1 Exercises

1.1

Construct congruences modulo 12 with no solutions, just one solution, and more than one solution.

$2x \equiv 1 \pmod{12}$.
$5x \equiv 3 \pmod{12}$.
$6x \equiv 6 \pmod{12}$.

1.2

Which congruences have no solutions?
(a) $3x \equiv 1 \pmod{10}$.
(b) $4x \equiv 1 \pmod{10}$.
(c) $5x \equiv 1 \pmod{10}$.
(d) $6x \equiv 1 \pmod{10}$.
(e) $7x \equiv 1 \pmod{10}$.

(b), **(c)**, **(d)**.

1.3

After Exercise 2, can you guess a criterion for telling when a congruence has no solutions?

Such a criterion is probably $(a, m) \nmid b$.

1.4

Solve
(a) $8x \equiv 1 \pmod{15}$.
(b) $9x + 10y = 11$.

(a) $8x \equiv 1 \equiv 16 \pmod{15}$. $x \equiv 2 \pmod{15}$. $x = 2$.
(b) $9x \equiv 11 \equiv 81 \pmod{10}$. $x = 9 + 10t$. $9 * (9 + 10t) + 10y = 11$. $y = -7 - 9t$.

1.5

Determine the number of solutions of each of the following congruences:

$$3x \equiv 6 \pmod{15}, \quad 4x \equiv 8 \pmod{15}, \quad 5x \equiv 10 \pmod{15}$$
$$6x \equiv 11 \pmod{15}, \quad 7x \equiv 14 \pmod{15}$$

$(3, 15) = 3$, and $3 \mid 6$, so 3 solutions.
$(4, 15) = 1$, and $1 \mid 8$, so 1 solution.
$(5, 15) = 5$, and $5 \mid 10$, so 5 solutions.
$(6, 15) = 3$, but $3 \nmid 11$, so no solutions.
$(7, 15) = 1$, and $1 \mid 14$, so 1 solution.

1.6

Find all the solutions of $5x \equiv 10 \pmod{15}$.
We can reduce this to $x \equiv 2 \pmod{3}$, so $x = 2$. However now must add back all the other viable $x + 3t$. So $x \in \{2, 5, 8, 11, 14\}$.

1.7

Solve the rest of the congruences in Exercise 5.

$3x \equiv 6 \pmod{15}$ is solved by $x \in \{2, 7, 12\}$.

$4x \equiv 8 \pmod{15}$ is solved by $x = 2$.
$7x \equiv 14 \pmod{15}$ is solved by $x = 2$.

1.8

Verify that 52 satisfies each of the three congruences.

$3|52-1$. $5|52-2$. $7|52-3$.

2 Problems

2.1

Solve each of the following:

$$2x \equiv 1 \pmod{17}, \quad 3x \equiv 1 \pmod{17},$$
$$3x \equiv 6 \pmod{18}, \quad 40x \equiv 777 \pmod{1777}$$

$x = 9$.
$x = 6$.
$x \in \{2, 8, 14\}$.
$40x \equiv -1000 \pmod{1777}$. $x \equiv 25 \pmod{1777}$. $x = 25$.

2.2

Solve each of the following:

$$2x \equiv 1 \pmod{19}, \quad 3x \equiv 1 \pmod{19},$$
$$4x \equiv 6 \pmod{18}, \quad 20x \equiv 984 \pmod{1984}$$

$x = 10$.
$x = 13$.
$x \in \{6, 15\}$.
$10x \equiv 492 \equiv -500 \pmod{992}$. $x \in \{942, 1934\}$.

2.3

Solve the systems
(a) $x \equiv 1 \pmod 2$, $x \equiv 1 \pmod 3$.
(b) $x \equiv 3 \pmod 5$, $x \equiv 5 \pmod 7$, $x \equiv 7 \pmod{11}$.
(c) $2x \equiv 1 \pmod 5$, $3x \equiv 2 \pmod 7$, $4x \equiv 3 \pmod{11}$.

(a) $x = 2k_1 + 1 \equiv 1 \pmod 3$. So $k_1 \equiv 0 \pmod 3$. Now write $k_1 = 3k_2$, so $x = 6k_2 + 1 \Rightarrow x \equiv 1 \pmod 6$.
(b) $x = 5k_1 + 3 \equiv 5 \pmod 7$. So $5k_1 \equiv 2 \pmod 7$, which simplifies to $k_1 \equiv 6 \pmod 7$. Now write $k_1 = 7k_2 + 6$, meaning $x = 35k_2 + 33$. We know $35k_2 + 33 \equiv 7 \pmod{11}$, or $35k_2 \equiv 7 \pmod{11}$. Solving, we get $k_2 \equiv 9 \pmod{11}$. So can write $k_2 = 11k_3 + 9$. Plugging back into the equation for x, get $x = 385k_3 + 348$, or $x \equiv 348 \pmod{385}$.
(c) Can write the first congruence as $x \equiv 3 \pmod 5$, and x as $x = 3 + 5k_1$. So, plugging this into the second congruence, get $3(3 + 5k_1) = 9 + 15k_1 \equiv 2 \pmod 7$, or $15k_1 \equiv k_1 \equiv 0 \pmod 7$. So, can write $k_1 = 7k_2$ and plug back into our equation for x to get $x = 3 + 35k_2$. Plugging this into the third congruence, have $4(3 + 35k_2) = 12 + 140k_2 \equiv 3 \pmod{11}$, or $k_2 \equiv 3 \pmod{11}$. So, can write $k_2 = 11k_3 + 3$ and plug back into our equation for x to get $x = 108 + 385k_3$, or $x \equiv 108 \pmod{385}$.

2.4

Solve the systems
(a) $x \equiv 1 \pmod 2$, $x \equiv 2 \pmod 3$.
(b) $x \equiv 2 \pmod 5$, $2x \equiv 3 \pmod 7$, $3x \equiv 4 \pmod{11}$.
(c) $x \equiv 31 \pmod{41}$, $x \equiv 59 \pmod{26}$.

(a) From the first congruence, can write x as $x = 1 + 2k_1 \equiv 2 \pmod 3$, meaning $k_1 \equiv 2 \pmod 3$ So, now write $k_1 = 2 + 3k_2$ and substitute back into the equation for x to get $x = 5 + 6k_2$, or $x \equiv 5 \pmod 6$.
(b) From the first congruence, can write x as $x = 2 + 5k_1$. From the second, we know that $4 + 10k_1 \equiv 3 \pmod 7$, or $k_1 \equiv 2 \pmod 7$. Now write $k_1 = 2 + 7k_2$, which we plug backinto the equation for x to get $x = 12 + 35k_2$. From the third congruence, we have $36 + 105k_2 \equiv 4 \pmod{11}$, or $k_2 \equiv 2 \pmod{11}$. So $k_3 = 2 + 11k_2$ and $x = 82 + 385k_3$, or $x \equiv 82 \pmod{385}$.
(c) From the first congruence, can write x as $x = 31 + 41k_1 \equiv 59 \pmod{26}$. So $41k_1 \equiv 28 \pmod{26}$, or $x \equiv 14 \pmod{26}$. So can write $k_1 = 14 + 26k_2$ and plug it back into the equation for x to get $x = 605 + 1066k_2$, or $x \equiv 605 \pmod{1066}$.

2.5

What possibilities are there for the number of solutions of a linear congruence $\pmod{20}$?

There can be 0, 1, 2, 5, 10 or 20 solutions.

2.6

Construct linear congruences modulo 20 with no solutions, just one solution, and more than one solution. Can you find one with 20 solutions?

$2x \equiv 3 \pmod{20}$.
$3x \equiv 3 \pmod{20}$.
$20x \equiv 0 \pmod{20}$.

2.7

Solve $9x \equiv 4 \pmod{1453}$.

$$\begin{aligned} 9x &\equiv -1449 \pmod{1453} \\ x &\equiv -161 \pmod{1453} \\ x &\equiv 1292 \pmod{1453} \end{aligned}$$

2.8

Solve $4x \equiv 9 \pmod{1453}$.

$$\begin{aligned} 2x &\equiv 731 \pmod{1453} \\ x &\equiv 1092 \pmod{1453} \end{aligned}$$

2.9

Solve for x and y:
(a) $x + 2y \equiv 3 \pmod 7$, $3x + y \equiv 2 \pmod 7$.
(b) $x + 2y \equiv 3 \pmod 6$, $3x + y \equiv 2 \pmod 6$.

(a) Write $x + 2y = 3 + 7k_1$, $3x + y = 2 + 7k_2$. Then, subtract to get $-5x = -1 + 7(k_1 - k_2)$. So, $5x \equiv 1 \pmod 7$, or $x \equiv 3 \pmod 7$. By inspection, this means $7|y$, i.e. $y \equiv 0 \pmod 7$.
(b) Write $x + 2y = 3 + 6k_1$, $4x + y = 2 + 6k_2$. Subtract to get $7x = 1 - 6k_1 + 12k_2$. $7x = 1 \pmod 6$, or $x \equiv 1 \pmod 6$. Then $y \equiv 1 \pmod 6$.

2.10

Solve for x and y:
(a) $x + 2y \equiv 3 \pmod 9$, $3x + y \equiv 2 \pmod 9$.
(b) $x + 2y \equiv 3 \pmod{10}$, $3x + y \equiv 2 \pmod{10}$.

(a) Write $x+2y = 3+9k_1$, $3x+y = 2+9k_2$. Subtract to get $5x = 1-9k_1+18k_2$, or $5x \equiv 1 \pmod 9$, whose solution is $x \equiv 2 \pmod 9$. Then $y \equiv 5 \pmod 9$.
(b) Write $x + 2y = 3 + 10k_1$, $3x + y = 2 + 10k_2$. Subtract to get $5x \equiv 1 \pmod{10}$. There are no solutions to this congruence.

2.11

When the marchers in the annual Mathematics Department Parade lined up 4 abreast, there was 1 odd person; when they tried 5 in a line, there were 2 left over; and when 7 abreast, there were 3 left over. How large is the Department?

Let x be the cardinality of the Mathematics Department. Restating the prompt, have:

$$x \equiv 1 \pmod 4, \quad x \equiv 2 \pmod 5, \quad x \equiv 3 \pmod 7$$

The solution to this system is:

$$\begin{aligned} x &= 1 + 4k_1 \equiv 2 \pmod 5 \\ k_1 &\equiv 4 \pmod 5 \\ x &= 17 + 20k_2 \equiv 3 \pmod 7 \\ k_2 &\equiv 0 \pmod 7 \\ x &\equiv 17 \pmod{140} \end{aligned}$$

2.12

Find a multiple of 7 that leaves the remainder 1 when divided by 2, 3, 4, 5 or 6.

We can write number as $7x$, such that $7x \equiv 1 \pmod k$ for $k \in [2, 6]$.

$$\begin{aligned} 7x &\equiv 1 \pmod 2 \\ x &\equiv 1 \pmod 2 \\ 7 + 14k_1 &\equiv 1 \pmod 3 \\ k_1 &\equiv 0 \pmod 3 \\ 7 + 42k_2 &\equiv 1 \pmod 4 \\ k_2 &\equiv 1 \pmod 4 \\ 49 + 168k_3 &\equiv 1 \pmod 5 \\ k_3 &\equiv 4 \pmod 5 \\ 721 + 840k_3 &\equiv 1 \pmod 6 \\ 840k_3 &\equiv 0 \pmod 6 \end{aligned}$$

So, 721 is such a multiple of 7.

2.13

Find the smallest odd n, $n > 3$, such that $3|n$, $5|n + 2$, and $7|n + 4$.

n is odd can be written as $n \equiv 1 \pmod 2$. Add this to the remaining conditions to get a system of congruences:

$$n \equiv 1 \pmod 2, \quad n \equiv 0 \pmod 3, \quad n \equiv 3 \pmod 5, \quad n \equiv 3 \pmod 7.$$

Solving:

$$\begin{aligned}
n &\equiv 1 \pmod 2 \\
1 + 2k_1 &\equiv 0 \pmod 3 \\
k_1 &\equiv 1 \pmod 3 \\
3 + 6k_2 &\equiv 3 \pmod 5 \\
k_2 &\equiv 0 \pmod 5 \\
3 + 30k_3 &\equiv 3 \pmod 7 \\
k_3 &\equiv 0 \pmod 7 \\
n &= 3 + 210t
\end{aligned}$$

The smallest odd $n > 3$ is when $t = 1$, i.e $n = 213$.

2.14

Find the smallest integer n, $n > 2$, such that $2|n$, $3|n+1$, $4|n+2$, $5|n+3$ and $6|n+4$.

Since $6|n+4 \Rightarrow 3|n+1$ and $4|n+2 \Rightarrow 2|n$, we can remove the latter two to get a system of congruences for which no two moduli have a greatest common divisor greater than 1:

$$n \equiv 2 \pmod 6, \quad n \equiv 2 \pmod 5, \quad n \equiv 2 \pmod 4.$$

Solving:

$$\begin{aligned}
n &\equiv 2 \pmod 6 \\
2 + 6k_1 &\equiv 2 \pmod 5 \\
k_1 &\equiv 0 \pmod 5 \\
2 + 30k_2 &\equiv 2 \pmod 4 \\
1 + 15k_2 &\equiv 1 \pmod 2 \\
k_2 &\equiv 0 \pmod 2 \\
n &= 2 + 60t
\end{aligned}$$

The smallest $n > 2$ is when $t = 1$, i.e $n = 62$.

2.15

Find a positive integer such that half of it is a square, a third of it is a cube, and a fifth of it is a fifth power.

Any n such n must be divisible by the primes 2, 3, and 5. Let's examine candidate ns made up exclusively of these factors. Then we can write:

$$\begin{aligned}
n &= 2^{2x_2+1} * 3^{2x_3} * 5^{2x_5} \\
n &= 2^{3y_2} * 3^{3y_3+1} * 5^{3y_5} \\
n &= 2^{5z_2} * 3^{5z_3} * 5^{5z_5+1}
\end{aligned}$$

From this we can derive a system of congruences for each prime's exponent. Starting with the exponents of 2:

$$\begin{aligned}
2x_2 &\equiv 2 \pmod 3 \\
x_2 &\equiv 1 \pmod 3 \\
x_2 &= 1 + 3t \\
2 + 6t &\equiv 4 \pmod 5 \\
t &\equiv 2 \pmod 5 \\
x_2 &\equiv 7 \pmod{15}
\end{aligned}$$

Now exponents of 3:

$$\begin{aligned}
3y_3 &\equiv 1 \pmod{2} \\
y_3 &\equiv 1 \pmod{2} \\
y_3 &= 1 + 2t \\
3 + 6t &\equiv 4 \pmod{5} \\
t &\equiv 1 \pmod{5} \\
y_3 &\equiv 3 \pmod{10}
\end{aligned}$$

Now exponents of 5:

$$\begin{aligned}
5z_5 &\equiv 1 \pmod{2} \\
z_5 &\equiv 1 \pmod{2} \\
z_5 &= 1 + 2t \\
5 + 10t &\equiv 2 \pmod{3} \\
t &\equiv 0 \pmod{3} \\
y_3 &\equiv 1 \pmod{6}
\end{aligned}$$

So, can construct such an example n from $n = 2^{15} * 3^{10} * 5^6 = 30,233,088,000,000$.

2.16

The three consecutive integers 48, 49, and 50 each have a square factor.
(a) Find n such that $3^2|n$, $4^2|n+1$, and $5^2|n+2$.
(b) Can you find n such that $2^2|n$, $3^2|n+1$, and $4^2|n+2$?

(a) We can write this as a system of congruences:

$$n \equiv 0 \pmod{9}, \quad n \equiv 15 \pmod{16}, \quad n \equiv 23 \pmod{25}$$

Solving:

$$\begin{aligned}
n &= 9k_1 \\
9k_1 &\equiv 15 \pmod{16} \\
k_1 &\equiv 7 \pmod{16} \\
n &= 63 + 144k_2 \\
63 + 144k_2 &\equiv 23 \pmod{25} \\
k_2 &\equiv 15 \pmod{25} \\
n &= 63 + 144(15 + 25t) \\
n &\equiv 2223 \pmod{3600}
\end{aligned}$$

(b) Write this as a system of congruences:

$$n \equiv 0 \pmod{4}, \quad n \equiv 8 \pmod{9}, \quad n \equiv 14 \pmod{16}$$

Solving:

$$\begin{aligned}
n &= 4k_1 \\
4k_1 &\equiv 8 \pmod{9} \\
k_1 &\equiv 2 \pmod{9} \\
n &= 8 + 36k_2 \\
8 + 36k_2 &\equiv 14 \pmod{16} \\
6k_2 &\equiv 1 \pmod{16}
\end{aligned}$$

There is no such n because the congruence $6k_2 \equiv 1 \pmod{16}$ has no solutions.

2.17

If $x \equiv r \pmod{m}$ and $x \equiv s \pmod{m+1}$, show that

$$x \equiv r(m+1) - sm \pmod{m(m+1)}$$

Similarly to previous exercises:

$$\begin{aligned}
x &= r + mk_1 \\
r + mk_1 &\equiv s \pmod{m+1} \\
mk_1 &\equiv s - r \pmod{m+1} \\
mk_1 &\equiv s - r + (r-s)(m+1) \pmod{m+1} \\
mk_1 &\equiv m(r-s) \pmod{m+1} \\
k_1 &\equiv r - s \pmod{m+1} \\
x &= r + m(r - s + (m+1)t) \\
x &= r(m+1) - sm + m(m+1)t \\
x &\equiv r(m+1) - sm \pmod{m(m+1)}
\end{aligned}$$

2.18

What three positive integers, upon being multiplied by 3, 5, and 7 respectively and the products divided by 20, have remainders in arithmetic progression with common difference 1 and quotients equal to remainders?

To begin, one can write the three numbers as follows:

$$\begin{aligned}
3x &= k + 20k = 21k \\
5y &= k + 1 + 20(k+1) = 21k + 21 \\
7z &= k + 2 + 20(k+2) = 21k + 42
\end{aligned}$$

From which the following congruences can be derived:

$$\begin{aligned}
3x &\equiv 0 \pmod{21} \\
x &\equiv 0 \pmod{7} \\
x &= 7t_x \\
5y &\equiv 0 \pmod{21} \\
y &\equiv 0 \pmod{21} \\
y &= 21t_y \\
7z &\equiv 0 \pmod{21} \\
z &\equiv 0 \pmod{3} \\
y &= 3t_z
\end{aligned}$$

Plugging back into the first set of equations:

$$\begin{aligned}
t_x &= k \\
5t_y &= k + 1 \\
t_z &= k + 2
\end{aligned}$$

Notice that $5|k+1$, so $k = 4$ is a good candidate. This implies $x = 7 * 4$, $y = 21 * 1$ and $z = 3 * 6$, or

$$x = 28, \quad y = 21, \quad z = 18$$

As it turns out, these three numbers have the desired properties.

2.19

Suppose that the moduli in the system

$$x \equiv a_i \pmod{m_i}, \quad i = 1, 2, ..., k$$

are not relatively prime in pairs. Find a condition that the a_i must satisfy in order that the system have a solution.

Recall the algorithm we employed to solve such systems of congruences:

$$\begin{aligned} x &= a_1 + m_1 k_1 \\ a_1 + m_1 k_1 &\equiv a_2 \pmod{m_2} \\ m_1 k_1 &\equiv a_2 - a_1 \pmod{m_2} \end{aligned}$$

By **Theorem 1**, $k_i x \equiv a_i \pmod{m_i}$ has no solutions if $(k_i, m_i) \nmid a_i$. In the congruence above, if there are any a_i, a_j such that $(m_i, m_j) \nmid a_i - a_j$, then the system won't have a solution. If the system does have a solution, then we'll have $k_1 \equiv a^* \pmod{m_2}$, from which it follows that $x = a_1 + m_1(a^* + m_2 k_2) = a_1 + m_1 a^* + m_1 m_2 k_2$, or $x \equiv a_{ij} \pmod{m_i m_j}$, and we can simply restate our problem with the congruences for m_i, m_j combined. In other words, $(m_i, m_j)|(a_i - a_j)$ for all $i \neq j$ is such a necessary condition.

2.20

How many multiples of b are there in the sequence

$$a, 2a, 3a, ..., ba \text{ ?}$$

One can rewrite the series as

$$bx_1 + r_1, bx_2 + r_2, ..., bx_b + r_b$$

We are looking for those terms in which r_i is 0, i.e. $bx_i = ia$, implying the linear congruence $bx \equiv 0 \pmod{a}$. From **Theorem 1**, we know there are (a, b) solutions to this congruence, corresponding to (a, b) multiples of b in the sequence.