PROBLEM SET 2
MATH 115
NUMBER THEORY
PROFESSOR PAUL VOJTA

NOAH RUDERMAN

Problems 1.4.4ab, 2.1.6, 2.1.12, 2.1.20, 2.1.32, 2.1.40, 2.1.59, 2.2.6abc, 2.2.8, 2.3.4, 2.3.7, 2.3.14, 2.3.16, 2.3.17, and 2.3.20 from *An Introduction to The Theory of Numbers*, 5th edition, by Ivan Niven, Herbert S. Zuckerman, and Hugh L. Montgomery

Date: July 7, 2014.

Problem (1.4.4)

Solution.

a. Consider a set A with $n \in \mathbb{N}$ elements, for an even n. Let us find a recursive expression for the number of partitions, each of which only containing two elements. Let $P(n)$ be the number of ways we may form such partitions in a finite set of n elements. Consider an arbitrary element $k \in A$. There are $(n-1)$ ways k can be paired with another element, and $P(n-2)$ ways the remaining $n-2$ elements can be partitioned into sets of 2. So we write

$$P(n) = (n-1) \cdot P(n-2)$$

Clearly, there is one way to form a partition with only 2 elements so

$$P(2) = 1.$$

Now $|\mathscr{S}| = 2n$, so the number of ways we can partition $\mathscr{S}$ into sets of cardinality 2 is

$$\begin{aligned} P(2n) &= (2n-1)P(2n-2) \\ &= (2n-1)(2n-3)P(2n-4) \\ &\dots \\ &= (2n-1)(2n-3)\cdots 5 \cdot 3 \cdot P(2) \\ &= (2n-1)(2n-3)\cdots 5 \cdot 3 \cdot 1 \end{aligned}$$

We note that

$$\begin{aligned} (2n)(2n-1)(2n-2)\cdots(2)(1) &= (2n)! \\ [(2n-1)(2n-3)\cdots(5)(3)(1)]\,[(2n)(2n-2)\cdots(6)(4)(2)] &= (2n)! \\ [(2n-1)(2n-3)\cdots(5)(3)(1)]\,[2^n(n)(n-1)\cdots(3)(2)(1)] &= (2n)! \\ [(2n-1)(2n-3)\cdots(5)(3)(1)]\,2^n n! &= (2n)! \end{aligned}$$

$$(2n-1)(2n-3)\cdots 5 \cdot 3 \cdot 1 = \frac{(2n)!}{2^n n!} \tag{1}$$

b. It is easy to see that

$$(n+1)(n+2)\cdots(2n) = \frac{(2n)!}{n!}$$

Using equation 1, we see that

$$\begin{aligned}\frac{(n+1)(n+2)\cdots(2n)}{2^n} &= \frac{(2n)!}{2^n n!} \\ &= (2n-1)(2n-3)\cdots 5\cdot 3\cdot 1 \in N\end{aligned}$$

so $n_0 = \prod_{k=1}^{n}(n+k)$ is divisible by 2^n. Furthermore, the quotient of $\frac{n_0}{2^n}$ is odd, since the product of odd numbers is always odd. Thus, $\frac{n_0}{2^n}$ is not divisible by 2, and thus n_0 is not divisible by 2^{n+1}, because if it were, $\frac{n_0}{2^{n+1}} = \frac{n_0 \big/ 2^n}{2}$ would be an integer, which we have shown is impossible.

Problem (2.1.6)

Solution.

Let p be a prime number. If $a^2 \equiv b^2 \mod p$ then

$$\begin{aligned} a^2 &\equiv b^2 \mod p \\ p &\mid a^2 - b^2 \\ p &\mid (a+b)(a-b) \end{aligned}$$

By Theorem 1.15, p must divide $(a+b)$ or $(a-b)$.

Problem (2.1.12)

Solution.

We want to show that $19 \not| 4n^2 + 4$ for any $n \in \mathbb{Z}$.

Theorem 2.12 tells us that $x^2 \equiv -1 \mod p$ for a given prime p if and only if $p = 2$ or $p \equiv 1 \mod 4$.

Since $19 \equiv 3 \not\equiv 1 \mod 4$, we see that for any $n \in \mathbb{Z}$,

$$\begin{aligned} n^2 &\not\equiv -1 \mod 19 \\ n^2 + 1 &\not\equiv 0 \mod 19 \\ 4(n^2 + 1) &\not\equiv 0 \mod 19 \\ 4n^2 + 4 &\not\equiv 0 \mod 19 \\ 19 &\not| (4n^2 + 4). \end{aligned}$$

Problem (2.1.20)

Solution.

We use Theorem 2.3(3). Let $m_1 = 2$, $m_2 = 3$, $m_3 = 7$, $x = n^7 - n$, $n \in \mathbb{Z}$, and $y = 0$. Then $n^7 - n \equiv 0 \mod m_i$ if and only if $n^7 - n \equiv 0 \mod 42$.

Using Fermat's Theorem (Theorem 2.7), we see that

$$\begin{aligned} n^7 &\equiv n \mod 7 \\ n^7 - n &\equiv 0 \mod 7. \end{aligned}$$

Likewise, we see that

$$\begin{aligned} n^7 &= \left(n^3\right)^2 n \\ n^7 &\equiv n^2 \cdot n \mod 3 && \text{(Fermat)} \\ n^7 &= n^3 \\ n^7 &\equiv n \mod 3 && \text{(Fermat)} \\ n^7 - n &\equiv 0 \mod 3. \end{aligned}$$

And finally, we see that

$$\begin{aligned} n^7 &= \left(n^2\right)^3 n \\ n^7 &\equiv n^3 \cdot n \mod 2 && \text{(Fermat)} \\ n^7 &= n^4 \\ n^7 &= \left(n^2\right)^2 \\ n^7 &\equiv n^2 \mod 2 && \text{(Fermat)} \\ n^7 &\equiv n \mod 2 && \text{(Fermat)} \\ n^7 - n &\equiv 0 \mod 2. \end{aligned}$$

Since we have shown for any $n \in \mathbb{Z}$, $n^7 - n \equiv 0 \mod m_i$ for $i = 1, 2, 3$, Theorem 2.3(3) implies

$$n^7 - n \equiv 0 \mod \operatorname{lcm}(m_1, m_2, m_3) = 42,$$

which is equivalent to the statement

$$42 \mid n^7 - n$$

for all $n \in \mathbb{Z}$.

Problem (2.1.32)

Solution.

Suppose m is odd. Clearly, the set $\{1, 2, 3, \ldots, m\}$ is a complete residue system modulo m. Since m is odd, $2 \not| \, m$, so $\gcd(2, m) = 1$. By Theorem 2.6, $\{2 \cdot 1, 2 \cdot 2, 2 \cdot 3, \ldots 2 \cdot m\} = \{2, 4, 6, \ldots 2m\}$ is also a complete residue system modulo m.

Problem (2.1.40)

Solution.

Let m be odd. Clearly, $1, 2, 3, \dots, m$ is a complete residue system. By definition, for any other complete residue system $r_1, r_2, r_3, \dots, r_m$, each $r_i \equiv j_i$ for $1 \leq i \leq m$ and a unique $1 \leq j_i \leq m$. Thus, we may write the sum of elements as

$$\begin{aligned}
\sum_{i=1}^{m} r_i &= \sum_{i=1}^{m} (j_i + k_i m) && \text{where } j_i + k_i m = r_i, k_i \in \mathbb{Z} \\
&= \sum_{i=1}^{m} j_i + \sum_{i=1}^{m} k_i m \\
&= \sum_{j=1}^{m} j + \sum_{i=1}^{m} k_i m && \text{since each } j_i \text{ is unique} \\
&= \frac{m(m+1)}{2} + m \sum_{i=1}^{m} k_i \\
&= m \left(\frac{(m+1)}{2} + \sum_{i=1}^{m} k_i \right).
\end{aligned}$$

Clearly, $\sum_{i=1}^{m} k_i \in \mathbb{Z}$. Since m is odd, $\frac{m+1}{2} \in \mathbb{Z}$, so $\left(\frac{(m+1)}{2} + \sum_{i=1}^{m} k_i \right) \in \mathbb{Z}$ and

$$m \,\Big|\, \sum_{i=1}^{m} r_i$$

for any complete residue system $r_1, r_2, \dots, r_m$ modulo m.

Now we aim to prove the analogous result for a reduce residue system given any $m > 2$. Let U_m represent the group of units modulo m whose elements are less than m. A unit is an element of $\mathbb{Z}_m$ which has an inverse under multiplication. By Theorem 2.9, an element $a \in Z_m$ will have an inverse if $\gcd(a, m) = 1$. Clearly, U_m a reduced residue system.

First we aim to show that if $a \in U_m$, then $m - a \in U_m$. Assume $\gcd(a, m) = 1$. By Theorem 1.9, $\gcd(a, m) = \gcd(-a, m) = \gcd(-a + mx, m)$ for any $x \in \mathbb{Z}$. Choose $x = 1$. Thus,

$$1 = \gcd(a, m) = \gcd(m - a, m),$$

so $a \in U_m$ if and only if $m - a \in U_m$. (Note that the sum of these two numbers, a and $m - a$, is equal to m.)

Next we aim to show that there is no such element $a' \in \mathbb{Z}$ where $a' = m - a'$ and $\gcd(m, a') = 1$. If $a' = m - a'$, then $a' = \frac{m}{2}$. If m is odd, no such number exists, so we assume that m is even. Thus, $\frac{m}{2} \in \mathbb{N}$. Clearly,

$$\gcd(a', m) = \gcd\left(\frac{m}{2}, m\right) = \frac{m}{2}.$$

We see that $\frac{m}{2} = 1$ only when $m = 2$. For all other positive numbers, no such a' exists. Thus, for every $a \in U_m$, where $m > 2$, there will be a $b \in U_m$ such that $a \neq b$ and $a + b = m$. This also implies that $|U_m|$ is even for $m > 2$.

Going on we will show that the reduced residue system $r_1, r_2, \ldots, r_s$, for $s \in \mathbb{N}$ where $r_i < m$ for $1 \leq i \leq s$ the elements sum to a number divisible by m if $m > 2$. Suppose $m > 2$. For a given $r_i \in U_m$, we have shown that there will be another $r_j \in U_m$, where $i \neq j$ and $r_i + r_j = m$. Noting that $s = |U_m|$, we see that

$$\sum_{i=1}^{s} r_i = \frac{s}{2}m,$$

where $\frac{s}{2} \in \mathbb{N}$ because the cardinality of U_m is even. Therefore,

$$m \mid \sum_{i=1}^{s} r_i.$$

Finally, we show that the above result holds for any reduced residue system. Consider the reduced residue system $q_1, q_2, \ldots, q_{s'}$. Since each reduced residue system has the same number of elements ($\phi(m)$), $s' = s$. Each element q_i is congruent to a unique r_j modulo m for $1 \leq i, j \leq m$. Put another way, $q_i = r_j + km$ for some $k \in \mathbb{Z}$. Since the ordering of our set does not matter, we will say $q_i \equiv r_i \mod m$ for each $1 \leq i \leq m$. Now we have

$$\begin{aligned}
\sum_{i=1}^{s} q_i &= \sum_{i=1}^{s} (r_i + k_i m) && (k_i \in \mathbb{Z}) \\
&= \sum_{i=1}^{s} r_i + \sum_{i=1}^{s} k_i m \\
&= \frac{s}{2}m + m\sum_{i=1}^{s} k_i \\
&= m\left(\frac{s}{2} + \sum_{i=1}^{s} k_i\right).
\end{aligned}$$

Since $\frac{s}{2} \in \mathbb{Z}$ and $\sum_{i=1}^{s} k_i \in \mathbb{Z}$, $\left(\frac{s}{2} + \sum_{i=1}^{s} k_i\right) \in \mathbb{Z}$. By definition, $m \mid \sum_{i=1}^{s} q_i$. Since the choice of a reduced residue system $q_1, q_2, \ldots, q_s$ was arbitrary, the condition that m divides the sum of the elements of a reduced residue system modulo m holds if $m > 2$.

Problem (2.1.59)

Solution.

Let p be prime. Suppose $p \mid a^2 + 2b^2$ for $a, b \in \mathbb{Z}$. Since $p \not| \, a, b$; $\gcd(p, a) = \gcd(p, b) = 1$. From Theorem 2.9, there exists $\bar{b} \in \mathbb{Z}_p$ such that $\bar{b}b = b\bar{b} \equiv 1 \mod p$. We have

$$\begin{aligned} p &\mid a^2 + 2b^2 \\ a^2 + 2b^2 &\equiv 0 \mod p \\ a^2 &\equiv -2b^2 \mod p \\ a^2\bar{b}^2 &\equiv -2b^2\bar{b}^2 \mod p \\ \left(a\bar{b}\right)^2 &= -2\left(b\bar{b}\right)^2 \\ \left(a\bar{b}\right)^2 &\equiv -2 \mod p. \end{aligned}$$

Thus, for $x = a\bar{b}$,

$$\begin{aligned} x^2 &= \left(a\bar{b}\right)^2 \\ &\equiv -2 \mod p, \end{aligned}$$

so the congruence $x^2 \equiv -2 \mod p$ has a solution if $p \mid a^2 + 2b^2$ and $p \not| \, a, b$.

Problem (2.2.6)

Solution.

We use Theorem 2.17 to determine the number of solutions.

a. A solution exists to the congruence

$$15x \equiv 25 \mod 35$$

because $g = \gcd(15, 35) = 5, and 5 \mid 25$. Furthermore, there are $g = 5$ solutions modulus 35.

b. No solution exists to the congruence

$$15x \equiv 24 \mod 35$$

because $g = \gcd(15, 35) = 5, and 5 \not| 24$.

c. A solution exists to the congruence

$$15x \equiv 0 \mod 35$$

because $g = \gcd(15, 35) = 5, and 5 \mid 0$. Furthermore, there are $g = 5$ solutions modulus 35.

Problem (2.2.8)

Solution.

Let p be an odd prime. We have

$$x^2 \equiv 1 \mod p^\alpha.$$

From this we see that

$$\begin{aligned} x^2 - 1 &\equiv 0 \mod p^\alpha \\ p^\alpha &\mid x^2 - 1 \\ p^\alpha &\mid (x+1)(x-1). \end{aligned} \tag{2}$$

This also implies

$$p \mid (x+1)(x-1).$$

By Theorem 1.15, p divides at least one of the factors on the right.

Next we aim to show that p cannot divide both $x+1$ and $x-1$. If it did, then by Theorem 1.1(3),

$$\begin{aligned} p &\mid 1 \cdot (x+1) + (-1) \cdot (x-1) \\ p &\mid 2. \end{aligned}$$

By Theorem 1.1(5), $p \mid 2$ implies $p \leq 2$. Because 2 is the smallest prime number, $p \leq 2$ implies $p = 2$ since p is prime. But we assumed p is odd, which is a contradiction since 2 is even. Thus, p cannot divide one of these terms. Since the term that p divides doesn't matter, we'll say that p divides $x+1$ but not $x-1$.

We know that $\gcd(p, x-1) = 1$. By repeated application of Theorem 1.8, we see that $\gcd(p^\alpha, x-1) = 1$. By Theorem 1.10 and equation 2, we see that $p^\alpha \mid (x+1)$. Since the term we assumed that p could divide was arbitrary, this analysis also works if p were to divide $x-1$ but not $x+1$.

Problem (2.3.4)

Solution.

We are being asked to solve the system of linear congruences

$$\begin{aligned} x &\equiv 1 \mod 3 \\ x &\equiv 2 \mod 4 \\ x &\equiv 3 \mod 5. \end{aligned}$$

We start with the third congruence. The solution is $x = 3 + 5b$, for $b \in \mathbb{Z}$. Now we use this value in the second congruence to get

$$\begin{aligned} 3 + 5b &\equiv 2 \mod 4 \\ 5b &\equiv -1 \mod 4 \\ b &\equiv -1 \mod 4 \\ b &\equiv 3 \mod 4, \end{aligned}$$

so $b = 3 + 4c$, for $c \in \mathbb{Z}$. We plug this in to get

$$\begin{aligned} x &= 3 + 5b \\ &= 3 + 5(3 + 4c) \\ &= 3 + 15 + 20c \\ &= 18 + 20c \end{aligned}$$

Next, we use this for the first congruence

$$\begin{aligned} 18 + 20c &\equiv 1 \mod 3 \\ 2c &\equiv 1 \mod 3 \\ 2c &\equiv 4 \mod 3 \\ c &\equiv 2 \mod 3 && \text{(because } \gcd(2,3) = 1\text{, using Theorem 2.3(1))} \end{aligned}$$

so $c = 2 + 3d$, for $d \in \mathbb{Z}$.

Finally, we have

$$\begin{aligned} x &= 18 + 20c \\ &= 18 + 20(2 + 3d) \\ &= 18 + 40 + 60d \\ &= 58 + 60d, \end{aligned}$$

which is the solution to all three congruences.

Problem (2.3.7)

Solution.

We aim to find whether or not the system of linear congruences

$$\begin{aligned} 5x &\equiv 1 \mod 6 \\ 4x &\equiv 13 \mod 15 \end{aligned}$$

has a solution, and if so what it is.

Using Theorem 2.1(5), we see that

$$5x \equiv 1 \mod 6$$

implies

$$\begin{aligned} 5x &\equiv 1 \mod 3 \\ 2x &\equiv 4 \mod 3 \\ x &\equiv 2 \mod 3, \qquad \text{(because } \gcd(2,3) = 1\text{, using Theorem 2.3(1))} \end{aligned} \tag{3}$$

and

$$4x \equiv 13 \mod 15$$

implies

$$4x \equiv 13 \mod 3$$

$$x \equiv 1 \mod 3. \tag{4}$$

Clearly, equations 3 and 4 are incompatible because $1 \not\equiv 2 \mod 3$. Thus, the system of linear congruences is inconsistent and no solutions exist.

Problem (2.3.14)

Solution.

We aim to solve the system of congruences

$$\begin{aligned} x^3+2x-3 &= 0 \mod 9\\ x^3+2x-3 &= 0 \mod 5\\ x^3+2x-3 &= 0 \mod 45. \end{aligned}$$

It is worth noting that by Theorem 2.16, the first two congruences are implied by the third.

We solve for the first two congruences and use the Chinese remainder theorem to find solutions in $\mathbb{Z}_{45}$.

Plugging in $x = 0, 1, 2, \dots, 8$, we find that the soltions to the first congruence are $x = 1, 2, 6 \mod 9$. Likewise, by plugging in $x = 0, 1, 2, 3, 4, 5$, we find that the solutions to the second congruence are $x = 1, 3 \mod 5$.

Using Theorem 2.20, we see that $\gcd(5, 9) = 1$ and $45 = 5 \cdot 9$, so the number of solutions $N(45) = N(5)N(9) = 2 \cdot 3 = 6$ for $f(x) = x^3 + 2x - 3$. All that needs to be done at this point is to use the Chinese remainder theorem to show six solutions in $\mathbb{Z}_{45}$.

I will calculate the first solution for brevity. The algorithm for finding solutions is the same for the remaining five.

Let's find solutions to

$$\begin{aligned} x &\equiv 1 \mod 9\\ x &\equiv 1 \mod 5 \end{aligned}$$

We start with $x = 1 + 9a$ for $a \in \mathbb{Z}$ and plug it into the second congruence

$$\begin{aligned} 1+9a &\equiv 1 \mod 5\\ 9a &\equiv 0 \mod 5\\ 9a &\equiv 90 \mod 5\\ a &\equiv 10 \mod 5 && \text{(because } \gcd(9,5) = 0 \text{ using Theorem 2.3(1))}\\ a &\equiv 0 \mod 5, \end{aligned}$$

so $a = 0 + 5b$. Plugging this into our first solution, we get

$$\begin{aligned} x &= 1 + 9a\\ &= 1 + 9(0 + 5b)\\ &= 1 + 45b, \end{aligned}$$

so $x \equiv 1 \mod 45$.

Finding the remaining five solutions is similarly tedious. The six solutions are

$$\begin{aligned} x &\equiv 1 \mod 45\\ x &\equiv 6 \mod 45\\ x &\equiv 11 \mod 45\\ x &\equiv 28 \mod 45 \end{aligned}$$

$$x \equiv 33 \mod 45$$
$$x \equiv 38 \mod 45$$

Problem (2.3.16)

Solution.

We aim to solve the congruence

$$x^3 - 9x^2 + 23x - 15 \equiv 0 \mod 503.$$

We are given 503 is prime and that

$$x^3 - 9x^2 + 23x - 15 = (x-1)(x-3)(x-5).$$

We see that

$$\begin{aligned} x^3 - 9x^2 + 23x - 15 \equiv 0 \mod 503 \\ 503 \mid x^3 - 9x^2 + 23x - 15 \\ 503 \mid (x-1)(x-3)(x-5). \end{aligned}$$

By Theorem 1.15, at least one of these terms is divisible by 503.

From this we can find the following solutions

$$\begin{array}{ccc} 503 \mid (x-1) & 503 \mid (x-3) & 503 \mid (x-5) \\ x-1 \equiv 0 \mod 503 & x-3 \equiv 0 \mod 503 & x-5 \equiv 0 \mod 503 \\ x \equiv 1 \mod 503 & x \equiv 3 \mod 503 & x \equiv 5 \mod 503 \end{array}$$

Problem (2.3.17)

Solution.

We aim to solve the congruence

$$x^3 - 9x^2 + 23x - 15 \equiv 0 \mod 143.$$

We see that $143 = 11 \cdot 13$ and

$$x^3 - 9x^2 + 23x - 15 = (x-1)(x-3)(x-5). \tag{5}$$

By Theorem 2.3(3), the first congruence is equivalent to the system of congruences

$$\begin{aligned} x^3 - 9x^2 + 23x - 15 &\equiv 0 \mod 11 \\ x^3 - 9x^2 + 23x - 15 &\equiv 0 \mod 13. \end{aligned}$$

By using equation 5, we see that the solutions to the above congruences are

$$\begin{aligned} x &\equiv 1 \mod 11 & x &\equiv 1 \mod 13 \\ x &\equiv 3 \mod 11 & x &\equiv 3 \mod 13 \\ x &\equiv 5 \mod 11 & x &\equiv 5 \mod 13. \end{aligned}$$

Now from Theorem 2.20, since $\gcd(11, 13) = 1$ and $11 \cdot 13 = 143$, $N(143) = N(11)N(13) = 3 \cdot 3 = 9$ for $f(x) = x^3 - 9x^2 + 23x - 15$, so we expect there to be 9 solutions to the original congruence.

We can find each solution by constructing 9 pairs of linear congruences and finding the solution with the Chinese Remainder Theorem.

I will solve an arbitrary pair of linear congruences. The remaining 8 are equally tedious.

Consider the following congruences

$$\begin{aligned} x &\equiv 3 \mod 11 \\ x &\equiv 5 \mod 13. \end{aligned}$$

The solution to the first congruence is $x = 3 + 11a$ for some $a \in \mathbb{Z}$. Now we plug this into the second congruence to get

$$\begin{aligned} 3 + 11a &\equiv 5 \mod 13 \\ 11a &\equiv 2 \mod 13 \\ -2a &\equiv 2 \mod 13 \\ 2a &\equiv -2 \mod 13 \\ a &\equiv -1 \mod 13 \qquad \text{(because } \gcd(2, 13) = 1 \text{ using Theorem 2.3(1))} \\ a &\equiv 12 \mod 13. \end{aligned}$$

so $a = 12 + 13b$, for $b \in \mathbb{Z}$. Plugging this into x we get

$$\begin{aligned} x &= 3 + 11a \\ &= 3 + 11(12 + 13b) \\ &= 3 + 132 + 143b \end{aligned}$$

$$= 135 + 143b,$$

so $x \equiv 135 \mod 143$ is one solution.

The full set of solutions is

$$\begin{aligned} x &\equiv 1 \mod 143 \\ x &\equiv 3 \mod 143 \\ x &\equiv 5 \mod 143 \\ x &\equiv 14 \mod 143 \\ x &\equiv 16 \mod 143 \\ x &\equiv 27 \mod 143 \\ x &\equiv 122 \mod 143 \\ x &\equiv 133 \mod 143 \\ x &\equiv 135 \mod 143 \end{aligned}$$

Problem (2.3.20)

Solution.

For $m_1, m_2 \in \mathbb{Z}^+$ fixed, and $a_1, a_2 \in \mathbb{Z}$ arbitrary, we have

$$\begin{aligned} x &\equiv a_1 \mod m_1 \\ x &\equiv a_2 \mod m_2. \end{aligned}$$

Let us try to find a solution to the above system of linear congruences. We start with the general solution to the first congruence: $x = a_1 + m_1 \cdot k$, for $k \in \mathbb{Z}$. Let $g = \gcd(m_1, m_2)$. Next we plug that into the second congruence

$$\begin{aligned} a_1 + m_1 \cdot k &\equiv a_2 \mod m_2 \\ k \cdot m_1 &\equiv a_2 - a_1 \mod m_2 \\ k\frac{m_1}{g} &\equiv \frac{a_2 - a_1}{g} \mod \frac{m_2}{g} && \text{by Theorem 2.3(1)} \quad (*) \\ k\frac{m_1}{g}\overline{\left(\frac{m_1}{g}\right)} &\equiv \frac{a_2 - a_1}{g}\overline{\left(\frac{m_1}{g}\right)} \mod \frac{m_2}{g} && (**) \\ k &\equiv \frac{a_2 - a_1}{g}\overline{\left(\frac{m_1}{g}\right)} \mod \frac{m_2}{g}, \end{aligned}$$

so $k = \frac{a_2-a_1}{g}\overline{\left(\frac{m_1}{g}\right)} + \frac{m_2}{g} \cdot o$, for $o \in \mathbb{Z}$.

We use (*) to note $a_2 - a_1$ must be divisible by g, or $a_1 \equiv a_2 \mod g$. We use (**) to note that $\gcd\left(\frac{m_1}{g}, \frac{m_2}{g}\right) = 1$ by Theorem 1.7, so $\frac{m_1}{g}$ has a unique inverse in $\mathbb{Z}_{\frac{m_2}{g}}$ by Theorem 2.9, which we denote as $\overline{\left(\frac{m_1}{g}\right)}$.

Each of the steps up to this point has been if and only statements, so a solution to the system of linear congruences

$$\begin{aligned} x &\equiv a_1 \mod m_1 \\ x &\equiv a_2 \mod m_2 \end{aligned}$$

exists if and only if $a_1 \equiv a_2 \mod g$, for $g = \gcd(m_1, m_2)$.

Now we can plug k back into x to get

$$\begin{aligned} x &= a_1 + m_1 \cdot k \\ x &= a_1 + m_1\left(\frac{a_2 - a_1}{g}\overline{\left(\frac{m_1}{g}\right)} + \frac{m_2}{g} \cdot o\right) \\ x &= a_1 + m_1\frac{a_2 - a_1}{g}\overline{\left(\frac{m_1}{g}\right)} + \frac{m_1 m_2}{g} \cdot o \\ x &= a_1 + m_1\frac{a_2 - a_1}{g}\overline{\left(\frac{m_1}{g}\right)} + \operatorname{lcm}(m_1, m_2) \cdot o && (***) \end{aligned}$$

$$x \equiv a_1 + m_1 \frac{a_2 - a_1}{g} \overline{\left(\frac{m_1}{g}\right)} \quad \text{mod } \operatorname{lcm}(m_1, m_2),$$

where (***) is using Theorem 1.13, which states that

$$\begin{aligned} \operatorname{lcm}(m_1, m_2) \gcd(m_2, m_2) &= |m_1 m_2| \\ \operatorname{lcm}(m_1, m_2) &= \frac{|m_1 m_2|}{\gcd(m_1, m_2)} \\ \operatorname{lcm}(m_1, m_2) &= \frac{m_1 m_2}{g} && \text{(since } m_1, m_2 \in \mathbb{Z}^+\text{)} \end{aligned}$$

Clearly, if a solution to our original set of linear congruences exists, the solution will be a single congruence class (recall that inverses are unique in $\mathbb{Z}_n$ if they exist) modulo $\operatorname{lcm}(m_1, m_2)$. Thus, the solution is unique modulo $\operatorname{lcm}(m_1, m_2)$.