Chapter 3 Solutions

An Introduction to Mathematical Thinking: Algebra and Number Systems

William J. Gilbert and Scott A. Vanstone, Prentice Hall, 2005

Solutions prepared by William J. Gilbert and Alejandro Morales

Exercise 3-1:

Which of the following integers are congruent modulo 4?

$$-12,\ -11,\ -9,\ -6,\ -4,\ -1,\ 0,\ 1,\ 2,\ 3,\ 5,\ 7,\ 10$$

Solution: Look at the quotients and remainders on division by 4.

x	-12	-11	-9	-6	-4	-1	0	1	2	3	5	7	10
q	-3	-3	-3	-2	-1	-1	0	0	0	0	1	1	2
r	0	1	3	2	0	3	0	1	2	3	1	3	2

Then the following sets of numbers give members of the same equivalence class under congruence modulo 4:

$$\{-12,-4,0\},\ \{-11,1,5\},\ \{-6,2,10\},\ \{-9,-1,3,7\}.$$

Exercise 3-2:

Which of the following integers are congruent modulo 6?

$$-147,\ -91,\ -22,\ -14,\ -2,\ 2,\ 4,\ 5,\ 21,\ 185$$

Solution: Look at the quotients and remainders on division by 6.

x	-147	-91	-22	-14	-2	2	4	5	21	185
q	-25	-16	-4	-3	-1	0	0	0	3	30
r	3	5	2	4	4	2	4	5	3	5

Then the following sets of numbers give members of the same equivalence class under congruence modulo 6:

$$\{2,-22\},\ \{21,-147\},\ \{4,-2,-14\},\ \{185,5,-91\}.$$

Exercise 3-3:

What is the remainder when 8^{24} is divided by 3?

Solution:

$$\begin{aligned} 8 &\equiv 2 \pmod 3 \\ 2^4 &= 16 \equiv 1 \pmod 3 \\ 8^{24} &\equiv 2^{24} \pmod 3 \\ &\equiv (2^4)^6 \pmod 3 \\ &\equiv 1^6 \pmod 3 \\ &\equiv 1 \pmod 3 \end{aligned}$$

Hence the remainder when 8^{24} is divided by 3 is 1.

Exercise 3-4:

Let $N = 3^{729}$. What is the last digit in the decimal representation of N? What are the last digits in the base 9 and base 8 representations of N?

Solution: For the base 10 representation (the decimal representation),

$$N = \sum_{i=0}^{k} a_i 10^i = a_0 + 10(a_1 + 10a_2 + 10^2 a_3 + \ldots + 10^{k-1} a_k).$$

The last digit in the decimal representation is a_0, and $N \equiv a_0 \pmod{10}$ with $0 \leq a_0 < 10$. We therefore have to determine the remainder when N is divided by 10.

Now $3^2 \equiv -1 \pmod{10}$, hence $3^4 \equiv 1 \pmod{10}$. The exponent 729 can be written as $729 = 4 \cdot 182 + 1$. Thus

$$\begin{aligned} 3^{729} &= 3^{4 \cdot 182 + 1} \\ &= 3(3^4)^{182}. \end{aligned}$$

Hence

$$\begin{aligned} 3^{729} &\equiv 3(3^4)^{182} \pmod{10} \\ &\equiv 3(1)^{182} \pmod{10} \\ &\equiv 3 \pmod{10} \end{aligned}$$

and we see that the last digit in the decimal expansion of N is 3.

Similarly, the last digit in the base 9 representation is the remainder upon division by 9. However $3^2 \equiv 0 \pmod 9$, so

$$\begin{aligned} 3^{729} &= 3^2 \cdot 3^{727} \\ &\equiv 0 \cdot 3^{727} \pmod 9 \\ &\equiv 0 \pmod 9 \end{aligned}$$

and the last digit in the base 9 representation of N is 0.

Also, the last digit in the base 8 representation is the remainder upon division by 8. Now $3^2 \equiv 1 \pmod 8$, so

$$\begin{aligned} 3^{729} &= 3^{2\cdot 364+1} \\ &\equiv 3(3^2)^{364} \pmod 8 \\ &\equiv 3(1)^{364} \pmod 8 \\ &\equiv 3 \pmod 8 \end{aligned}$$

and the last digit in the base 8 representation of N is 3.

Exercise 3-5:

What is the remainder when 10^{45} is divided by 7?

Solution:

$$\begin{aligned} 10 &\equiv 3 \pmod 7 \\ 10^2 &\equiv 3^3 \equiv 2 \pmod 7 \\ 10^3 &\equiv 10 \cdot 10^2 \equiv 3 \cdot 2 \equiv 6 \equiv -1 \pmod 7 \\ 10^6 &\equiv \left(10^3\right)^2 \equiv (-1)^2 \equiv 1 \pmod 7 \\ 10^{45} &\equiv 10^{7\cdot 6+3} \pmod 7 \\ &\equiv \left(10^6\right)^7 \left(10^3\right) \pmod 7 \\ &\equiv 1 \cdot 6 \pmod 7 \\ &\equiv 6 \pmod 7 \end{aligned}$$

Hence the remainder when 10^{45} is divided by 7 is 6.

Exercise 3-6:

Is $6^{17} + 17^6$ divisible by 3 or 7?

Solution: For divisibility by 3, it easy to see that $6 \equiv 0 \pmod 3$ and $17 \equiv 1 \pmod 3$. Thus

$$\begin{aligned} 6^{17} + 17^6 &\equiv 0^{17} + (-1)^6 \pmod 3 \\ &\equiv 1 \pmod 3 \end{aligned}$$

Therefore 3 does not divide $6^{17} + 17^6$.

For divisibility by 7, we have $6 \equiv -1 \pmod 7$ and $17 \equiv 3 \pmod 7$. Therefore

$$\begin{aligned} 6^{17} + 17^6 &\equiv (-1)^{17} + 3^6 \pmod 7 \\ &\equiv (-1) + \left(3^2\right)^3 \pmod 7 \\ &\equiv (-1) + 9^3 \pmod 7 \\ &\equiv (-1) + 2^3 \pmod 7 \\ &\equiv -1 + 8 \pmod 7 \\ &\equiv 0 \pmod 7. \end{aligned}$$

Hence $6^{17} + 17^6$ is divisible by 7.

Exercise 3-7:

Show that an integer of the form $5n + 3$, where $n \in \mathbb{P}$, can never be a perfect square.

Solution: Every integer is congruent to 0, 1, 2, 3, 4, or 5 modulo 5. Their squares have the following form.

Modulo 5					
x	0	1	2	3	4
x^2	0	1	4	4	1

This table summarizes these facts.

(1) The square of any integer divisible by 5 is divisible by 5.

(2) The square of any integer of the form $5n + 1$ or $5n + 4$ has remainder 1 when divided by 5.

(3) The square of any integer of the form $5n + 2$ or $5n + 3$ has remainder 4 when divided by 5.

Hence the square of any integer has remainder 0, 1, or 4 modulo 5. Thus no integer has a square with remainder 3. That is, $5n+3$ is never a perfect square.

Exercise 3-8:

For the following congruence, determine whether there exists a positive integer k so that the congruence is satisfied. If so, find the smallest such k.

$2^k \equiv 1 \pmod{11}$

Solution: Let us run through the first few positive integers for k.

Modulo 11										
k	1	2	3	4	5	6	7	8	9	10
2^k	2	4	8	5	-1	9	7	3	6	1

We conclude that there is a solution and the smallest value of k is 10.

Exercise 3-9:

For the following congruence, determine whether there exists a positive integer k so that the congruence is satisfied. If so, find the smallest such k.

$3^k \equiv 1 \pmod{17}$

Solution: Fermat's Little Theorem tells us $3^{16} \equiv 1 \pmod{17}$, so $k = 16$ is one solution, but this might not be the smallest such k.

Modulo 17																
k	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
3^k	3	9	10	13	5	15	11	16	14	8	7	4	12	2	6	1

Therefore $k = 16$ is the smallest such k.

Exercise 3-10:

For the following congruence, determine whether there exists a positive integer k so that the congruence is satisfied. If so, find the smallest such k.

$2^k \equiv 1 \pmod{14}$

Solution 1: The number 2^k is always even for $k \geq 1$, so it can never be congruent to 1 modulo 14.

Solution 2:

$$\begin{aligned} 2^1 &\equiv 2 \pmod{14} \\ 2^2 &\equiv 4 \pmod{14} \\ 2^3 &\equiv 8 \pmod{14} \\ 2^4 &\equiv 2 \pmod{14} \end{aligned}$$

Therefore we can multiple the first congruence below by powers of 2.

$$\begin{aligned} 2^1 &\equiv 2^4 \pmod{14} \\ 2^2 &\equiv 2^5 \pmod{14} \\ 2^3 &\equiv 2^6 \pmod{14} \\ 2^4 &\equiv 2^7 \pmod{14} \quad \text{and so on} \end{aligned}$$

$$\begin{aligned} 2^1 \equiv 2^4 \equiv 2^7 \equiv \cdots \equiv 2^{3r+1} \pmod{14} \\ 2^2 \equiv 2^5 \equiv 2^8 \equiv \cdots \equiv 2^{3r+2} \pmod{14} \\ 2^3 \equiv 2^6 \equiv 2^9 \equiv \cdots \equiv 2^{3r} \pmod{14} \end{aligned}$$

Thus no positive power of 2 is congruent to 1 modulo 14.

Exercise 3-11:

For the following congruence, determine whether there exists a positive integer k so that the congruence is satisfied. If so, find the smallest such k.

$4^k \equiv 1 \pmod{19}$

Solution: Fermat's Little Theorem tells us $4^{18} \equiv 1 \pmod{19}$, so $k = 18$ is one solution, but this might not be the smallest such k.

Modulo 19												
k	1	2	3	4	5	6	7	8	9	10	...	18
4^k	4	-3	7	9	-2	11	6	5	1	4	...	1

Hence the smallest such k is 9.

[See Problem 3-97 which shows that the smallest must be a divisor of 18.]

Exercise 3-12:

Find tests for determining whether an integer in base 10 is divisible by 8.

Solution:
Since $10^3 \equiv 0 \pmod 8$ it follows that

$$a_r 10^r + a_{r-1}10^{r-1} + \cdots + a_1 10 + a_0 \equiv a_2 10^2 + a_1 10 + a_0 \pmod 8.$$

Hence a number is divisible by 8 if and only if the number represented by its last 3 decimal digits is divisible by 8.

Exercise 3-13:

Find tests for determining whether an integer in base 10 is divisible by 12.

Solution: By Proposition 3.64, $12|x$ if and only if $3|x$ and $4|x$.

Combining the tests for divisibility by 3 and 4 in base 10 we get that a number is divisible by 12 in base 10 if and only if the number determined by its last two digits is divisible by 4 and the sum of its digits is divisible by 3.

Exercise 3-14:

Find tests for determining whether an integer in base 10 is divisible by 7.

Solution: There is no very efficient test for divisibility by 7.

We have

$$\begin{aligned}
10 &\equiv 3 \pmod 7 \\
10^2 &\equiv 2 \pmod 7 \\
10^3 &\equiv 6 \equiv -1 \pmod 7 \\
10^4 &\equiv 4 \equiv -3 \pmod 7 \\
10^5 &\equiv -2 \pmod 7 \\
10^6 &\equiv 1 \pmod 7
\end{aligned}$$

and so $10^{6r} \equiv 1$, $10^{6r+1} \equiv 3$, $10^{6r+2} \equiv 2$, $10^{6r+3} \equiv -1$, $10^{6r+4} \equiv -3$, and $10^{6r+5} \equiv -2 \pmod 7$. Hence

$$\begin{aligned}
&(a_t \ldots a_4 a_3 a_2 a_1 a_0)_{10} \\
&\quad\equiv 10^t a_t + \cdots + 10^4 a_4 + 10^3 a_3 + 10^2 a_2 + 10 a_1 + a_0 \pmod 7 \\
&\quad\equiv \cdots - 3a_4 - a_3 + 2a_2 + 3a_1 + a_0 \pmod 7 \\
&\quad\equiv (\cdots - a_9 + a_6 - a_3 + a_0) + 2(\cdots - a_{11} + a_8 - a_5 + a_2) \\
&\qquad +3(\cdots - a_{10} + a_7 - a_4 + a_0) \pmod 7.
\end{aligned}$$

Hence the number on the left is divisible by 7 if and only if the number on the right is congruent to 0 modulo 7. In most cases it would be easier to just divide the original number by 7.

Exercise 3-15:

Find tests for determining whether an integer in base 8 is divisible by 7.

Solution: Since $8 \equiv 1 \pmod 7$, it follows that $8^r \equiv 1 \pmod 7$ for all positive integers r. Thus

$$\begin{aligned}(a_t \dots a_4 a_3 a_2 a_1 a_0)_8 &\equiv 8^t a_t + \cdots + 8^4 a_4 + 8^3 a_3 + 8^2 a_2 + 8a_1 + a_0 \pmod 7 \\ &\equiv a_t + \cdots + a_4 + a_3 + a_2 + a_1 + a_0 \pmod 7.\end{aligned}$$

Hence a number is divisible by 7 if and only if the sum of the digits in the base 8 representation is divisible by 7.

Exercise 3-16:

Find tests for determining whether an integer in base 12 is divisible by 13.

Solution: Since $12 \equiv -1 \pmod{13}$, we have

$$\begin{aligned}(a_t \dots a_3 a_2 a_1 a_0)_{12} &\equiv 12^t a_t + \cdots + 12^3 a_3 + 12^2 a_2 + 12a_1 + a_0 \pmod{13} \\ &\equiv (-1)^t a_t + \cdots + a_4 - a_3 + a_2 - a_1 + a_0 \pmod{13}.\end{aligned}$$

Therefore, to determine whether a number in base 12 is divisible by 13, we just need to check if the alternating sum of its digits is divisible by 13.

Exercise 3-17:

Determine whether 514000 is divisible by 2, 3, 4, 5, 6, 8, 9, 10 or 11.

Solution:

2: Yes - last digit is even.

3: No - sum of digits is 10, and $3 \nmid 10$.

4: Yes - number determined by last 2 digits is 00 and $4|00$.

5: Yes - last digit is 0.

6: No - not divisible by 3.

8: Yes - number determined by last 3 digits is 000 and $8|000$.

9: No - not divisible by 3 or sum of digits is 10 and $9 \nmid 10$.

10: Yes - last digit is 0.

11: No - alternating sum of digits is 8 and $11 \nmid 8$.

Exercise 3-18:

Determine whether 111111 is divisible by 2, 3, 4, 5, 6, 8, 9, 10 or 11.

Solution:

2: No - last digit is odd.

3: Yes - sum of digits is 6, and $3 \mid 6$.

4: No - last 2 digits not divisible by 4.

5: No - last digit not 0 or 5.

6: No - not divisible by 2.

8: No - not divisible by 2.

9: No - sum of digits is 6, and $9 \nmid 6$.

10: No - last digit not 0.

11: Yes - alternating sum of digits is 0, which is divisible by 11.

Exercise 3-19:

Determine whether 179652 is divisible by the following numbers: 2, 3, 4, 5, 6, 8, 9, 10 or 11.

Solution:

2: Yes - last digit is even.

3: Yes - sum of digits is 30, and $3 \mid 30$.

4: Yes - number determined by last 2 digits is 52 and $4 \mid 52$.

5: No - last digit is not 0 or 5.

6: Yes - divisible by both 2 and 3.

8: No - number determined by last 3 digits is 652 and $8 \nmid 652$.

9: No - sum of digits is 30 and $9 \nmid 30$.

10: No - last digit is not 0.

11: Yes - alternating sum of digits is 0 and $11 \mid 0$.

Exercise 3-20:

Determine whether 7654321 is divisible by $2, 3, 4, 5, 6, 8, 9, 10$ or 11.

Solution:

2: No - last digit is odd.

3: No - sum of digits is 28, and $3 \nmid 28$.

4: No - last 2 digits not divisible by 4.

5: No - last digit not 0 or 5.

6: No - not divisible by 2.

8: No - not divisible by 2.

9: No - sum of digits is 28, and $9 \not| 28$.

10: No - last digit not 0.

11: No - alternating sum of digits is 4, and $11 \not| 4$.

Exercise 3-21:

Check the following calculation by casting out nines.

$$12453 \times 7057 - 84014651 = 3869170$$

Solution: Modulo 9, this gives

$$6 \times 1 - 2 \equiv 7 \pmod 9$$

which is not true. Hence the original calculation contains an error.

Exercise 3-22:

Determine whether the following relation on $\mathbb{Z}$ is reflexive, symmetric, or transitive. If it is an equivalence relation, determine its quotient set.

aRb if and only if $a - b \neq 1$

Solution:

(i) This relation is reflexive because for all $a \in \mathbb{Z}$, $a - a = 0 \neq 1$. Hence aRa.

(ii) This relation is not symmetric. If aRb so that $a - b \neq 1$, then $b - a$ could be 1. For example, if $b = 1$ and $a = 0$, then $a - b = -1$ but $b - a = 1$, so that $b \not R a$.

(iii) This relation is not transitive. For example, take $a = 1$ and $c = 0$, so that $a - c = 1$ and $a \not R c$. If we now choose $b = 3$, we have $a - b = -2$ and $b - c = 3$, so aRb and bRc, but $a \not R c$.

Thus aRb is not an equivalence relation.

Exercise 3-23:

Determine whether the following relation on $\mathbb{Z}$ is reflexive, symmetric, or transitive. If it is an equivalence relation, determine its quotient set.

aRb if and only if $a \leq b$

Solution:

(i) This relation is reflexive, for all $a \in \mathbb{Z}$, $a = a$ so $a \leq a$. Hence aRa.

(ii) This relation is not symmetric. Suppose aRb, i.e. $a \leq b$. If $a < b$ then $b > a$ so $a \not R b$.

(iii) This relation is transitive. Suppose aRb and bRc i.e. $a \leq b$ and $b \leq c$. This implies that $a \leq c$ and aRc.

Thus aRb is not an equivalence relation.

Exercise 3-24:

Determine whether the following relation on $\mathbb{Z}$ is reflexive, symmetric, or transitive. If it is an equivalence relation, determine its quotient set.

aRb if and only if $a - b$ is a multiple of 3

Solution:

This is just the relation of congruence mod 3. In general, we have seen that "congruence mod n" is always an equivalence relation. The quotient set is of course just the congruence classes modulo 3.

Exercise 3-25:

Determine whether the following relation on $\mathbb{Z}$ is reflexive, symmetric, or transitive. If it is an equivalence relation, determine its quotient set.

aRb if and only if $|a - b| < 3$

Solution:

(i) This relation is reflexive. For all $a \in \mathbb{Z}$, $|a - a| = 0$ and $0 < 3$. Hence aRa.

(ii) This relation is symmetric. Suppose aRb, i.e. $|a - b| < 3$. Then

$$|b - a| = |a - b| < 3.$$

Hence bRa.

(iii) This relation is not transitive. If a and b are within distance 3 of each other, and b and c are within distance 3 of each other, then this does not imply that a and c are within distance 3 of each other.

For example, take $a = 4$, $b = 2$, and $c = 0$. Then $|a - b| = 2$, $|b - c| = 2$, and $|a - c| = 4$. That is, aRb, bRc, but $a \not R c$.

Thus aRb is not an equivalence relation.

Exercise 3-26:

Determine whether the following relation on $\mathbb{Z}$ is reflexive, symmetric, or transitive. If it is an equivalence relation, determine its quotient set.

aRb if and only if $a|b$

Solution:

(i) This is reflexive since $a|a$ for all a.

(ii) This is not symmetric, since $1|2$ but $2 \not| 1$.

(iii) This is transitive since $a|b$ and $b|c$ implies $a|c$ (by Proposition 2.11 (i)).
Hence aRb is not an equivalence relation.

Exercise 3-27:

Construct addition and multiplication tables for the following set of integers modulo m and find, if possible, multiplicative inverses of each of the elements in the set.

$\mathbb{Z}_2$

Solution:

Addition in $\mathbb{Z}_2$

$+$	$[0]$	$[1]$
$[0]$	$[0]$	$[1]$
$[1]$	$[1]$	$[0]$

Mult. in $\mathbb{Z}_2$

$\cdot$	$[0]$	$[1]$
$[0]$	$[0]$	$[0]$
$[1]$	$[0]$	$[1]$

The multiplicative inverse of $[1]$ is $[1]$ and, of course, $[0]$ does not have an inverse.

Exercise 3-28:

Construct addition and multiplication tables for the following set of integers modulo m and find, if possible, multiplicative inverses of each of the elements in the set.

$\mathbb{Z}_3$

Solution:

Addition in $\mathbb{Z}_3$

$+$	$[0]$	$[1]$	$[2]$
$[0]$	$[0]$	$[1]$	$[2]$
$[1]$	$[1]$	$[2]$	$[0]$
$[2]$	$[2]$	$[0]$	$[1]$

Multiplication in $\mathbb{Z}_3$

$\cdot$	$[0]$	$[1]$	$[2]$
$[0]$	$[0]$	$[0]$	$[0]$
$[1]$	$[0]$	$[1]$	$[2]$
$[2]$	$[0]$	$[2]$	$[1]$

The multiplicative inverse of $[1]$ is $[1]$, the multiplicative inverse of $[2]$ is $[2]$ and, of course, $[0]$ does not have an inverse.

Exercise 3-29:

Construct addition and multiplication tables for the following set of integers modulo m and find, if possible, multiplicative inverses of each of the elements in the set.

$\mathbb{Z}_7$

Solution:

Addition in $\mathbb{Z}_7$

+	[0]	[1]	[2]	[3]	[4]	[5]	[6]
[0]	[0]	[1]	[2]	[3]	[4]	[5]	[6]
[1]	[1]	[2]	[3]	[4]	[5]	[6]	[0]
[2]	[2]	[3]	[4]	[5]	[6]	[0]	[1]
[3]	[3]	[4]	[5]	[6]	[0]	[1]	[2]
[4]	[4]	[5]	[6]	[0]	[1]	[2]	[3]
[5]	[5]	[6]	[0]	[1]	[2]	[3]	[4]
[6]	[6]	[0]	[1]	[2]	[3]	[4]	[5]

Multiplication in $\mathbb{Z}_7$

·	[0]	[1]	[2]	[3]	[4]	[5]	[6]
[0]	[0]	[0]	[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]	[4]	[5]	[6]
[2]	[0]	[2]	[4]	[6]	[1]	[3]	[5]
[3]	[0]	[3]	[6]	[2]	[5]	[1]	[4]
[4]	[0]	[4]	[1]	[5]	[2]	[6]	[3]
[5]	[0]	[5]	[3]	[1]	[6]	[4]	[2]
[6]	[0]	[6]	[5]	[4]	[3]	[2]	[1]

$[1]^{-1} = [1]$, $[2]^{-1} = [4]$, $[3]^{-1} = [5]$, $[4]^{-1} = [2]$, $[5]^{-1} = [3]$, $[6]^{-1} = [6]$, and, of course, [0] does not have and inverse.

Exercise 3-30:

Construct addition and multiplication tables for the following set of integers modulo m and find, if possible, multiplicative inverses of each of the elements in the set.

$\mathbb{Z}_8$

Solution:

Addition in $\mathbb{Z}_8$

+	[0]	[1]	[2]	[3]	[4]	[5]	[6]	[7]
[0]	[0]	[1]	[2]	[3]	[4]	[5]	[6]	[7]
[1]	[1]	[2]	[3]	[4]	[5]	[6]	[7]	[0]
[2]	[2]	[3]	[4]	[5]	[6]	[7]	[0]	[1]
[3]	[3]	[4]	[5]	[6]	[7]	[0]	[1]	[2]
[4]	[4]	[5]	[6]	[7]	[0]	[1]	[2]	[3]
[5]	[5]	[6]	[7]	[0]	[1]	[2]	[3]	[4]
[6]	[6]	[7]	[0]	[1]	[2]	[3]	[4]	[5]
[7]	[7]	[0]	[1]	[2]	[3]	[4]	[5]	[6]

Multiplication in $\mathbb{Z}_8$

x	[0]	[1]	[2]	[3]	[4]	[5]	[6]	[7]
[0]	[0]	[0]	[0]	[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]	[4]	[5]	[6]	[7]
[2]	[0]	[2]	[4]	[6]	[0]	[2]	[4]	[6]
[3]	[0]	[3]	[6]	[1]	[4]	[7]	[2]	[5]
[4]	[0]	[4]	[0]	[4]	[0]	[4]	[0]	[4]
[5]	[0]	[5]	[2]	[7]	[4]	[1]	[6]	[3]
[6]	[0]	[6]	[4]	[2]	[0]	[6]	[4]	[2]
[7]	[0]	[7]	[6]	[5]	[4]	[3]	[2]	[1]

The following elements have multiplicative inverses:

$$[1]^{-1} = [1], \quad [3]^{-1} = [3], \quad [5]^{-1} = [5], \quad [7]^{-1} = [7].$$

Exercise 3-31:

If $d = \gcd(a, m)$ and $d|c$, then show that the congruence $ax \equiv c \pmod{m}$ is equivalent to

$$\frac{a}{d}x \equiv \frac{c}{d} \pmod{\frac{m}{d}}.$$

Solution:

The integer x is a solution of $ax \equiv c \pmod{m}$ if and only if $m|ax - c$. Now $m|ax - c$ if and only if there exists an integer q such that $ax - c = qm$, or equivalently, such that

$$\frac{a}{d}x - \frac{c}{d} = q\frac{m}{d}$$

where $\gcd(a, m) = d$. This happens if and only if

$$\frac{a}{d}x \equiv \frac{c}{d} \pmod{\frac{m}{d}}.$$

Exercise 3-32:

Solve the congruence

$$3x \equiv 5 \pmod{13}.$$

Solution:

Since the $\gcd(3, 13) = 1$, this congruence has exactly one congruence class of solutions modulo 13. Applying the Euclidean Algorithm to 3 and 13, we see that it terminates after one step.

$$13 = 4 \cdot 3 + 1$$

Therefore, $(-4) \cdot 3 \equiv 1 \pmod{13}$. We proceed by multiplying both sides of the original equation by -4.

$$(-4) \cdot 3x \equiv (-4) \cdot 5 \pmod{13}$$

$$x \equiv 6 \pmod{13}$$

Check: $3 \cdot 6 = 18 \equiv 5 \pmod{13}$.

Exercise 3-33:

Solve the congruence

$$4x \equiv 6 \pmod{14}.$$

Solution:

This is equivalent to the Diophantine equation

$$4x + 14y = 6 \text{ for some } y \in \mathbb{Z}.$$

Now $\gcd(4, 14) = 2$ and $2|6$ so the congruence has a solution. By inspection $4(-2) + 14(1) = 6$ Hence $x = -2$, $y = 1$ is one solution to the Diophantine equation.

By the Linear Congruence Theorem 3.54 the complete solution to the congruence is

$$\begin{array}{rrcl} & x & \equiv & -2 \pmod{\frac{14}{2}} \\ \text{that is} & x & \equiv & 5 \pmod{7} \end{array}$$

or as

$$\begin{array}{rrcl} & x & \equiv & 5,\ 5+7 \pmod{14} \\ \text{that is} & x & \equiv & 5,\ 12, \pmod{14}. \end{array}$$

Check: $(4)(5) - 6 \equiv 14 \equiv 0 \pmod{14}$.

Exercise 3-34:

Solve the congruence

$$5x \equiv 7 \pmod{15}.$$

Solution:

Here, $\gcd(5, 15) = 5$, but $5 \not| 7$, so there is no solution.

Exercise 3-35:

Solve the congruence

$$29x \equiv 43 \pmod{128}.$$

Solution:

The congruence is equivalent to the Diophantine equation

$$29x + 128y = 43, \text{ for some } y \in \mathbb{Z}.$$

Since $\gcd(29, 128) = 1$, we can find a solution to $29x + 128y = 1$ by applying the Euclidean Algorithm to 29 and 128.

$29x$	$+128y$	$=\ r$
1	0	29
0	1	128
1	0	29
-4	1	12
9	-2	5
-22	5	2
53	-12	1

Hence one solution to $29x + 128y = 1$ is $x = 53$, $y = -12$. Multiplying by 43, we obtain

$$29(2279) + 128(-516) = 43.$$

Therefore $x = 2279$ is one integer solution to $29x \equiv 43 \pmod{128}$. Since $2279 \equiv 103 \pmod{128}$, it follows from the Linear Congruence Theorem 3.54 that the complete solution to the congruence is

$$x \equiv 103 \pmod{128}.$$

Check: $(29)(103) - 43 \equiv 23(128) \equiv 0 \pmod{128}$.

Exercise 3-36:

Solve the congruence

$$1713x \equiv 871 \pmod{2000}.$$

Solution: This is equivalent to the Diophantine equation

$$1713x + 2000y = 871 \text{ for some } y \in \mathbb{Z}.$$

We use the Extended Euclidean Algorithm to calculate the $\gcd(1713, 2000)$.

$2000y$	$+1713x$	$=\ r$	q_i
1	0	2000	
0	1	1713	
1	-1	287	1
-5	6	278	5
6	-7	9	1
-185	216	8	30
191	-223	1	1
-1713	2000	0	8

Hence $\gcd(1713, 2000) = 1$ and the congruence has a solution. The above calculations shows that

$$1713(-223) + 2000(191) = 1.$$

Multiplying by 871 we get

$$1713(-194233) + 2000(166361) = 871.$$

Hence $x = -194233$, $y = 166361$ is one solution to the Diophantine equation. By the Linear Congruence Theorem 3.54, the complete solution to the congruence is

$$\begin{aligned} x &\equiv -194233 \pmod{2000} \\ \text{i.e.} \quad x &\equiv 1767 \pmod{2000}. \end{aligned}$$

Check: $(1713)(1767) - 871 \equiv 3026000 \equiv 0 \pmod{2000}$.

Exercise 3-37:

Solve the congruence

$$1426x \equiv 597 \pmod{2000}.$$

Solution:

There can be no solution since $\gcd(1426, 2000) = 2$ and 2 does not divide 597.

Exercise 3-38:

Solve the congruence

$$x^2 \equiv 6x \pmod{8}.$$

Solution: Consider the following table.

Modulo 8								
$x \equiv$	0	1	2	3	4	5	6	7
$x^2 \equiv$	0	1	4	1	0	1	4	1
$6x \equiv$	0	6	4	2	0	6	4	2

Therefore x is a solution to $x^2 \equiv 6x \pmod{8}$ iff $x \equiv 0, 2, 4, 6 \pmod{8}$

Note: We could write the solution as $x \equiv 0 \pmod{2}$; that is, x is even.

Check: If $x = 2k$ for $k \in \mathbb{Z}$ then $4k^2 - 12k = 4k(k-3)$ and one of k and $k-3$ is even. Therefore $8|x^2 - 6x$.

Exercise 3-39:

Solve the congruence

$$x^2 + 2x \equiv 3 \pmod{8}.$$

Solution: Consider the following table.

Modulo 8								
$x \equiv$	0	1	2	3	4	5	6	7
$x^2 \equiv$	0	1	4	1	0	1	4	1
$x^2 + 2x \equiv$	0	3	0	7	0	3	0	7

From the above table we see that $x^2 + 2x \equiv 3 \pmod 8$ if

$$x \equiv 1 \text{ or } 5 \pmod 8.$$

Exercise 3-40:

Solve the congruence

$$4x^3 + 2x + 1 \equiv 0 \pmod 5.$$

Solution:

Modulo 5					
$x \equiv$	0	1	2	3	4
$x^3 \equiv$	0	1	3	2	4
$4x^3 + 2x + 1 \equiv$	1	2	0	2	0

Hence the complete solution is $x \equiv 2 \text{ or } 4 \pmod 5$

Exercise 3-41:

Solve the congruence

$$x^9 + x^7 + x^6 + 1 \equiv 0 \pmod 2.$$

Solution: If x is even then the left side is odd, and if x is odd then the left side is even. Hence the solution to the congruence is $x \equiv 1 \pmod 2$; that is, x is odd.

Exercise 3-42:

Find the inverse of $[4]$ in $\mathbb{Z}_{11}$.

Solution: We have to solve the following congruence.

$$\begin{aligned} 4x &\equiv 1 \pmod{11} \\ 4x &\equiv 12 \pmod{11} \\ x &\equiv 3 \pmod{11}, \text{ since } \gcd(4, 11) = 1 \end{aligned}$$

Therefore, $[4]^{-1} = [3]$ in $\mathbb{Z}_{11}$.
Check: $[4][3] = [12] = [1]$ in $\mathbb{Z}_{11}$.

Exercise 3-43:

Find the inverse of $[2]$ in $\mathbb{Z}_{41}$.

Solution: We have to solve the following congruence.

$$\begin{aligned} 2x &\equiv 1 \pmod{41} \\ 2x &\equiv 42 \pmod{41} \\ x &\equiv 21 \pmod{41} \text{ since } \gcd(2,41) = 1 \end{aligned}$$

Therefore $[2]^{-1} = [21]$ in $\mathbb{Z}_{41}$.

Check: $2(21) \equiv 1 \pmod{41}$.

Exercise 3-44:

Find the inverse of $[23]$ in $\mathbb{Z}_{41}$.

Solution: We must solve $23x \equiv 1 \pmod{41}$. Apply the Extended Euclidean Algorithm to 41 and 23.

$41y + 23x = r$			q_i
1	0	41	
0	1	23	
1	−1	18	1
−1	2	5	1
4	−7	3	1
−5	9	2	3
9	−16	1	1
−23	41	0	1

Hence $23(-16) + 41(9) = 1$. Therefore $23(-16) \equiv 1 \pmod{41}$ and

$$[23]^{-1} = [-16] = [25] \in \mathbb{Z}_{41}.$$

Check: $23 \cdot 25 = 575 = 14 \cdot 41 + 1$.

Exercise 3-45:

Solve the equation $[4][x] + [8] = [1]$ in $\mathbb{Z}_9$.

Solution:

$[4][x] + [8] = [4x + 8] = [1]$. This is equivalent to solving

$$\begin{aligned} 4x &\equiv -7 \pmod{9} \\ 4x &\equiv 2 \pmod{9}. \end{aligned}$$

This congruence is equivalent to the Diophantine Equation $4x+9y = 2$ for $y \in \mathbb{Z}$. Since $\gcd(4,9) = 1$, the congruence equation has a solution. By inspection $4(-4) + 9(2) = 2$. Therefore $x = -4$ and $y = 2$ is a particular solution. By Theorem 3.54, the complete solution is

$$\begin{aligned} x &\equiv -4 \pmod{9} \\ &\equiv 5 \pmod{9} \\ [x] &= [5] \in \mathbb{Z}_9. \end{aligned}$$

Check: $[4][5] + [8] = [28] = [1] \in \mathbb{Z}_9$

Exercise 3-46:

Solve the equation $[3][x] = [18]$ in $\mathbb{Z}_{19}$.

Solution: This is equivalent to solving

$$\begin{aligned} 3x &\equiv 18 \pmod{19}. \\ x &\equiv 6 \pmod{19} \quad \text{since } \gcd(3, 19) = 1. \end{aligned}$$

Therefore $[x] = [6]$ is the complete solution.

Exercise 3-47:

Solve the equation $([x] - [2])([x] - [3]) = [0]$ in $\mathbb{Z}_6$.

Solution: Consider the following table.

Modulo 6						
$x \equiv$	0	1	2	3	4	5
$x - 2 \equiv$	-2	-1	0	1	2	3
$x - 3 \equiv$	-3	-2	-1	0	1	2
$(x - 2)(x - 3) \equiv$	0	2	0	0	2	0

Therefore $(x - 2)(x - 3) \equiv 0 \pmod{6}$ for $x \equiv 0, 2, 3, 5 \pmod{6}$ and the solutions are $x = [0], [2], [3], [5] \in \mathbb{Z}_6$.

Exercise 3-48:

For what integer values of a does $x^2 \equiv a \pmod{7}$ have a solution?

Solution: Consider all the squares modulo 7.

Modulo 7							
$x \equiv$	0	1	2	3	4	5	6
$x^2 \equiv$	0	1	4	2	2	4	1

Thus $x^2 \equiv a \pmod{7}$ has a solution for $a \equiv 0, 1, 2, 4 \pmod{7}$.

Exercise 3-49:

Solve the following simultaneous congruence:

$$\begin{aligned} x &\equiv 4 \pmod{5} \\ x &\equiv 3 \pmod{4}. \end{aligned}$$

Solution: By the Chinese Remainder Theorem the system of congruences has a solution, since $\gcd(5, 4) = 1$.

An integer x satisfies the first congruence if and only if $x = 4 + 5y$ for some $y \in \mathbb{Z}$. Substitute this value of x into the second congruence,

$$\begin{aligned} 4 + 5y &\equiv 3 \pmod 4 \\ y &\equiv 3 \pmod 4. \end{aligned}$$

This is equivalent to $y = 3 + 4z$ for some $z \in \mathbb{Z}$. The solution for both congruences is therefore

$$x = 4 + 5(3 + 4z) = 19 + 20z;$$

that is, $x \equiv 19 \pmod{20}$.

Check: $19 + 20z \equiv 3 \pmod 4$ and $19 + 20z \equiv 4 \pmod 5$.

Exercise 3-50:

Solve the following simultaneous congruences.

$$\begin{aligned} x &\equiv 46 \pmod{51} \\ x &\equiv 27 \pmod{52} \end{aligned}$$

Solution: By the Chinese Remainder Theorem the system of congruences has a solution, since $\gcd(51, 52) = 1$.

Now convert one congruence to an integer equation, involving another variable, and substitute into the other congruence. [A useful trick is to choose the larger congruence to convert, as the resulting congruence you have to solve will be of smaller modulus.]

An integer x satisfies the second congruence if and only if $x = 27 + 52y$ for some $y \in \mathbb{Z}$. Substitute this into the first congruence.

$$\begin{aligned} 27 + 52y &\equiv 46 \pmod{51} \\ y &\equiv 52y \equiv 46 - 27 \equiv 19 \pmod{51} \end{aligned}$$

The complete solution for y is $y = 19 + 51n$ for $n \in \mathbb{Z}$. Hence

$$x = 27 + (19 + 51n)52 = 1015 + 51 \cdot 52n$$

for $n \in \mathbb{Z}$. Therefore, the complete solution for x is $x \equiv 1015 \pmod{2652}$.

Check: If $x = 1015 + 2652z$ then $x \equiv 46 \pmod{51}$ and $x \equiv 27 \pmod{52}$.

Exercise 3-51:

Solve the following simultaneous congruences.

$$\begin{aligned} x &\equiv 1 \pmod 2 \\ x &\equiv 2 \pmod 3 \\ x &\equiv 3 \pmod 7 \end{aligned}$$

Solution: By the Chinese Remainder Theorem, the first two congruences have a unique solution, since $\gcd(2,3) = 1$, and the solution is one congruence class modulo 6. Again by the Chinese Remainder Theorem, the solution to the first two congruences and the last congruence have a unique solution, since $\gcd(6,7) = 1$, and the solution is one congruence class modulo 42.

Now, $x \equiv 1 \pmod 2$ and $x \equiv 2 \pmod 3$ are equivalent to $x \equiv -1 \pmod 2$ and $x \equiv -1 \pmod 3$ respectively. Hence, by Proposition 3.64, the solution to the first two is $x \equiv -1 \pmod 6$.

We have reduced the three simultaneous congruences to two simultaneous congruences.

$$\begin{aligned} x &\equiv -1 \pmod 6 \\ x &\equiv 3 \pmod 7. \end{aligned}$$

An integer x satisfies the second congruence if and only if $x = 3 + 7y$ for $y \in \mathbb{Z}$. Substitute this into the first congruence.

$$\begin{aligned} 3 + 7y &\equiv -1 \pmod 6 \\ y &\equiv 7y \equiv -1 - 3 \equiv 2 \pmod 6 \end{aligned}$$

This is equivalent to $y = 2 + 6z$ for $z \in \mathbb{Z}$. The solution for both congruences is therefore

$$x = 3 + (2 + 6z)7 = 17 + 42z.$$

That is $x \equiv 17 \pmod{42}$.

Check: $17+42z \equiv 1 \pmod 2$, $17+42z \equiv 2 \pmod 3$, $17+42z \equiv 3 \pmod 7$.

Exercise 3-52:

Solve the following simultaneous congruences.

$$\begin{aligned} 2x &\equiv 11 \pmod{13} \\ 3x &\equiv 7 \pmod 9 \\ 7x &\equiv 5 \pmod 8 \end{aligned}$$

Solution: Because $\gcd(3,9) = 3$ which does not divide 7, the second congruence $3x \equiv 7 \pmod 9$ has no solutions. Hence the system has no solutions.

Exercise 3-53:

Solve the following simultaneous congruences.

$$\begin{aligned} 2x &\equiv 4 \pmod 7 \\ 18x &\equiv 43 \pmod{23} \end{aligned}$$

Solution:
As $\gcd(2,7) = 1$, the first congruence has one solution modulo 7, by Theorem

3.54. Now $x \equiv 2 \pmod 7$ satisfies the congruence, so it must be the complete solution.

The second congruence can be rewritten as $18x \equiv 20 \pmod{23}$. This is equivalent to the Diophantine equation

$$18x + 23y = 20 \text{ for some } y \in \mathbb{Z}.$$

Apply the Extended Euclidean Algorithm to 23 and 18.

$23y$	$+18x$	$= r$	q_i
1	0	23	
0	1	18	
1	−1	5	1
−3	4	3	3
4	−5	2	1
−7	9	1	1
18	−23	0	1

As $\gcd(18, 23) = 1$, the equation has a solution. The next to last row shows that $18(9) + 23(-7) = 1$. Multiplying by 20 gives $18(180) + 23(-140) = 20$. Therefore $x = 180$ and $y = -140$ is a particular solution to the Diophantine equation. By Theorem 3.54, the complete solution to the second congruence is

$$\begin{aligned} x &\equiv 180 \pmod{23} \\ &\equiv 19 \pmod{23}. \end{aligned}$$

Hence the given system of simultaneous congruences is equivalent to the system

$$\begin{aligned} x &\equiv 2 \pmod 7 \\ x &\equiv 19 \pmod{23}. \end{aligned}$$

As $\gcd(7, 23) = 1$, the Chinese Remainder Theorem shows that the system has one solution modulo $7 \cdot 23$.

An integer x satisfies the second congruence if and only if $x = 19 + 23y$ for $y \in \mathbb{Z}$. Substituting into the first congruence,

$$\begin{aligned} 19 + 23y &\equiv 2 \pmod 7 \\ 2y &\equiv 4 \pmod 7. \end{aligned}$$

Since $\gcd(2, 7) = 1$, this has the solution $y \equiv 2 \pmod 7$, which is equivalent to $y = 2 + 7z$ for $z \in \mathbb{Z}$.

The solution for both congruences is therefore

$$x = 19 + 23(2 + 7z) = 65 + 161z \quad \text{for all } x \in \mathbb{Z}.$$

That is, $x \equiv 65 \pmod{161}$.

Alternate Solution:
As $\gcd(2, 7) = 1$, the first congruence has one solution modulo 7, by Theorem

3.54. Now $x \equiv 2 \pmod 7$ satisfies the congruence, so it must be the complete solution, and $x = 2 + 7y$ for $y \in \mathbb{Z}$.

Substitute this into to second congruence and determine if there is a solution.

$$\begin{aligned} 18x &\equiv 43 \pmod{23} \\ 18(2+7y) &\equiv 43 \pmod{23} \\ 126y &\equiv 43 - 36 \pmod{23} \\ 11y &\equiv 7 \pmod{23} \\ 22y &\equiv 14 \pmod{23} \\ y &\equiv -14 \equiv 9 \pmod{23} \end{aligned}$$

Hence there is a solution to both congruences and it is

$$x = 2 + 7(9 + 23z) = 65 + 161z \quad \text{for all } x \in \mathbb{Z}.$$

That is, $x \equiv 65 \pmod{161}$.

Check: If $x = 65+161z$ then $2x \equiv 130 \equiv 4 \pmod 7$. Now $x \equiv -4 \pmod{23}$, so $18x \equiv -72 \equiv -3 \equiv 43 \pmod{23}$.

Exercise 3-54:

Solve the following simultaneous congruences.

$$\begin{aligned} 161x &\equiv 49 \pmod{200} \\ 74x &\equiv 1 \pmod{53} \end{aligned}$$

Solution:

The first congruence is equivalent to the Diophantine Equation $161x+200y = 49$ for some $y \in \mathbb{Z}$. Apply the Extended Euclidean Algorithm to 200 and 161.

$200y + 161x = r$			q_i
1	0	200	
0	1	161	
1	−1	39	1
−4	5	5	4
29	−36	4	7
−33	41	1	1
200	−161	0	7

The $\gcd(200, 161) = 1$, so the congruence has a solution. From the next t last row we see that $161(41) + 200(-33) = 1$. Multiplying by 49 gives

$$161(2009) + 200(-1617) = 49.$$

Therefore $x = 1763$ and $y = -1617$ is a particular solution, and by Theorem 3.54, the complete solution to the congruence is

$$\begin{aligned} x &\equiv 2009 \pmod{200} \\ &\equiv 9 \pmod{200}. \end{aligned}$$

An integer x satisfies the first congruence if and only if $x = 9 + 200y$ for some $y \in \mathbb{Z}$. Substitute this into the second congruence and determine if there is a solution.

$$\begin{aligned} 74(9 + 200y) &\equiv 1 \pmod{53} \\ 14800y &\equiv -665 \pmod{53} \\ 13y &\equiv 24 \pmod{53} \end{aligned}$$

This is equivalent to the Diophantine Equation $13y + 53s = 24$. This has a solution, since $\gcd(13, 53) = 1$. Either apply the Extended Euclidean Algorithm to 13 and 53, or notice that

$$\begin{aligned} 13(-4) + 53 &= 1 \\ 13(-96) + 53(24) &= 24. \end{aligned}$$

Therefore $y = -96$ and $s = 24$ is a particular solution, and by Theorem 3.54, the complete solution to the congruence $13y \equiv 24 \pmod{53}$ is

$$\begin{aligned} y &\equiv -96 \pmod{53} \\ &\equiv 10 \pmod{53}. \end{aligned}$$

So $y = 10 + 53z$ for $z \in \mathbb{Z}$.

The solution for both congruences is therefore

$$x = 9 + 200(10 + 53z) = 2009 + 10600z \quad \text{for } z \in \mathbb{Z}$$

That is, $x \equiv 2009 \pmod{10600}$.

Check: If $x = 2009 + 10600z$ then

$$\begin{aligned} 161x &\equiv 161 \cdot (2009) \equiv 323449 \equiv 49 \pmod{200} \\ 74x &\equiv 74 \cdot (2009) \equiv 148666 \equiv 1 \pmod{53}. \end{aligned}$$

Exercise 3-55:

Find the two smallest positive integer solutions of $x \equiv 5 \pmod{7}$ and $x \equiv 24 \pmod{25}$.

Solution: We must first solve the system of congruences

$$\begin{aligned} x &\equiv 5 \pmod{7} \\ x &\equiv 24 \pmod{25}. \end{aligned}$$

Since $\gcd(7, 25) = 1$, the Chinese Remainder Theorem tells us that the system of congruences has a solution modulo 175.

An integer x satisfies the congruence $x \equiv 5 \pmod{7}$ if and only if

$$x = 5 + 7y \text{ for some } y \in \mathbb{Z}.$$

Substituting into the second congruence we have

$$\begin{aligned} 5+7y &\equiv 24 \pmod{25} \\ 7y &\equiv 19 \pmod{25}. \end{aligned}$$

This is equivalent to the equation $7y + 25s = 19$ for some $s \in \mathbb{Z}$. By inspection $7(-7) + 25(2) = 1$, multiplying by 19 gives $7(-133) + 25(38) = 19$. Hence $y = -133$ and $s = 38$ is a particular solution to the equation. Therefore the complete solution of the congruence is

$$\begin{aligned} y &\equiv -133 \pmod{25} \\ &\equiv 17 \pmod{25} \end{aligned}$$

This is equivalent to $17 + 25z = y$ for $z \in \mathbb{Z}$. The solution for both congruences is therefore

$$x = 5 + 7(17 + 25z) = 124 + 175z$$

or equivalently

$$x \equiv 124 \pmod{175}.$$

The smallest positive solutions occur when $z = 0$ and 1, so $x = 124$ and 299.
Check: $124 - 5 \equiv 119 \equiv 0 \pmod 7$ and $124 - 24 \equiv 100 \equiv 0 \pmod{25}$.

Problem 3-56:

If p is a prime, prove that $x^2 \equiv y^2 \pmod p$ if and only if $x \equiv \pm y \pmod p$.

Solution:

Let $x^2 \equiv y^2 \pmod p$. Then $x^2 - y^2 \equiv 0 \pmod p$; i.e. $(x+y)(x-y) \equiv 0 \pmod p$ and $p|(x+y)(x-y)$ Since p is prime, by Theorem 2.53 either $p|x+y$ or $p|x-y$; i.e.

$$\begin{aligned} x &\equiv -y \text{ or } x \equiv y \pmod p \\ x &\equiv \pm y \pmod p. \end{aligned}$$

Conversely suppose $x \equiv \pm y \pmod p$. Then, squaring, $x^2 \equiv y^2 \pmod p$.

Problem 3-57:

If p is an odd prime, show that $x^2 \equiv a \pmod p$ has a solution for exactly half the values of a between 1 and $p-1$ inclusive. Furthermore, if $1 \le a \le p-1$ and $x^2 \equiv a \pmod p$ has a solution, show that it has exactly two congruence classes of solutions modulo p.

Solution:

We use the result of Problem 3-56 that, for p prime, $x^2 \equiv y^2 \pmod p$ if and only if $x \equiv \pm y \pmod p$. In particular, $x^2 \equiv 0 \pmod p$ if and only if $x \equiv 0 \pmod p$.

Note that if $1 \le i < p/2$ then $p/2 < p - i \le p - 1$ and

$$(p-i)^2 \equiv (-i)^2 \equiv i^2 \pmod p.$$

Hence if $x^2 \equiv a \pmod{p}$ has a solution where $a \not\equiv 0 \pmod{p}$, then there exists i with $1 \leq i < p/2$ and $i^2 \equiv a \pmod{p}$. Therefore the values of $a \not\equiv 0 \pmod{p}$ for which the congruence $x^2 \equiv a \pmod{p}$ has a solution are congruent to

$$1^2,\ 2^2,\ 3^2,\ \ldots, \left(\frac{p-1}{2}\right)^2 \pmod{p}.$$

Some of these squares could give the same congruence class modulo p, though we shall now show that they are all distinct. Suppose

$$i^2 \equiv j^2 \pmod{p} \quad \text{with } 1 \leq j \leq i < p/2.$$

Then $p|(i-j)(i+j)$ and, since p is prime, it follows from Theorem 2.53 that either $p|i+j$ or $p|i-j$. However $2 \leq i+j < p$ and $0 \leq i-j < p/2$, so the only possibility is $i-j=0$. Therefore the congruence classes $1^2, 2^2, \ldots, (\frac{p-1}{2})^2$ are all distinct modulo p and there are $\frac{p-1}{2}$ possible values for a between 1 and $p-1$.

Therefore the congruence $x^2 \equiv a \pmod{p}$ has a solution for exactly half the values of a between 1 and $p-1$. If $x^2 \equiv a \pmod{p}$ has a solution with $1 \leq a \leq p-1$ then there are exactly two congruence classes of solutions modulo p of the form $x \equiv i,\ p-i \pmod{p}$ for $1 \leq i < p/2$.

Problem 3-58:

Does $x^3 \equiv a \pmod{p}$ always have a solution for every value of a, whenever p is prime?

Solution:

The congruence $x^3 \equiv a \pmod{p}$ does not always have a solution for every a and every prime p.

For example, when $p = 7$:

Modulo 7							
$x \equiv$	1	2	3	4	5	6	0
$x^3 \equiv$	1	1	6	1	6	6	0

So the equation $x^3 \equiv 2 \pmod{7}$, for example, has no solution.

Problem 3-59:

Choose any integer larger than 10, subtract the sum of its digits from it, cross out one nonzero digit from the result, and let the sum of the remaining digits be s. From a knowledge of s alone, is it possible to find the digit that was crossed out?

Solution:

Let the integer be $x > 10$, so it has at least 2 digits and the described procedure is possible. If the sum of the digits of x is $d_r + \cdots + d_1 + d_0$ then $x - (d_r + \cdots + d_1 + d_0) \equiv 0 \pmod{9}$ by Theorem 3.21. If $x - (d_r + \cdots d_1 + d_0) = y_t y_{t-1} \ldots y_1 y_0$ then $y_i + y_1 + \cdots + y_t \equiv 0 \pmod{9}$. If we cross out some digit,

say y_i, then the sum of the remaining digits, $s = y_0 + y_1 + \cdots + y_t - y_i \equiv -y_i \pmod 9$. Hence $y_i \equiv -s \pmod 9$. Since y_i is nonzero, $1 \leq y_i \leq 9$ and y_i can be determined from s.

[Note that $0 \equiv 9 \pmod 9$, so if we crossed out a zero digit, we could not distinguish that from crossing out a 9, from the knowledge of s alone.]

Problem 3-60:

Prove that $21|(3n^7 + 7n^3 + 11n)$ for all integers n.

Solution:

The relation $21|(3n^7 + 7n^3 + 11n)$ holds if and only if both the following congruences hold.

$$\begin{aligned} 3n^7 + 7n^3 + 11n &\equiv 0 \pmod 3 \\ 3n^7 + 7n^3 + 11n &\equiv 0 \pmod 7 \end{aligned}$$

The first congruence is equivalent to $n^3 + 2n \equiv 0 \pmod 3$ and this holds for all n by Fermat's Little Theorem because $n^3 \equiv n \pmod 3$. The second congruence is equivalent to $3n^7 + 4n \equiv 0 \pmod 7$ which also holds for all n by Fermat's Little Theorem because $n^7 \equiv n \pmod 7$. Hence the divisibility relation holds for all integers n.

Problem 3-61:

Prove that $n^{91} \equiv n^7 \pmod{91}$ for all integers n. Is $n^{91} \equiv n \pmod{91}$ for all integers n?

Solution: Since $91 = 7 \cdot 13$, 91 is not prime. By Fermat's Little Theorem $n^6 \equiv 1 \pmod 7$ for all n coprime to 7. Hence

$$n^{91} \equiv (n^6)^{15} n \equiv 1^{15} \cdot n \equiv n \equiv n^7 \pmod 7.$$

This is true even if $7|n$.

Also by Fermat's little theorem, $n^k \equiv 1 \pmod{13}$ if $13 \nmid k$. Hence

$$n^{91} \equiv (n^{12})^7 n^7 \equiv n^7 \pmod{13}.$$

This congruence is still true if $13|n$.

Hence we have the two congruences

$$\begin{aligned} n^{91} &\equiv n^7 \pmod 7 \\ n^{91} &\equiv n^7 \pmod{13} \end{aligned}$$

for all integers n. By Proposition 3.64 this is equivalent to

$$n^{91} \equiv n^7 \pmod{91}.$$

From what we have proved above, the congruence $n^{91} \equiv n \pmod{91}$ is equivalent to $n^7 \equiv n \pmod{91}$, which is also equivalent to the two congruences $n^7 \equiv n \pmod 7$ and $n^7 \equiv n \pmod{13}$.

However, $2^7 \equiv 128 \equiv -2 \not\equiv 2 \pmod{13}$. Hence $2^{91} \equiv 2^7 \not\equiv 2 \pmod{91}$ and so $n^{91} \not\equiv n \pmod{91}$ for all n.

Problem 3-62:

For which positive values of k is $n^k \equiv n \pmod 6$ for all integers n?

Solution: The congruence $n^k \equiv n \pmod 6$ if and only if the simultaneous congruences

$$\begin{aligned} n^k &\equiv n \pmod 2 \\ n^k &\equiv n \pmod 3 \end{aligned}$$

hold for all n. The first congruence holds for all k, since if n is odd, both sides are congruent to 1, and if n is even, both sides are congruent to 0.

If k is odd, say $k = 2j + 1$, the second congruence holds for all n since, if $n \not\equiv 0 \pmod 3$, we can use Fermat's Little Theorem to obtain

$$n^k \equiv n^{2j+1} \equiv \left(n^2\right)^j n \equiv 1^j n \equiv n \pmod 3.$$

If $n \equiv 0 \pmod 3$, then both sides are congruent to 0.

If k is even however, say $k = 2j$, the second congruence does not hold for all n. For example, if $n \equiv 2 \pmod 3$ then

$$n^k \equiv 2^{2j} \equiv \left(2^2\right)^j \equiv 1^j \equiv 1 \not\equiv n \pmod 3.$$

Therefore $n^k \equiv n \pmod 6$, for all n, if and only if k is odd.

Problem 3-63:

For which positive values of k is $n^k \equiv n \pmod 4$ for all integers n?

Solution: If $k = 1$ then $n^k = n$ so the congruence $n^k \equiv n \pmod 4$ holds.

For $k \geq 2$, choose n such that $n \equiv 2 \pmod 4$. Then

$$n^k \equiv 2^k \equiv 2^2 2^{k-2} \equiv 0 \cdot 2^{k-2} \equiv 0 \not\equiv 2 \equiv n \pmod 4.$$

Hence the congruence is not satisfied for all integers n.

Therefore $n^k \equiv n \pmod 4$, for all integers n, if and only if $k = 1$.

Problem 3-64:

For which positive values of k is $n^k \equiv n \pmod 7$ for all integers n?

Solution: We shall show that the possible values of k are the positive integers with $k \equiv 1 \pmod 6$.

We first show that if $k \equiv 1 \pmod 6$, then $n^k \equiv n \pmod 7$. Let $k = 6m+1$ for some $m \in \mathbb{Z}$. Then $m \geq 0$ as $k > 0$. If $n \equiv 0 \pmod 7$, then certainly $n^k \equiv 0^k \equiv 0 \equiv n \pmod 7$. If $n \not\equiv 0 \pmod 7$ then, using Fermat's Little Theorem, we have

$$n^k \equiv n^{6m+1} \equiv \left(n^6\right)^m n \equiv 1^m n \equiv n \pmod 7.$$

Now we need to show that if $n^k \equiv n \pmod 7$, for all $n \in \mathbb{Z}$, then $k \equiv 1 \pmod 6$. Let $k = 6q + r$ with $0 \leq r < 6$, $q, r \in \mathbb{Z}$. Then $q \geq 0$ as $k > 0$.

Since $n^k \equiv n \pmod 7$ for all n, it certainly must hold for all n not divisible by 7. For these n, Fermat's Little Theorem yields $n^6 \equiv 1 \pmod 7$. So

$$n \equiv n^k \equiv n^{6q+r} \equiv (n^6)^q n^r \equiv 1^q n^r \equiv n^r \pmod 7.$$

For $r = 1$, this is certainly true, but for $r = 0, 2, 3, 4, 5$, there are integers n that do not satisfy this:

$$\begin{array}{ll} 2^0 \equiv 1 \not\equiv 2 \pmod 7; & 2^2 \equiv 4 \not\equiv 2 \pmod 7; \\ 2^3 \equiv 8 \not\equiv 2 \pmod 7; & 3^4 \equiv 4 \not\equiv 3 \pmod 7; \\ 2^5 \equiv 4 \not\equiv 2 \pmod 7. & \end{array}$$

Therefore we must have $r = 1$; i.e., $k = 6q + 1$ and $k \equiv 1 \pmod 6$.

Problem 3-65:

Prove, without using a calculator, that 641 divides the Fermat number

$$F(5) = 2^{2^5} + 1.$$

Solution:

We have to show that $2^{2^5} + 1 \equiv 0 \pmod{641}$; i.e. $2^{32} \equiv -1 \pmod{641}$. We therefore need to compute large powers of 2 modulo 641. We note that $641 = 640 + 1 = 2^7 \cdot 5 + 1$, so

$$\begin{aligned} 2^7 \cdot 5 &\equiv -1 \pmod{641} \\ (2^7 \cdot 5)^4 &\equiv (-1)^4 \pmod{641} \\ 2^{28} \cdot 625 &\equiv 1 \pmod{641} \\ 2^{28}(-16) &\equiv 1 \pmod{641}, \quad \text{since } 625 \equiv -16 \pmod{641} \\ -2^{32} &\equiv 1 \pmod{641} \\ 2^{32} &\equiv -1 \pmod{641}. \end{aligned}$$

Therefore, $641 | 2^{32} + 1$.

Problem 3-66:

Show that the product of two numbers of the form $4n + 1$ is still of that form. Hence show that there are infinitely many primes of the form $4n + 3$.

Solution:

If x is of the form $4n + 1$ then $x \equiv 1 \pmod 4$. If y is of the form $4n + 1$ then $y \equiv 1 \pmod 4$. Hence $xy \equiv 1 \pmod 4$, and is of the form $4n + 1$.

Suppose that there are only finitely many primes of the form $4n + 3$, say $p_1, p_2, \ldots, p_k$. Then their product

$$\begin{aligned} p_1 \cdot p_2 \cdots p_k &\equiv 3^k \pmod 4 \\ &\equiv (-1)^k \pmod 4 \\ &\equiv \begin{cases} 1 \pmod 4 & \text{if } k \text{ is even} \\ 3 \pmod 4 & \text{if } k \text{ is odd .} \end{cases} \end{aligned}$$

If k is even, consider $N = p_1 \cdot p_2 \cdots p_n + 2$, which is congruent to 3 (mod 4). Now N is odd and so is not divisible by 2. Since the product of primes of the form $4n + 1$ is still of that form, N cannot be the product of primes just of the form $4n + 1$. Therefore N must be divisible by a prime of the form $4n + 3$. This prime cannot be any of $p_1, p_2, \ldots, p_k$, because they leave remainder 2 when divided into N. Hence we obtain a new prime of the form $4n + 3$.

If k is odd, consider $N = p_1 \cdot p_2 \cdots p_k + 4$ which is congruent to 3 (mod 4). By a similar argument to that above, it follows that N must contain a new prime factor of the form $4n + 3$.

Therefore we have shown that $p_1, p_2, \ldots, p_k$ cannot be the complete set of primes of the form $4n + 3$, and so there must be an infinite number of such primes.

Problem 3-67:

Define a relation on the set of real numbers by

$$aRb \text{ if and only if } a - b = 2k\pi \text{ for some} k \in \mathbb{Z}.$$

(a) Prove that this is an equivalence relation.

(b) Which of the following are related?

$$5\pi \text{ and } -10\pi, -\pi \text{ and } \pi, 3 \text{ and } 9, \frac{2}{3}\pi \text{ and } -\frac{1}{3}\pi, \frac{11}{6}\pi \text{ and } \frac{23}{6}\pi?$$

(c) Two real numbers are equivalent if and only if they represent the same angle in radians. The equivalence classes therefore consist of the different angles. Denote the equivalence class containing a by $[a]$.
Show that addition of angles is well defined by

$$[a] + [b] = [a + b].$$

(d) Show, by a counterexample, that multiplication of angles if *not* well defined by

$$[a] \cdot [b] = [ab].$$

Solution: (a)

(i) Since $a - a = 2 \cdot 0\pi$ it follows that aRa.

(ii) If aRb then $a - b = 2k\pi$ and $b - a = 2(-k)\pi$, so bRa.

(iii) If aRb and bRc then $a - b = 2k\pi, b - c = 2\ell\pi$ for $k, \ell \in \pi$ Hence $a - c = (a - b) + (b - c) = 2(k + \ell)\pi$ and aRc.

Therefore R is an equivalence relation on the set of real numbers.

(b) $5\pi - (-10\pi) = 15\pi$ so 5π and -10π are not related.
$-\pi - \pi = -2\pi$ so $-\pi$ and π are related.

$3 - 9 = -6$, which is not an integral multiple of 2π, since π is not a rational number. Hence 3 and 9 are not related.

$\frac{2\pi}{3} - (\frac{-\pi}{3}) = \pi$ so $\frac{2\pi}{3}$ and $\frac{-\pi}{3}$ are not related. $\frac{11\pi}{6} - \frac{23\pi}{6} = \frac{-12\pi}{6} = -2\pi$, so $\frac{11\pi}{6}$ and $\frac{23\pi}{6}$ are related.

Hence $\pi R\pi$, and $\frac{11\pi}{6} R \frac{23\pi}{6}$.

(c) Let $[a] = [a']$ and $[b] = [b']$. Then aRa' and bRb' so that $a - a' = 2k\pi$ and $b - b^1 = 2\ell\pi$, where $k, \ell \in \mathbb{Z}$. Then $a+b = a'+2k\pi+b'+2\ell\pi = a'+b'+2(k+\ell)\pi$. Hence $(a+b)R(a'+b')$, so $[a+b] = [a'+b']$ whenever $[a] = [a']$ and $[b] = [b']$.

This means that addition of angles is well defined by $[a] + [b] = [a + b]$

(d) Now $[2\pi] = [0]$, but $[2\pi] \cdot [\pi] \neq [0] \cdot [\pi]$, since $2\pi \cdot \pi - 0 \cdot \pi = 2\pi^2$, which is not an integer multiple of 2π as π is not a rational number.

Therefore multiplication of angles is not well defined.

Problem 3-68:

(a) Find a relation R, on a set S, that is symmetric and transitive, but not reflexive.

(b) If there is an example to part (a), the following "proof," that every symmetric and transitive relation is reflexive, must be fallacious. Find the error. "Let R be a symmetric and transitive relation on the set S. For any $a, b \in S$, aRb implies that bRa, because R is symmetric. But aRb and bRa imply that aRa, because R is transitive. Since aRa, R must also be reflexive."

Solution: (a) Let $S = \{1, 2\}$ with the relation R defined by just $2R2$.

This relation is clearly symmetric. It is transitive, since the only case to check is

$$2R2 \text{ and } 2R2 \implies 2R2$$

which is true.

This relation is not reflexive, since 1 is not related to 1.

[An even more primitive example is $S = \{1\}$, with no elements related to each other.]

(b) For a relation to be reflexive, aRa must hold for each element a in the set. When a is not related to any other element in the set, we cannot use symmetry and transitivity to prove that a is related to itself.

Problem 3-69:

If $m = pq$ is a composite number, where $1 < p \leq q < m$, show that $\mathbb{Z}_m$ is not a field by showing that division by nonzero elements is not always possible in $\mathbb{Z}_m$.

Solution:

The question of division by a nonzero element is equivalent to the existence of an inverse for the element. Since $m = pq$ where $1 < p \leq q < m$, then in $\mathbb{Z}_m$ we have

$$[p] \neq 0, \quad [q] \neq 0 \quad \text{but} \quad [p][q] = [pq] = [m] = [0].$$

We shall show that the nonzero element $[p]$ has no inverse in $\mathbb{Z}_m$. If $[p]$ did have an inverse, then multiply both sides of the above equation by the inverse $[p]^{-1}$ and use the relation $[p]^{-1}[p] = [1]$ to obtain

$$\begin{aligned} [p]^{-1}[p][q] &= [p]^{-1}[0] \\ [1][q] &= [0] \\ [q] &= [0] \end{aligned}$$

which is a contradiction. Thus, our assumption that $[p]^{-1}$ existed was wrong. Hence division by $[p]$ in $\mathbb{Z}_m$ is not possible.

Problem 3-70:

Solve the following system of simultaneous equations in $\mathbb{Z}_{12}$.

$$\begin{array}{rcrcl} [8][x] & + & [3][y] & = & [9] \\ [6][x] & + & [5][y] & = & [2] \end{array}$$

Solution:

Note that it is possible to solve for $[y]$ in terms of $[x]$ in the second equation, since 5 is relatively prime to 12 and we can compute the inverse of $[5]$ in $\mathbb{Z}_{12}$. We have $5^2 = 25 \equiv 1 \pmod{12}$ so $[5][5] = [1]$, and the inverse of $[5]$ is itself in $\mathbb{Z}_{12}$. Multiply the second equation by $[5]$ to obtain

$$\begin{aligned} [5][6][x] + [5][5][y] &= [5][2] \\ [6][x] + [y] &= [10] \\ [y] &= [10] - [6][x]. \end{aligned}$$

Substitute this into the first equation,

$$\begin{aligned} [8][x] + [3]([10] - [6][x]) &= [9] \\ [8][x] + [6] + [6][x] &= [9] \\ [2][x] &= [3]. \end{aligned}$$

This final equation is a simple congruence to solve modulo 12. Since $\gcd(2, 12) = 2$, which does not divide 3, there are no solutions for x by the Linear Congruence Theorem 3.54. Therefore the simultaneous equations have no solutions in $\mathbb{Z}_{12}$.

Problem 3-71:

Solve the following system of simultaneous equations in $\mathbb{Z}_{11}$.

$$\begin{array}{rcrcl} [3][x] & + & [4][y] & = & [5] \\ [7][x] & + & [5][y] & = & [4] \end{array}$$

Solution:

Since the modulus is prime, all nonzero elements in $\mathbb{Z}_{11}$ have inverses and we can solve the system just as we would in real numbers.

By adding multiples of the equations we will cancel $[x]$ and solve for $[y]$. If we multiply the second equation by $[-2]$ we get

$$[-3][x] \ + \ [-10][y] \ = \ [-8]$$

If we add this to the first equation we get

$$\begin{array}{rcrcr} [3][x] & + & [4][y] & = & [5] \\ [-3][x] & + & [-10][y] & = & [-8] \\ \hline & & [5][y] & = & [8] \end{array}$$

Since 5 is relatively prime to 11, we may compute the inverse of $[5]$ in $\mathbb{Z}_{11}$. We have $5 \cdot 9 = 45 \equiv 1 \pmod{11}$, so $[5][9] = [1]$ and the inverse of $[5]$ is $[9]$. Therefore, if we multiply the equation by $[9]$ we get

$$[y] = [72] = [6]$$

To find $[x]$, we substitute $[y] = [6]$ into the first equation.

$$\begin{aligned} [3][x] + [4][6] &= [5] \\ [3][x] &= [5 - 24] \\ [3][x] &= [3] \end{aligned}$$

Clearly $[x] = [1]$ is a solution. Because 3 and 11 are coprime this is the only solution. Thus, the solution to the system of simultaneous equations in $\mathbb{Z}_{11}$ is

$$\begin{aligned} [x] &= [1] \\ [y] &= [6]. \end{aligned}$$

Check:

$$\begin{aligned} 3 \cdot 1 + 4 \cdot 6 &\equiv 27 \equiv 5 \pmod{11} \\ 7 \cdot 1 + 5 \cdot 6 &\equiv 37 \equiv 4 \pmod{11} \end{aligned}$$

Problem 3-72:

One common error in copying numbers is the transposition of adjacent digits. For example, 9578 might be copied as 9758. Will the method of casting out nines discover such an error? Discuss other methods of checking for errors.

Solution: Let

$$x = a_r 10^r + a_{r-1} 10^{r-1} + \ldots + a_{i+1} 10^{i+1} + a_i 10^i + \ldots + a_1 10 + a_0$$

be the number that is copied. Suppose that the transposition of adjacent digits occurs in the ith and $(i+1)$st digit. That is,

$$x' = a_r 10^r + a_{r-1} 10^{r-1} + \ldots + a_i 10^{i+1} + a_{i+1} 10^i + \ldots + a_1 10 + a_0$$

is the copied number. The method of casting out nines checks the numbers modulo 9. As we know by the test for divisibility by 9,

$$\begin{aligned} x &\equiv a_r 10^r + \ldots + a_{i+1}10^{i+1} + a_i 10^i + \ldots + a_0 \pmod 9 \\ &\equiv a_r + a_{r-1} + \ldots + a_{i+1} + a_i + \ldots + a_1 + a_0 \pmod 9 \end{aligned}$$

But x' has the same digits as x in different order so $x \equiv x' \pmod 9$. Hence the method of casting out nines will not detect the error.

By the same argument as above we can rule out the test of divisibility by 3. Now, the tests for divisibility by $2, 4, 5$ and 10 depend in the last digit or the last two digits of the number. Only if the transposition of adjacent digits happened in these digits could there be a possibility of detecting the error. But even then, the test would only work for certain numbers. For example if 542 gets copied as 524, both numbers are even.

Now the test for divisibility by 11 takes the alternating sum of digits. Using x and x' as defined above we have

$$x \equiv (-1)^r a_r + \ldots + (-1)^{i+1}a_{i+1} + (-1)^i a_i + \ldots - a_1 + a_0 \pmod{11}.$$

and if $a_i \neq a_{i+1}$,

$$x \equiv (-1)^r a_r + \ldots + (-1)^{i+1}a_i + (-1)^i a_{i+1} + \ldots - a_1 + a_0 \pmod{11}.$$

Subtracting these two congruences we get

$$x - x' \equiv 2(-1)^i(a_i - a_{i+1}) \pmod{11}.$$

Because $a_i - a_{i+1} \neq 0$ and $0 \leq a_i, a_{i+1} \leq 10 < 11$ then

$$2(-1)^i(a_i - a_{i+1}) \not\equiv 0 \pmod{11}.$$

So the test for divisibility by 11 will detect the error.

A modification of this method is used in the ISBN introduced in the next problem.

Problem 3-73:

Is 0-467-51402-X a valid ISBN?

Solution: Yes.

$$2 \cdot 4 + 3 \cdot 6 + 4 \cdot 7 + 5 \cdot 5 + 6 \cdot 1 + 7 \cdot 4 + 9 \cdot 2 \equiv 10$$

and 10 is represented by X.

Problem 3-74:

Is 1-56-004151-5 a valid ISBN?

Solution:

$$\begin{aligned} 1(1)+2(5)+3(6)+4(0)+5(0)+6(4)+7(1)+8(5)+9(1) & \\ &= 1+10+18+0+0+24+7+40+9 \\ &\equiv 7+2+7+7+9 \pmod{11} \\ &\equiv 32 \pmod{11} \\ &\equiv 10 \pmod{11} \end{aligned}$$

Hence, it is not a valid ISBN (The check digit should be 10 or X, not 5).

Problem 3-75:

What is the check digit for 14-200-0076- ?

Solution: Let a_{10} be the check digit for $14-200-0076-$? then

$$\begin{aligned} a_{10} &\equiv 1\cdot 1+2\cdot 4+3\cdot 2+7\cdot 8+6\cdot 9 \pmod{11} \\ &\equiv 125 \equiv 4 \pmod{11} \end{aligned}$$

Hence the check digit is $a_{10}=4$.

Problem 3-76:

What is the check digit for 0-4101-1286- ?

Solution: Let a_{10} be the check digit for 0-4101-1286- ? then

$$\begin{aligned} a_{10} &\equiv 2\cdot 4+3\cdot 1+5\cdot 1+6\cdot 1+7\cdot 2+8\cdot 8+9\cdot 6 \pmod{11} \\ &\equiv 3-2-1 \equiv 0 \pmod{11} \end{aligned}$$

Hence the check digit is $a_{10}=0$.

Problem 3-77:

If $\phi(m)$ is the Euler ϕ-function, show that $\phi(m)=\phi(2m)$ if and only if m is odd.

Solution:

If m is odd then $\gcd(m,2)=1$ and by the Euler-Phi Function Formula,

$$\phi(2m) \;=\; \phi(2)\phi(m) \;=\; 1\cdot\phi(m).$$

If m is even, write $m=2^i k$ where $\gcd(k,2)=1$ and $i>0$. Suppose $\phi(m)=\phi(2m)$ and use the Euler-Phi Function Formulas.

$$\begin{aligned} \phi(m) &= \phi(2m) \\ \phi(2^i k) &= \phi(2^{i+1}k) \\ \phi(2^i)\phi(k) &= \phi(2^{i+1})\phi(k) \\ 2^{i-1}\phi(k) &= 2^i\phi(k) \end{aligned}$$

Dividing both sides by the nonzero number $2^{i-1}\phi(k)$ gives $1 = 2$, which is a contradiction.

Therefore $\phi(m)$ can never be $\phi(2m)$, when m is even.

Problem 3-78:

Prove that $\phi(m) = m - 1$ if and only if m is prime.

Solution:

If m is a prime then $\phi(m) = m - 1$, by the Euler Phi Function Formula.

If $\phi(m) = m - 1$ then all the numbers from 1 to $m - 1$ are relatively prime with m. That is, there is no number from 2 to $m - 1$ that divides m. Note that $\phi(1) = 1$, so $m > 1$. Hence m must be prime.

Problem 3-79:

(Wilson's Theorem:) If p is prime, prove that

$$(p-1)! \equiv -1 \pmod{p}.$$

Solution:

We shall work inside $\mathbb{Z}_p$. If $p = 2$, then $1! \equiv -1 \pmod 2$ and the result is true.

Otherwise $p \geq 3$ is prime and the nonzero elements of $\mathbb{Z}_p$, $[1], [2], \ldots, [p-1]$, all have inverses. Now $[1]^{-1} = [1]$ and $[p-1]^{-1} = [-1]^{-1} = [-1] = [p-1]$. These are the only two elements of $\mathbb{Z}_p$ that are their own inverses, since if $x^2 = 1$ in $\mathbb{Z}_p$, then $(x-1)(x+1) = 0$ and $x = 1$ or $x = -1$, by Problem 3-56. Thus the other $p - 3$ nonzero elements $\{[2], [3], \ldots, [p-2]\}$ are paired off into $(p-3)/2$ pairs consisting of an element with its inverse. When we multiply these together, we will get [1]. Hence

$$\begin{array}{rcccc} [2] \cdot [3] \cdot [4] \cdots [p-3] \cdot [p-2] & = & [1]^{\frac{p-3}{2}} & = & [1] \\ [1] \cdot [2] \cdot [3] \cdot [4] \cdots [p-3] \cdot [p-2] \cdot [p-1] & = & [p-1] & = & [-1]. \end{array}$$

That is, $(p-1)! \equiv -1 \pmod p$.

Problem 3-80:

If p and q are integers, not divisible by 3 or 5, prove that $p^4 \equiv q^4 \pmod{15}$.

Solution:

Since 3 is a prime, and p is not divisible by 3 then by Fermat's Little Theorem, $p^2 \equiv 1 \pmod p$ and so $p^4 \equiv p^2 \cdot p^2 \equiv 1 \pmod 3$. Since 5 is prime and p is not divisible by 5 then by Fermat's Little Theorem, $p^4 \equiv 1 \pmod 5$ mod p.

We have the simultaneous congruences,

$$\begin{array}{rcl} p^4 & \equiv & 1 \pmod 3 \\ p^4 & \equiv & 1 \pmod 5. \end{array}$$

By Proposition 3.64, $p^4 \equiv 1 \pmod{15}$. Similarly, $q^4 \equiv 1 \pmod{15}$. Thus

$$p^4 \equiv q^4 \pmod{15}.$$

Problem 3-81:

Solve the simultaneous congruences

$$\begin{aligned} 9x &\equiv 21 \pmod{6} \\ 4x &\equiv 9 \pmod{13}. \end{aligned}$$

Solution: We can rewrite the simultaneous congruences as

$$\begin{aligned} 3x &\equiv 3 \pmod{6} \\ 4x &\equiv -4 \pmod{13}. \end{aligned}$$

Clearly $x \equiv 1 \pmod{6}$ is one solution to the first congruence. Since $\gcd(3, 6) = 3$, the complete solution by Theorem 3.54 is

$$x \equiv 1 \pmod{2}.$$

That is, x is odd.

Clearly $x \equiv -1 \pmod{13}$ is one solution to the second congruence. Since $\gcd(4, 13) = 1$ this is the complete solution.

To get the solution for the simultaneous congruences we must solve the system of congruences

$$\begin{aligned} x &\equiv 1 \equiv -1 \pmod{2} \\ x &\equiv -1 \pmod{13}. \end{aligned}$$

Since $\gcd(2, 13) = 1$, by Proposition 3.64 the complete solution is

$$x \equiv -1 \pmod{26}.$$

Modulo $6 \cdot 13 = 78$, this is

$$\begin{aligned} x &\equiv 25,\ 25 + 26,\ 25 + 52 \pmod{78} \\ &\equiv 25,\ 51,\ 77 \pmod{78}. \end{aligned}$$

Check:

$$\begin{aligned} 9(25) - 21 = 240 &= 6(34), & 4(25) - 9 &= 91 = 13(7) \\ 9(51) - 21 = 438 &= 6(73), & 4(51) - 9 &= 195 = 13(15) \\ 9(77) - 21 = 672 &= 6(112), & 4(77) - 9 &= 299 = 13(23) \end{aligned}$$

Problem 3-82:

Solve the simultaneous congruences

$$\begin{aligned} 3x &\equiv 7 \pmod{11} \\ 8x &\equiv 3 \pmod{9}. \end{aligned}$$

Solution:
Since $\gcd(3, 11) = 1$ and $\gcd(8, 9) = 1$, the first congruence has one solution modulo 11, and the second congruence one solution modulo 9. By the Chinese Remainder Theorem the simultaneous congruences will have one solution modulo 99, since $\gcd(11, 9) = 1$.

Solve one of these congruences. The second congruence can be written

$$\begin{aligned} -x &\equiv 3 \pmod{9} \\ x &\equiv -3 \equiv 6 \pmod{9}. \end{aligned}$$

Hence $x = 6 + 9z$ for $z \in \mathbb{Z}$. Substitute this into the first congruence

$$\begin{aligned} 3(6 + 9z) &\equiv 7 \pmod{11} \\ 27z &\equiv -11 \equiv 0 \pmod{11}. \end{aligned}$$

Since $\gcd(27, 11) = 1$, the solution is $z \equiv 0 \pmod{11}$, or $z = 11t$ for $t \in \mathbb{Z}$. Hence the solution the the simultaneous congruences is $x = 6 + 99t$, or

$$x \equiv 6 \pmod{99}.$$

Check: $3(6) - 7 = 11 = 11(1)$ and $8(6) - 3 = 45 = 9(5)$.

Problem 3-83:

Two watches, one of which gains 2 minutes per day, and the other which loses 3 minutes per day, read the correct time. When will both watches next give the same time? When will they next both give the correct time?

Solution:

We first need to know that there are 1440 minutes in a day. The answers might depend on whether the watches can tell the difference between A.M. and P.M. If they can, then we have to work modulo 1440; if not, then we work modulo 720. [Most digital watches can tell the difference, though they do not normally lose anything like 2 minutes per day.]

12 Hour Watch: If the watches cannot tell the difference between A.M. and P.M. then, after d days, the time on our first watch is given by

$$t + 2d \pmod{720}$$

and on our second watch is given by

$$t - 3d \pmod{720}.$$

In order for both watches to read the same time, we must have

$$t + 2d \equiv t - 3d \pmod{720}.$$

Clearly this occurs if and only if $5d \equiv 0 \pmod{720}$; that is, $720|5d$ or $144|d$. Therefore the two watches will next read the same time after 144 days.

If we want to know when they will both read the correct time, then we must have

$$t + 2d \equiv t \pmod{720} \qquad \text{and} \qquad t - 3d \equiv t \pmod{720}$$

or equivalently

$$2d \equiv 0 \pmod{720} \qquad \text{and} \qquad -3d \equiv 0 \pmod{720}.$$

Adding these congruences gives us

$$d \equiv 0 \pmod{720}.$$

This clearly satisfies both congruences and so must be the complete solution. Hence both watches will read the correct time again after 720 days.

24 Hour Watch: If the watches can tell the difference between A.M. and P.M. then, after d days, the time on our first watch is given by

$$t + 2d \pmod{1440}$$

and on our second watch is given by

$$t - 3d \pmod{1440}.$$

In order for both watches to read the same time, we must have

$$t + 2d \equiv t - 3d \pmod{1440}.$$

Clearly this occurs if and only if $5d \equiv 0 \pmod{1440}$; that is, $1440|5d$ or $288|d$. Therefore the two watches will next read the same time after 288 days.

If we want to know when they will both read the correct time, then we must have

$$t + 2d \equiv t \pmod{1440} \qquad \text{and} \qquad t - 3d \equiv t \pmod{1440}$$

or equivalently

$$2d \equiv 0 \pmod{1440} \qquad \text{and} \qquad -3d \equiv 0 \pmod{1440}.$$

Adding these congruences gives us

$$d \equiv 0 \pmod{1440}.$$

This clearly satisfies both congruences and so must be the complete solution. Hence both watches will read the correct time again after 1440 days.

Problem 3-84:

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

Solution: Since $99 = 9 \cdot 11$ and $\gcd(9, 11) = 1$, the congruence is equivalent to the simultaneous congruences

$$\begin{aligned} x^3 &\equiv 17 \equiv 6 \pmod{11} \\ x^3 &\equiv 17 \equiv 8 \pmod{9}. \end{aligned}$$

Modulo 11											
$x \equiv$	0	1	2	3	4	5	6	7	**8**	9	10
$x^3 \equiv$	0	1	8	5	9	4	7	2	**6**	3	10

Modulo 9									
$x \equiv$	0	1	**2**	3	4	**5**	6	7	**8**
$x^3 \equiv$	0	1	**8**	0	1	**8**	0	1	**8**

From the tables, the solutions are $x \equiv 8 \pmod{11}$ and $x \equiv 2, 5, 8 \pmod{9}$.

By the Chinese Remainder Theorem, there will be three solutions modulo 99. The first congruence is equivalent to $x = 8 + 11k$ for some $k \in \mathbb{Z}$. Substitute this into the modulo 9 congruence to obtain $8 + 11k \equiv 2, 5, 8 \pmod{9}$. So $11k \equiv 2k \equiv 3, 6, 0 \pmod{9}$. Multiply by 5 (the inverse of [2] in $\mathbb{Z}_9$) to obtain $k \equiv 6, 3, 0 \pmod{9}$. That is, $k = 6 + 9z$, $3 + 9z$, $9z$, for some $z \in \mathbb{Z}$. Hence

$$\begin{aligned} x &= 8 + 11(6 + 9z), \quad 8 + 11(3 + 9z), \quad 8 + 11(9z) \\ &= 74 + 99z, \quad 41 + 99z, \quad 8 + 99z \\ x &\equiv 74, \quad 41, \quad 8 \pmod{99}. \end{aligned}$$

Check: $74^3 \equiv 41^3 \equiv 8^3 \equiv 17 \pmod{99}$

Problem 3-85:

Solve $x^2 \equiv 7 \pmod{99}$.

Solution: Since $99 = 9 \cdot 11$ and $\gcd(9, 11) = 1$, the congruence is equivalent to the simultaneous congruences

$$\begin{aligned} x^2 &\equiv 7 \pmod{11} \\ x^2 &\equiv 7 \pmod{9}. \end{aligned}$$

Modulo 11											
$x \equiv$	0	1	2	3	4	5	6	7	8	9	10
$x^2 \equiv$	0	1	4	9	5	3	3	5	9	4	1

Modulo 9									
$x \equiv$	0	1	2	3	**4**	**5**	6	7	8
$x^2 \equiv$	0	1	4	0	**7**	**7**	0	4	1

We see from the tables that the congruence $x^2 \equiv 7 \pmod{11}$ has no solution. Therefore the original congruence $x^2 \equiv 7 \pmod{99}$ has no solution.

Problem 3-86:

If $\gcd(m, n) = d$, when do the simultaneous congruences

$$\begin{aligned} x &\equiv a \pmod{m} \\ x &\equiv b \pmod{n} \end{aligned}$$

have a solution?

Solution: An integer x satisfies the first congruence if and only if

$$x = a + my \quad \text{for some} \quad y \in \mathbb{Z}.$$

Substituting into the second congruence we have

$$\begin{aligned} a + my &\equiv b \pmod{n} \\ mx &\equiv b - a \pmod{n}. \end{aligned}$$

By Theorem 3.54, this linear congruence has an integer solution for x if and only if $\gcd(m, n) \mid b - a$.

Therefore, the two simultaneous congruences have a solution if and only if $d \mid b - a$.

Problem 3-87:

Let $M = m_1 m_2 \dots m_n$, where $\gcd(m_i, m_j) = 1$ whenever $i \neq j$, and let $M_i = M/m_i$. Let $y \equiv b_i \pmod{m_i}$ be a solution to $M_i y \equiv 1 \pmod{m_i}$. Prove that the simultaneous congruences

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\vdots \\ x &\equiv a_n \pmod{m_n} \end{aligned}$$

have the solution

$$x \equiv a_1 b_1 M_1 + a_2 b_2 M_2 + a_3 b_3 M_3 + \cdots + a_n b_n M_n \pmod{M}.$$

Solution:
Because $\gcd(m_i, m_j) = 1$ whenever $i \neq j$, the Chinese Remainder Theorem shows the system of simultaneous congruences has one solution modulo M.

Our goal is to show that

$$x_0 = a_1 b_1 M_1 + a_2 b_2 M_2 + a_3 b_3 M_3 + \cdots + a_n b_n M_n$$

is one particular integer solution to each congruence.

Consider the first congruence modulo m_1. If $j \neq 1$, then

$$M_j = \frac{M}{m_j} = \frac{m_1 \cdots m_n}{m_j} = m_1 m_2 \cdots m_{j-1} m_{j+1} \cdots m_n$$

so $m_1 | M_j$ and $M_j \equiv 0 \pmod{m_1}$. Using the fact that $y = b_1$ is a solution to $M_1 y \equiv 1 \pmod{m_1}$, we have $b_1 M_1 \equiv 1 \pmod{m_1}$ and so

$$\begin{aligned} x_0 &\equiv a_1 b_1 M_1 + a_2 b_2 M_2 + \cdots + a_n b_n M_n \pmod{m_1} \\ &\equiv a_1 b_1 M_1 + 0 + \cdots + 0 \pmod{m_1} \\ &\equiv a_1 \pmod{m_1}. \end{aligned}$$

Therefore x_0 satisfies the first congruence.

Similarly, x_0 satisfies each of the other congruences. By the Generalized Chinese Remainder Theorem, the complete solution to the system is

$$x \equiv a_1 b_1 M_1 + a_2 b_2 M_2 + a_3 b_3 M_3 + \cdots + a_n b_n M_n \pmod{M}.$$

Problem 3-88:

Solve the simultaneous equations

$$\begin{array}{rcrcr} 100x & - & 9y & = & 4264 \\ 11x & + & 109y & = & 909 \end{array}$$

(a) modulo 9

(b) modulo 11

(c) in integers, using (a) and (b), given the fact that x and y have unique solutions and both are positive integers less than 100.

Solution: **(a)** Modulo 9, we can rewrite the equations as

$$\begin{aligned} x &\equiv 7 \pmod{9} \\ 2x + y &\equiv 0 \pmod{9}. \end{aligned}$$

Substituting x in the second equation gives

$$\begin{aligned} 14 + y &\equiv 0 \pmod{9} \\ y &\equiv 4 \pmod{9}. \end{aligned}$$

Hence the solution to the simultaneous equations modulo 9 is

$$x \equiv 7 \pmod{9} \quad \text{and} \quad y \equiv 4 \pmod{9}.$$

Check: $7 - 7 = 0 \cdot 9$ and $14 + 4 = 18 = 2 \cdot 9$.

(b) Modulo 11, we can rewrite the equations as

$$\begin{aligned} x + 2y &\equiv 7 \pmod{11} \\ -y &\equiv 7 \pmod{11}. \end{aligned}$$

Substituting y in the first equation gives

$$\begin{aligned} x - 14 &\equiv 7 \pmod{11} \\ x &\equiv 10 \pmod{11}. \end{aligned}$$

Hence the solution to the simultaneous equations modulo 11 is

$$x \equiv 10 \pmod{11} \quad \text{and} \quad y \equiv 4 \pmod{11}.$$

Check: $10 + 8 - 7 = 11 \cdot 1$ and $4 + 7 = 11 \cdot 1$.

(c) From parts (a) and (b) we know that x satisfies the congruences

$$\begin{aligned} x &\equiv 7 \pmod 9 \\ x &\equiv 10 \pmod{11}. \end{aligned}$$

An integer x satisfies the second congruence if and only if

$$x = 10 + 11z \quad \text{for some } z \in \mathbb{Z}.$$

Substituting into the first congruence we have

$$\begin{aligned} 10 + 11z &\equiv 7 \pmod 9 \\ 2z &\equiv -3 \equiv 6 \pmod 9. \end{aligned}$$

By inspection $z \equiv 3 \pmod 9$ is a solution. This is equivalent to $z = 3 + 9t$ for all $t \in \mathbb{Z}$. The solution for both congruences is therefore

$$x = 10 + 11(3 + 9t) = 43 + 99t.$$

On the other hand, for y satisfies the system of congruences

$$\begin{aligned} y &\equiv 4 \pmod 9 \\ y &\equiv 4 \pmod{11}. \end{aligned}$$

Because $\gcd(9, 11) = 1$, Proposition 3.64 tells us that this is equivalent to

$$y \equiv 4 \pmod{99}.$$

Given that x and y are positive integers less than 100, the only possible solution is $x = 43$ and $y = 4$.

Check:

$$\begin{aligned} 100(43) - 9(4) &= 4300 - 36 = 4264 \\ 11(43) + 109(4) &= 473 + 436 = 909 \end{aligned}$$

Problem 3-89:

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 e be the number of eggs in the basket. Then

$$e \equiv 1 \equiv -1 \pmod 2 \tag{1}$$
$$e \equiv 2 \equiv -1 \pmod 3 \tag{2}$$
$$e \equiv 3 \equiv -1 \pmod 4 \tag{3}$$
$$e \equiv 4 \equiv -1 \pmod 5 \tag{4}$$
$$e \equiv 5 \equiv -1 \pmod 6 \tag{5}$$
$$e \equiv 0 \pmod 7. \tag{6}$$

Because $\gcd(2,3) = 1$ and $\gcd(4,5) = 1$, by Proposition 3.64, the congruences (1) and (2), and (3) and (4) are equivalent to

$$\begin{aligned} e &\equiv -1 \pmod 6 \quad (7) \\ e &\equiv -1 \pmod{20}. \quad (8) \end{aligned}$$

Congruence (7) is the same as the congruence (5). Therefore e satisfies the two congruences

$$\begin{aligned} e &\equiv -1 \pmod{20} \quad (8) \\ e &\equiv 0 \pmod 7. \quad (6) \end{aligned}$$

Congruence (8) is equivalent to $e = 20y - 1$ for some $y \in \mathbb{Z}$. Substitute this in congruence (6) to get

$$\begin{aligned} 20y - 1 &\equiv 0 \pmod 7 \\ 20y &\equiv 1 \pmod 7 \\ -y &\equiv 1 \pmod 7 \\ y &\equiv -1 \equiv 6 \pmod 7. \end{aligned}$$

Hence $y = 6 + 7z$ for $z \in \mathbb{Z}$ and

$$\begin{aligned} e &= 20(6 + 7z) - 1 \\ &= 119 + 140z. \end{aligned}$$

The solution to the system of congruences is $e \equiv 119 \pmod{140}$ and the minimum number of eggs that were in the basket is 119.

Check:

$$\begin{aligned} 119 &= 2 \cdot 59 + 1 \\ &= 3 \cdot 39 + 2 \\ &= 4 \cdot 29 + 3 \\ &= 5 \cdot 23 + 4 \\ &= 6 \cdot 19 + 5 \\ &= 7 \cdot 17 \end{aligned}$$

Problem 3-90:

Use Problem 3-87 to solve each of these three simultaneous congruences.

(a) $x \equiv 2 \pmod 7$, $x \equiv 5 \pmod{11}$, $x \equiv 11 \pmod{17}$

(b) $x \equiv 0 \pmod 7$, $x \equiv 8 \pmod{11}$, $x \equiv 10 \pmod{17}$

(c) $x \equiv 5 \pmod 7$, $x \equiv 6 \pmod{11}$, $x \equiv 14 \pmod{17}$

Solution: Problem 3-87 is most suitable for solving this type of problem where there are several simultaneous congruences to solve using the same modulii but different right sides.

If we let $m_1 = 7, m_2 = 11$ and $m_3 = 17$, then our moduli satisfy the criterion given in Problem 3-87 that gcd(m_i, m_j)=1 for $i \neq j$. We must construct b_i such that $M_i b_i \equiv 1 \pmod{m_i}$ where $M_i = m_1 m_2 m_3 / m_i$. We use the Euclidean Algorithm to construct such b_i.

Apply the Extended Euclidean Algorithm to 7 and 187.

$187y + 7x = r$			q_i
1	0	187	
0	1	7	
1	−26	5	26
−1	27	2	1
3	−80	1	2
−7	187	0	2

Therefore $3 \cdot 187 - 80 \cdot 7 = 1$. Hence $1 \equiv 3 \cdot 187 \pmod{7}$, so

$$b_1 \equiv 3 \pmod{7}.$$

Apply the Extended Euclidean Algorithm to 11 and 119.

$119y + 11x = r$			q_i
1	0	119	
0	1	11	
1	−10	9	10
−1	11	2	1
5	−54	1	4
−11	119	0	2

Therefore $5 \cdot 119 - 54 \cdot 11 = 1$. Hence $1 \equiv 5 \cdot 119 \pmod{11}$, so

$$b_2 \equiv 5 \pmod{11}.$$

Apply the Euclidean algorithm to 17 and 77.

$77y + 17x = r$			q_i
1	0	77	
0	1	17	
1	−4	9	4
−1	5	8	1
2	−9	1	1
−17	77	0	8

Therefore $2 \cdot 77 - 9 \cdot 17 = 1$. Hence $1 \equiv 2 \cdot 77 \pmod{17}$, so

$$b_3 \equiv 2 \pmod{17}.$$

We may now use Problem 3-83. to solve the three parts of the problem.

$$\begin{aligned}
\text{(a)} \quad x &\equiv 2\cdot 3\cdot 187 + 5\cdot 5\cdot 119 + 11\cdot 2\cdot 77 \pmod{1309} \\
&\equiv 1122 + 357 + 385 \\
&\equiv 555 \pmod{1309}
\end{aligned}$$

$$\begin{aligned}
\text{(b)} \quad x &\equiv 0\cdot 3\cdot 187 + 8\cdot 5\cdot 119 + 10\cdot 2\cdot 77 \pmod{1309} \\
&\equiv 0 + 833 + 231 \\
&\equiv 1064 \pmod{1309}
\end{aligned}$$

$$\begin{aligned}
\text{(c)} \quad x &\equiv 5\cdot 3\cdot 187 + 6\cdot 5\cdot 119 + 14\cdot 2\cdot 77 \pmod{1309} \\
&\equiv 187 + 952 + 847 \\
&\equiv 677 \pmod{1309}
\end{aligned}$$

Check:

x	mod 7	mod 11	mod 17
555	2	5	11
1064	0	8	10
677	5	6	14

Problem 3-91:

Use Problem 3-87 to find the solution to these simultaneous congruences.

$x \equiv a_1 \pmod 9, \quad x \equiv a_2 \pmod{11}$.

Solution:

Since $\gcd(9, 11) = 1$, Problem 3-87 can be used. Using the same variable names as in Problem 3-87, $m_1 = 9$, $m_2 = 11$, $M = 9\cdot 11 = 99$, $M_1 = M/m_1 = 11$ and $M_2 = M/m_2 = 9$. The congruence $M_1 y \equiv 1 \pmod{m_1}$ is $11y \equiv 1 \pmod 9$ and, by inspection, one solution is $b_1 = 5$. Similarly, the congruence $M_2 y \equiv 1 \pmod{m_2}$ is $9y \equiv 1 \pmod{11}$ and, by inspection, one solution is also $b_2 = 5$.

By Problem 3-87 the simultaneous congruences have the solution

$$\begin{aligned}
x &\equiv a_1 b_1 M_1 + a_2 b_2 M_2 \pmod{99} \\
&\equiv a_1(5\cdot 11) + a_2(5\cdot 9) \pmod{99} \\
&\equiv 55a_1 + 45a_2 \pmod{99}.
\end{aligned}$$

Check:

$$\begin{aligned}
55a_1 + 45a_2 &\equiv 55a_1 \equiv a_1 \pmod 9 \\
55a_1 + 45a_2 &\equiv 45a_2 \equiv a_2 \pmod{11}
\end{aligned}$$

Problem 3-92:

Use Problem 3-87 to find the solution to these simultaneous congruences.

$x \equiv a_1 \pmod 3, \quad x \equiv a_2 \pmod 8, \quad x \equiv a_3 \pmod{25}$.

Solution:

Since $\gcd(3,8)=1$, $\gcd(8,25)=1$, $\gcd(3,25)=1$, Problem 3-87 can be used. Using the same variable names as in Problem 3-87, $m_1=3$, $m_2=8$, $m_3=25$, $M=3\cdot 8\cdot 25=600$, $M_1=M/m_1=8\cdot 25=200$, $M_2=M/m_2=3\cdot 25=75$, and $M_3=M/m_3=3\cdot 8=24$.

The congruence $M_1y\equiv 1 \pmod{m_1}$ is $200y\equiv 1 \pmod 3$. This is $2y\equiv 1 \pmod 3$ and, by inspection, one solution is $b_1=2$. The congruence $M_2y\equiv 1 \pmod{m_2}$ is $75y\equiv 1 \pmod 8$. This is $3y\equiv 1 \pmod 8$ and, by inspection, one solution is $b_2=3$. The congruence $M_3y\equiv 1 \pmod{m_3}$ is $24y\equiv 1 \pmod{25}$, which clearly has a solution $b_3=-1$.

By Problem 3.87 the simultaneous congruences have the solution

$$\begin{aligned} x &\equiv a_1b_1M_1+a_2b_2M_2+a_3b_3M_3 \pmod{600} \\ &\equiv a_1(2\cdot 200)+a_2(3\cdot 75)+a_3(-1\cdot 24) \pmod{600} \\ &\equiv 400a_1+225a_2-24a_3 \pmod{600} \\ &\equiv 400a_1+225a_2+576a_3 \pmod{600}. \end{aligned}$$

Check:

$$\begin{array}{lllll} 400a_1+225a_2-24a_3 & \equiv & 400a_1 & \equiv & a_1 \pmod 3 \\ 400a_1+225a_2-24a_3 & \equiv & 225a_2 & \equiv & a_2 \pmod 8 \\ 400a_1+225a_2-24a_3 & \equiv & -24a_3 & \equiv & a_3 \pmod{25} \end{array}$$

Problem 3-93:

Find positive integers a, b, m_1, m_2 such that

$$\begin{aligned} a &\equiv b \pmod{m_1} \\ a &\equiv b \pmod{m_2} \\ a &\not\equiv b \pmod{m_1m_2}. \end{aligned}$$

Solution:
If $\gcd(m_1,m_2)=1$, Proposition 3.64 tells us that $a\equiv b \pmod{m_1m_2}$. If such positive integers a, b, m_1, m_2 exist then the $\gcd(m_1,m_2)\neq 1$.

For example, take $a=13$, $b=1$, $m_1=2$, $m_2=4$. Then

$$\begin{aligned} 13 &\equiv 1 \pmod 2 \\ 13 &\equiv 1 \pmod 4 \\ 13 &\equiv 5 \not\equiv 1 \pmod 8 \end{aligned}$$

and this is one of many examples.

Problem 3-94:

Find all the integer solutions to the Diophantine equation $5x^2+x+6=7y$.
Solution:
We are seeking integer solutions, so $7y\equiv 0 \pmod 7$. Hence

$$5x^2+x+6\equiv 0 \pmod 7.$$

Modulo 7							
$x \equiv$	0	1	**2**	3	4	5	6
$x^2 \equiv$	0	1	4	2	1	4	1
$5x^2 + x + 6 \equiv$	6	5	**0**	5	6	3	3

Therefore $x \equiv 2 \pmod 7$ is the only solution. That is, $x = 2 + 7z$ for any $z \in \mathbb{Z}$ and then

$$\begin{aligned} 7y &= 5(2+7z)^2 + (2+7z) + 6 \\ &= 5(4 + 28z + 49z^2) + 8 + 7z \\ &= 28 + 147z + 245z^2 \\ y &= 4 + 21z + 35z^2. \end{aligned}$$

Thus the complete solution is

$$\left.\begin{aligned} x &= 2 + 7z \\ y &= 4 + 21z + 35z^2 \end{aligned}\right\} \text{ for any } z \in \mathbb{Z}.$$

Check: Try $z = -1$, so $x = -5$ and $y = 4 - 21 + 35 = 18$. Then

$$5x^2 + x + 6 \;=\; 125 - 5 + 6 \;=\; 126 \;=\; 7 \cdot 18.$$

Problem 3-95:

(a) Prove that if p and q are coprime, and x is an integer such that

$$\begin{aligned} x &\equiv p \pmod q \\ x &\equiv q \pmod p \end{aligned}$$

then $x \equiv p + q \pmod{pq}$.

(b) Show by means of a counterexample that the condition that p and q are coprime is necessary.

Solution: (a)

Since $x \equiv p \pmod q$, $x = p + qy$, for some $y \in \mathbb{Z}$. Substitute this into the second congruence.

$$\begin{aligned} p + qy &\equiv q \pmod p \\ q(y-1) &\equiv 0 \pmod p \end{aligned}$$

Hence $p | q(y-1)$. Since $\gcd(p, q) = 1$, by Proposition 2.28, $p | y - 1$. Therefore $y - 1 = pz$ for some $z \in \mathbb{Z}$ and

$$\begin{aligned} x &= p + q(1 + pz) \\ &= p + q + pqz \\ x &\equiv p + q \pmod{pq}. \end{aligned}$$

(b) As an example in which $\gcd(p, q) \neq 1$, take $p = 4$ and $q = 6$. Then $x = 22$ is a solution to $x \equiv 4 \pmod 6$ and $x \equiv 6 \pmod 4$. But $22 \not\equiv 4 + 6 \equiv 10 \pmod{24}$. Hence the condition that p and q are coprime is necessary.

Problem 3-96:

Solve the congruence

$$x^3 - 29x^2 + 35x + 38 \equiv 0 \pmod{195}.$$

Solution:

Now, $195 = 3{\cdot}5{\cdot}13$ and $3, 5$, and 13 are coprime in pairs. By Proposition 3.64, the congruence modulo 195 is equivalent to the following system of simultaneous congruences.

$$\begin{aligned} x^3 - 29x^2 + 35x + 38 &\equiv 0 \pmod 3 \\ x^3 - 29x^2 + 35x + 38 &\equiv 0 \pmod 5 \\ x^3 - 29x^2 + 35x + 38 &\equiv 0 \pmod{13} \end{aligned}$$

Reducing by the modulii, these are the same as the following.

$$\begin{aligned} x^3 + x^2 + 2x + 2 &\equiv 0 \pmod 3 \\ x^3 + x^2 \qquad + 3 &\equiv 0 \pmod 5 \\ x^3 - 3x^2 - 4x - 1 &\equiv 0 \pmod{13} \end{aligned}$$

Modulo 3: It follows from Corollary 3.43 to Fermat's Little Theorem that $x^3 \equiv x \pmod 3$ for all $x \in \mathbb{Z}$. Therefore the modulo 3 congruence is equivalent to

$$\begin{aligned} x + x^2 + 2x + 2 &\equiv 0 \pmod 3 \\ x^2 &\equiv 1 \pmod 3. \end{aligned}$$

Modulo 3			
$x \equiv$	0	**1**	**2**
$x^2 \equiv$	0	**1**	**1**

We see from the above table that $x \equiv 1 \pmod 3$ and $x \equiv 2 \pmod 3$ are the solutions to the modulo 3 congruence.

Modulo 5: Use the brute force method to try all the possibilities for the modulo 5 congruence.

Modulo 5					
$x \equiv$	0	**1**	**2**	3	4
$x^2 \equiv$	0	1	4	4	1
$x^3 \equiv$	0	1	3	2	4
$x^3 + x^2 + 3 \equiv$	3	**0**	**0**	4	3

We see from the above table that $x \equiv 1 \pmod 5$ and $x \equiv 2 \pmod 5$ are the solutions to the modulo 5 congruence.

Modulo 5: Again, use the brute force method to try all the possibilities for the modulo 13 congruence $f(x) \equiv 0 \pmod{13}$ where $f(x) = x^3 - 3x^2 - 4x - 1$.

Modulo 13													
$x \equiv$	0	1	**2**	**3**	4	5	6	7	8	9	10	**11**	12
$x^2 \equiv$	0	1	4	9	3	12	10	10	12	3	9	4	1
$x^3 \equiv$	0	1	8	1	12	8	8	5	5	1	12	5	12
$f(x) \equiv$	12	6	**0**	**0**	12	3	5	11	1	7	9	**0**	12

We see from the table that $x \equiv 2,\ 3,\ 11 \pmod{13}$ are the solutions to the modulo 13 congruence.

Modulo 195: We now need to combine all the above solutions into solutions modulo 195.

$$\begin{aligned} x &\equiv 1,\ 2 \pmod 3 \\ x &\equiv 1,\ 2 \pmod 5 \\ x &\equiv 2,\ 3,\ 11 \pmod{13} \end{aligned}$$

Taking all possible combinations and using the Chinese Remainder Theorem we will get $2 \cdot 2 \cdot 3 = 12$ solutions modulo 195. This is a case in which Problem 3-87 is useful, since we have to solve 12 simultaneous congruences using the same modulii, but different right sides.

[Note that the first two congruences have the obvious solutions $x \equiv 1,\ 2 \pmod{15}$, but also two more solutions where $x \equiv 1 \pmod 3$, $x \equiv 2 \pmod 5$, and $x \equiv 2 \pmod 3$, $x \equiv 1 \pmod 5$.]

Using the same variable names as in Problem 3-87, $m_1 = 3$, $m_2 = 5$, $m_3 = 13$, $M = 3 \cdot 5 \cdot 13 = 195$, $M_1 = M/m_1 = 5 \cdot 13 = 65$, $M_2 = M/m_2 = 3 \cdot 13 = 39$, and $M_3 = M/m_3 = 3 \cdot 5 = 15$.

The congruence $M_1 y \equiv 1 \pmod{m_1}$ is $65y \equiv 1 \pmod 3$. This is $2y \equiv 1 \pmod 3$ and, by inspection, one solution is $b_1 = 2$. The congruence $M_2 y \equiv 1 \pmod{m_2}$ is $39y \equiv 1 \pmod 5$, which clearly has a solution $b_2 = -1$. The congruence $M_3 y \equiv 1 \pmod{m_3}$ is $15y \equiv 1 \pmod{13}$. This is $2y \equiv 1 \pmod{13}$ or $14y \equiv 7 \pmod{13}$, which clearly has a solution $b_3 = 7$.

By Problem 3-87, the solution to the simultaneous congruences

$$x \equiv a_1 \pmod 3, \quad x \equiv a_2 \pmod 5, \quad x \equiv a_3 \pmod{13}$$

is

$$\begin{aligned} x &\equiv a_1 b_1 M_1 + a_2 b_2 M_2 + a_3 b_3 M_3 \pmod{195} \\ &\equiv (2 \cdot 65)a_1 + (-1 \cdot 39)a_2 + (7 \cdot 15)a_3 \pmod{195} \\ &\equiv 130a_1 - 39a_2 + 105a_3 \pmod{195}. \end{aligned}$$

Mod 3	Mod 5	Mod 13	Modulo 195				
a_1	a_2	a_3	$130a_1 - 39a_2 + 105a_3$				
1	1	2	130 - 39 + 210	=	301	$\equiv$	106
1	1	3	130 - 39 + 315	=	406	$\equiv$	16
1	1	11	130 - 39 + 210	=	1246	$\equiv$	76
1	2	2	130 - 39 + 210	=	262	$\equiv$	67
1	2	3	130 - 39 + 315	=	367	$\equiv$	172
1	2	11	130 - 39 + 210	=	1207	$\equiv$	37
2	1	2	130 - 39 + 210	=	431	$\equiv$	41
2	1	3	130 - 39 + 315	=	536	$\equiv$	146
2	1	11	130 - 39 + 210	=	1376	$\equiv$	11
2	2	2	130 - 39 + 210	=	392	$\equiv$	2
2	2	3	130 - 39 + 315	=	497	$\equiv$	107
2	2	11	130 - 39 + 210	=	1337	$\equiv$	167

Hence the 12 solutions to the congruence $x^3 - 29x^2 + 35x + 38 \equiv 0 \pmod{195}$ are

$$x \equiv 2,\ 11,\ 16,\ 37,\ 41,\ 67,\ 76,\ 106,\ 107,\ 146,\ 167,\ 172 \pmod{195}.$$

Check: Try $x = 2$ and 16.

$$\begin{aligned} 2^3 - 29 \cdot 2^2 + 35 \cdot 2 + 38 &= 0 \\ 16^3 - 29 \cdot 16^2 + 35 \cdot 16 + 38 &= -1755 = -9 \cdot 195 \end{aligned}$$

Problem 3-97:

If p is prime and k is the smallest positive integer such that $a^k \equiv 1 \pmod{p}$ then prove that k divides $p - 1$.

Solution:

If p divides a then $a^m \equiv 0 \pmod{p}$ for every $m \in \mathbb{Z}$. Therefore no such k exists in this case.

Hence if there is a smallest positive integer k such that $a^k \equiv 1 \pmod{p}$ then p does not divide a and Fermat's Little Theorem implies $a^{p-1} \equiv 1 \pmod{p}$.

If $p = 2$ and $2 \nmid a$ then $a^1 \equiv 1 \pmod{p}$. It is clear that $k = 1$ and $1|2 - 1$.

If $p > 2$, divide $p - 1$ by k according to the Division Algorithm to obtain unique integers q and r such that

$$p - 1 = qk + r \quad \text{where} \quad 0 \le r < k.$$

Now, by Fermat's Little Theorem and the definition of k,

$$\begin{aligned} a^{p-1} &\equiv 1 \pmod{p} \\ a^{qk+r} &\equiv 1 \pmod{p} \\ (a^k)^q \cdot a^r &\equiv 1 \pmod{p} \\ 1^q \cdot a^r &\equiv 1 \pmod{p} \\ a^r &\equiv 1 \pmod{p} \end{aligned}$$

If $0 < r < k$ then r would be a smaller positive integer than k satisfying that $a^r \equiv 1 \pmod{p}$, which is a contradiction. Hence we can conclude that $r = 0$, which implies that k divides $p - 1$.

Problem 3-98:

Find the remainder when 17^{40} is divided by 27.

Solution:

We have to calculate the remainder modulo 27. Now we know that the Euler phi function $\phi(27) = \phi(3^3) = 27 \cdot \left(1 - \frac{1}{3}\right) = 18$. Because $\gcd(17, 27) = 1$, the Euler-Fermat Theorem tells us that $17^{18} \equiv 1 \pmod{27}$. Now, by the Division Algorithm, $40 = 18(2) + 4$. Therefore,

$$17^{40} \equiv 17^{18(2)+4} \equiv 1 \cdot 17^4 \pmod{27}.$$

By repeated squaring,

$$\begin{array}{rcl} 17^2 & \equiv & 289 \equiv 19 \pmod{27}. \\ 17^4 & \equiv & (17^2)^2 \equiv 19^2 \equiv 361 \equiv 10 \pmod{27} \end{array}$$

Thus, the remainder of 17^{40} when divided by 27 is 10.

Problem 3-99:

Find the remainder when 5^{183} is divided by 99.

Solution:

We have to calculate the remainder modulo 99. Now we know that the Euler phi function $\phi(99) = \phi(3^2 \cdot 11) = 33 \cdot \left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{11}\right) = 60$. Hence because $\gcd(5, 99) = 1$, the Euler-Fermat Theorem tells us that $5^{60} \equiv 1 \pmod{99}$. Now, by the Division Algorithm, $183 = 60(3) + 3$. Therefore,

$$5^{183} \equiv 5^{60(3)+3} \equiv 1 \cdot 5^3 \equiv 125 \equiv 26 \pmod{99}.$$

Thus, the remainder of 5^{183} when divided by 99 is 26.

Problem 3-100:

Find the remainder when $2^{2^{405}}$ is divided by 23.

Solution:

We have to calculate the remainder modulo 23. Now we know that 23 is a prime and so Fermat's Little Theorem tells us that $2^{22} \equiv 1 \pmod{23}$. Therefore $2^{22k} \equiv 1 \pmod{23}$ for any positive integer k, and so we would like to look at the exponent $e = 2^{405}$ modulo 22. By Proposition 3.64,

$$e \equiv 2^{405} \pmod{22} \qquad \Longleftrightarrow \qquad \begin{cases} e \equiv 2^{405} \pmod{2} \\ e \equiv 2^{405} \pmod{11} \end{cases}$$

We know that $2^{405} \equiv 0 \pmod 2$, so the first congruence is equivalent to $e \equiv 0 \pmod 2$. Fermat's Little Theorem tells us that $2^{10} \equiv 1 \pmod{11}$. By the Division Algorithm, $405 = 10(40) + 5$, so, for the second congruence,

$$2^{405} \equiv 2^{10(40)+5} \equiv 1 \cdot 2^5 \equiv 32 \equiv 10 \pmod{11}.$$

Thus, the congruence $x \equiv 2^{405} \pmod{22}$ is equivalent to the simultaneous congruences

$$\begin{aligned} e &\equiv 0 \pmod 2 \\ e &\equiv 10 \pmod{11}. \end{aligned}$$

The solution $x \equiv 10 \pmod{22}$ satisfies both congruences so, by the Chinese Remainder Theorem, it is the complete solution. Hence

$$2^{405} \equiv 10 \pmod{22}$$

and $2^{405} = 10 + 22z$ for some $z \in \mathbb{Z}$. Therefore,

$$2^{2^{405}} \equiv 2^{22z+10} \equiv 2^{10} \equiv 1024 \equiv 12 \pmod{23}.$$

Hence the remainder when $2^{2^{405}}$ is divided by 23 is 12.

Problem 3-101:

Find the last two digits of 747^{130}.

Solution:

For the last two digits, we have to calculate the remainder modulo 100. We know that $\phi(100) = \phi(2^2 \cdot 5^2) = 100 \cdot \left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{5}\right) = 40$. Because $\gcd(747, 100) = 1$, the Euler-Fermat Theorem tells us that

$$747^{40} \equiv 1 \pmod{100}$$

and so $747^{40k} \equiv 1 \pmod{100}$ for any positive integer k. By the Division Algorithm, $130 = 40(3) + 10$, so

$$747^{130} \equiv 747^{40(3)+10} \equiv 1 \cdot 747^{10} \equiv 47^{10} \pmod{100}.$$

Because $100 = 25 \cdot 4$ and $\gcd(4, 25) = 1$, Proposition 3.64 tells us that

$$x \equiv 47^{10} \pmod{100} \qquad \Longleftrightarrow \qquad \begin{cases} x \equiv 47^{10} \pmod 4 \\ x \equiv 47^{10} \pmod{25}. \end{cases}$$

The congruence modulo 4 is equivalent to $x \equiv (-1)^{10} \equiv 1 \pmod 4$.

The congruence modulo 25 is equivalent to

$$x \equiv (-3)^{10} \equiv 3^{10} \equiv 3 \cdot \left(3^3\right)^3 \equiv 3 \cdot 27^3 \equiv 3 \cdot 2^3 \equiv 24 \pmod{25}.$$

Thus, the congruence $x \equiv 47^{10} \pmod{100}$ is equivalent to the simultaneous congruences

$$\begin{aligned} x &\equiv 1 \pmod 4 \\ x &\equiv 24 \pmod{25}. \end{aligned}$$

An integer x satisfies the second congruence if and only if

$$x = 24 + 25y \quad \text{for some integer } y \in \mathbb{Z}$$

Substitute this into the first congruence.

$$\begin{aligned} 24 + 25y &\equiv 1 \pmod 4 \\ y &\equiv 1 \pmod 4 \\ y &= 1 + 4z \quad \text{for } z \in \mathbb{Z} \\ x &= 24 + 25(1 + 4z) \quad \text{for } z \in \mathbb{Z} \\ &= 49 + 100z \quad \text{for } z \in \mathbb{Z} \end{aligned}$$

Thus, the remainder of 47^{10} modulo 100 is 49 and these are precisely the last two digits of 747^{130}.

Problem 3-102:

Find the last two digits of 287^{449}.

Solution:

For the last two digits, we have to calculate the remainder modulo 100. We know that $\phi(100) = \phi(2^2 \cdot 5^2) = 100 \cdot \left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{5}\right) = 40$. Because $\gcd(287, 100) = 1$, the Euler-Fermat Theorem tells us that

$$287^{40} \equiv 1 \pmod{100}$$

and so $287^{40k} \equiv 1 \pmod{100}$ for any positive integer k. By the Division Algorithm, $449 = 40(11) + 9$, so

$$287^{449} \equiv 287^{40(11)+9} \equiv 1 \cdot 287^9 \equiv 87^9 \pmod{100}.$$

Because $100 = 25 \cdot 4$ and $\gcd(4, 25) = 1$, Proposition 3.64 tells us that

$$x \equiv 87^9 \pmod{100} \qquad \Longleftrightarrow \qquad \begin{cases} x \equiv 87^9 \pmod 4 \\ x \equiv 87^9 \pmod{25}. \end{cases}$$

The modulo 4 congruence is equivalent to $x \equiv (-1)^9 \equiv -1 \pmod 4$.

The modulo 25 congruence is equivalent to

$$x \equiv 12^9 \equiv \left(12^3\right)^3 \equiv 1728^3 \equiv 3^3 \equiv 27 \equiv 2 \pmod{25}.$$

Thus, the congruence $x \equiv 87^9 \pmod{100}$ is equivalent to the simultaneous congruences

$$\begin{aligned} x &\equiv 3 \pmod 4 \\ x &\equiv 2 \pmod{25}. \end{aligned}$$

An integer x satisfies the second congruence if and only if

$$x = 2 + 25y \quad \text{for some integer } y \in \mathbb{Z}$$

Substitute this into the first congruence.

$$\begin{aligned} 2 + 25y &\equiv 3 \pmod 4 \\ y &\equiv 1 \pmod 4 \\ y &= 1 + 4z \quad \text{for } z \in \mathbb{Z} \\ x &= 2 + 25(1 + 4z) \quad \text{for } z \in \mathbb{Z} \\ &= 27 + 100z \quad \text{for } z \in \mathbb{Z} \end{aligned}$$

Thus, the remainder of 87^9 modulo 100 is 27 and these are precisely the last two digits of 287^{449}.

Problem 3-103:

Find the last two digits of 95^{95}.

Solution:

For the last two digits, we have to calculate the remainder modulo 100. Because $100 = 25 \cdot 4$ and $\gcd(4, 25) = 1$, Proposition 3.64 tells us that

$$x \equiv 95^{95} \pmod{100} \qquad \Longleftrightarrow \qquad \begin{cases} x \equiv 95^{95} \pmod 4 \\ x \equiv 95^{95} \pmod{25}. \end{cases}$$

The modulo 4 congruence is equivalent to $x \equiv (-1)^{95} \equiv -1 \pmod 4$.

Since $95^{95} = (5 \cdot 19)^{95} = 5^{95} \cdot 19^{95}$, it is clear that $5^2 | 95^{95}$, so $95^{95} \equiv 0 \pmod{25}$. Hence the modulo 25 congruence is equivalent to $x \equiv 0 \pmod{25}$.

Thus, the congruence $x \equiv 95^{95} \pmod{100}$ is equivalent to the simultaneous congruences

$$\begin{aligned} x &\equiv -1 \pmod 4 \\ x &\equiv 0 \pmod{25} \end{aligned}$$

The second congruence has solutions $x \equiv 0,\ 25,\ 50,\ 75 \pmod{100}$ so, by inspection, $x = 75$ is a solution to both. Hence, by the Chinese Remainder Theorem,

$$x \equiv 75 \pmod{100}$$

is the complete solution to the simultaneous congruences.

Thus, the remainder modulo 100 of 95^{95} is 75 and these are precisely the last two digits of 95^{95} .

Problem 3-104:

Find the last two digits of 2554^{3333}.

Solution:

For the last two digits, we have to calculate the remainder modulo 100. The congruence $2554^{3333} \equiv \pmod{100}$ is equivalent to $54^{3333} \equiv \pmod{100}$. Because $100 = 25 \cdot 4$ and $\gcd(4, 25) = 1$, Proposition 3.64 tells us that

$$x \equiv 54^{3333} \pmod{100} \qquad \Longleftrightarrow \qquad \begin{cases} x \equiv 54^{3333} \pmod{4} \\ x \equiv 54^{3333} \pmod{25}. \end{cases}$$

The congruence modulo 4 is equivalent to $x \equiv 2^{3333} \equiv 0 \pmod{4}$.

The modulo 25 congruence is equivalent to $x \equiv 4^{3333} \equiv 2^{6666} \pmod{25}$. Since $\gcd(2, 25) = 1$ and $\phi(25) = \phi(5^2) = 25\left(1 - \frac{1}{5}\right) = 20$, the Euler-Fermat Theorem tells us that $2^{20} \equiv 1 \pmod{25}$. By the Division Algorithm we have $6666 = 20(333) + 6$, so

$$x \equiv 2^{6666} \equiv 2^{20(333)+6} \equiv \left(2^{20}\right)^{333} \cdot 2^6 \equiv 1 \cdot 2^6 \equiv 64 \equiv 14 \pmod{25}.$$

Thus, the congruence $x \equiv 2554^{3333} \pmod{100}$ is equivalent to the simultaneous congruences,

$$\begin{aligned} x &\equiv 0 \pmod{4} \\ x &\equiv 14 \pmod{25}. \end{aligned}$$

The second congruence has solutions $x \equiv 14,\ 39,\ 64,\ 89 \pmod{100}$ so, by inspection, $x = 64$ is a solution to both. Hence, by the Chinese Remainder Theorem

$$x \equiv 64 \pmod{100}$$

is the complete solution to the simultaneous congruences.

Thus, the remainder modulo 100 of 2554^{3333} is 64 and these are precisely the last two digits of 2554^{3333} .