pmod{\operatorname{lcm}(m_1, m_2)}}$.

(c) Prove the first statement.

Proof. Let a_1 and a_2 be integers and let m_1 and m_2 be positive integers with GCD d. We prove the biconditional by mutual implication.

($\Rightarrow$) Suppose that $a_1 \equiv a_2 \pmod{d}$. Solutions to the first congruence are of the form $n = a_1 + m_1 x$ for some integer x. However, we may write $a_1 = a_2 + dk$ with integer k, so we have $n = a_2 + dk + m_1 x$. Substituting, $a_2 + dk + m_1 x \equiv a_2 \pmod{m_2}$, that is, $m_1 x \equiv -dk \pmod{m_2}$.

By LCT, this has a solution x_0 because $\gcd(m_1, m_2) = d$ and $d \mid -dk$, and all solutions are given by $x = x_0 + m_2 y$ for some integer y. Backsubstituting, $n = a_1 + m_1(x_0 + m_2 y) = a_1 + m_1 x_0 + m_1 m_2 y$. Therefore, the system S has solutions.

($\Leftarrow$) Suppose that S has a solution. Then, there is some n such that $n = a_1 + m_1 p = a_2 + m_2 q$ for integers p and q. Rearranging, $a_1 - a_2 = m_1 p + m_2 q$. This is an LDE in $a_1 - a_2$. By the LDET, it has solutions if and only if $\gcd(m_1, m_2) \mid (a_1 - a_2)$. This is equivalent by definition to saying $a_1 \equiv a_2 \pmod{d}$. $\square$

RP07. Solve $x^3 \equiv 17 \pmod{99}$.

Solution. We can split the modulus to simplify the problem: $99 = 3 \times 3 \times 11$. By SMT, we can solve three simultaneous congruences. However, since 3 appears twice, those congruences are redundant. Then, we may equivalently solve the simultaneous congruences

$$x^3 \equiv 17 \equiv 2 \pmod{3} \quad \text{and} \quad x^3 \equiv 17 \equiv 6 \pmod{11}$$

For the first congruence, we make a table

$x \pmod 3$	0	1	2
$x^2 \pmod 3$	0	1	1
$x^3 \pmod 3$	0	1	2

and see from the last row that the solution is all x such that $x \equiv 2 \pmod 3$. Repeating for the second congruence, we make a table

$x \pmod{11}$	0	1	2	3	4	5	6	7	8	9	10
$x^2 \pmod{11}$	0	1	4	9	5	3	3	5	9	4	1
$x^3 \pmod{11}$	0	1	8	5	9	4	7	2	6	3	10

and see again in the last row that the solution is all x such that $x \equiv 8 \pmod{11}$. Now, we apply the Chinese Remainder Theorem. There must exist some x_0 so the solution set is all x congruent to x_0 modulo 33.

Note that solutions between 0 and 32 that are congruent to 8 modulo 11 are 8, 19, and 30. Of these, only 8 is congruent to 2 modulo 3. Therefore, the solution is all x such that $x \equiv 8 \pmod{33}$, or, equivalently,

$$x \equiv 8, 41, 74 \pmod{99}$$ □

RP08. Solve $x^2 + 25x \equiv 54 \pmod{63}$.

Solution. First, notice that $x^2 + 25x - 54$ factors as $(x-2)(x+27)$. Split the modulus as $63 = 7 \times 9$, so by SMT, we can solve two simultaneous congruences:

$$(x-2)(x+27) \equiv 0 \pmod 7 \qquad (x-2)(x+27) \equiv 0 \pmod 9$$

Since $-27 \equiv 1 \pmod 7$ and $-27 \equiv 0 \pmod 9$, we can equivalently write $x \equiv 1, 2 \pmod 7$ and $x \equiv 0, 2 \pmod 9$.

Now, since 7 and 9 are coprime, we take all combinations of the above and apply CRT to each pair, obtaining the set of solutions:

- If $x \equiv 1 \pmod 7$ and $x \equiv 0 \pmod 9$, then $x \equiv 36 \pmod{63}$
- If $x \equiv 1 \pmod 7$ and $x \equiv 2 \pmod 9$, then $x \equiv 29 \pmod{63}$
- If $x \equiv 2 \pmod 7$ and $x \equiv 0 \pmod 9$, then $x \equiv 9 \pmod{63}$
- If $x \equiv 2 \pmod 7$ and $x \equiv 2 \pmod 9$, then $x \equiv 2 \pmod{63}$

Therefore, by CRT, $x \equiv 2, 9, 29, 36 \pmod{63}$ are the only solutions. □

RP09. Find the smallest positive integer a such that $5n^{13} + 13n^5 + a(9n) \equiv 0 \pmod{65}$ for all integers n.

Solution. Let n be an integer. Since $65 = 5 \times 13$, we split the congruence with SMT:

$$\begin{aligned} 5n^{13} + 13n^5 + a(9n) &\equiv 0 \pmod 5 \\ 3n^5 + a(4n) &\equiv 0 \pmod 5 \end{aligned} \qquad \begin{aligned} 5n^{13} + 13n^5 + a(9n) &\equiv 0 \pmod{13} \\ 5n^{13} + a(9n) &\equiv 0 \pmod{13} \end{aligned}$$

Now, we apply CFℓT to both congruences to obtain

$$\begin{aligned} 3n + a(4n) &\equiv 0 \pmod 5 \\ (3 + 4a)n &\equiv 0 \pmod 5 \end{aligned} \qquad \begin{aligned} 5n + a(9n) &\equiv 0 \pmod{13} \\ (5 + 9a)n &\equiv 0 \pmod{13} \end{aligned}$$

This has a trivial solution when $n \equiv 0 \pmod{65}$, but since n is arbitrary, we must otherwise have that $3 + 4a \equiv 0 \pmod 5$ and $5 + 9a \equiv 0 \pmod{13}$ by CAD. We solve the simultaneous congruence

$$4a \equiv 2 \pmod 5 \qquad 9a \equiv 8 \pmod{13}$$

noting that since 5 and 13 are prime, solutions exist. In fact, we can bruteforce to find $a \equiv 3 \pmod 5$ and $a \equiv 11 \pmod{13}$. Then, by the CRT, $a \equiv 63 \pmod{65}$ and the smallest positive such integer is $a = 63$. □

RP10. Prove that for distinct primes p and q, $(p^{q-1} + q^{p-1}) \equiv 1 \pmod{pq}$.

Proof. Let p and q be distinct primes. Since $q - 1$ and $p - 1$ are positive integers, p^{q-1} is a multiple of p and q^{p-1} of q. By definition, $p^{q-1} \equiv 0 \pmod p$ and $q^{p-1} \equiv 0 \pmod q$. Since $p \nmid q$ and $q \nmid p$, by FℓT, we have $q^{p-1} \equiv 1 \pmod p$ and $p^{q-1} \equiv 1 \pmod q$. Therefore, by CAM, we have the simultaneous congruences

$$\begin{aligned} \left(p^{q-1} + q^{p-1}\right) &\equiv 1 \pmod p \\ \left(p^{q-1} + q^{p-1}\right) &\equiv 1 \pmod q \end{aligned}$$

As distinct primes, $\gcd(p, q) = 1$. Then, by SMT, $(p^{q-1} + q^{p-1}) \equiv 1 \pmod{pq}$. □

RP11. If a and b are integers, $3 \nmid a$, $3 \nmid b$, $5 \nmid a$, and $5 \nmid b$, prove that $a^4 \equiv b^4 \pmod{15}$

Proof. Let x be an integer where $3 \nmid x$ and $5 \nmid x$. We exhaust possibilities for $x \pmod{15}$:

$x \pmod{15}$	1	2	4	7	8	11	13	14
$x^2 \pmod{15}$	1	4	1	4	4	1	4	1
$x^4 \pmod{15}$	1	1	1	1	1	1	1	1

Therefore, for any integer x neither a multiple of 3 nor 5, $x^4 \equiv 1 \pmod{15}$. It follows that for any two integers a and b, with both neither multiples of 3 nor 5, $a^4 \equiv b^4 \pmod{15}$. □

Challenge

C01. A basket contains a number of eggs and when the eggs are removed 2, 3, 4, 5 and 6 at a time, there are 1, 2, 3, 4 and 5, respectively, left over. When the eggs are removed 7 at a time there are none left over. Assuming none of the eggs broke during the preceding operations, determine the minimum number of eggs that were in the basket.

Solution. Let n be the number of eggs in the basket. Since removing 6 eggs leaves at least 5 eggs, $n \geq 11$. We interpret the constraints as a system of linear congruences:

$$\begin{aligned} n &\equiv 1 \pmod 2 & n &\equiv 2 \pmod 3 \\ n &\equiv 3 \pmod 4 & n &\equiv 4 \pmod 5 \\ n &\equiv 5 \pmod 6 & n &\equiv 0 \pmod 7 \end{aligned}$$

Note that all multiples of 7 are odd, so we may ignore the first condition. Also, we may write $n = 7m$ for some integer m and simplify:

$$\begin{aligned} 7m \equiv m &\equiv 2 \pmod 3 & 7m \equiv 3m &\equiv 3 \pmod 4 \\ 7m \equiv 2m &\equiv 4 \pmod 5 & 7m \equiv m &\equiv 5 \pmod 6 \end{aligned}$$

Since 3 and 4 are coprime, we apply CD to the second congruence, $m \equiv 1 \pmod 4$. By definition and the first congruence, $m = 2 + 3p$ for an integer p. Apply CAM and CD:

$$\begin{aligned} 2 + 3p &\equiv 1 \pmod 4 & 2(2 + 3p) &\equiv 4 \pmod 5 & 2 + 3p &\equiv 5 \pmod 6 \\ 3p &\equiv 3 \pmod 4 & 6p &\equiv 0 \pmod 5 & 3p &\equiv 3 \pmod 6 \\ p &\equiv 1 \pmod 4 & p &\equiv 0 \pmod 5 & 3p &\equiv 3 \pmod 6 \end{aligned}$$

We find by inspection that $p = 1$ is a solution to the third congruence, so by LCT, it is equivalently $p \equiv 1 \pmod 2$ (i.e. p is odd). However, this is also implied by the first congruence, leaving us with two congruences. Since 4 and 5 are coprime, we may apply the Chinese Remainder Theorem. By inspection, $p = 5$ is a solution. Therefore, all p are of the form $p \equiv 5 \pmod{20}$ or $p = 5 + 20q$ for an integer q.

It follows that $m = 2 + 3(5 + 20q) = 17 + 60q$ and that $n = 7(17 + 60q) = 119 + 420q$. Since $119 < 420$, the lowest possible value of n is 119 eggs. □