Introduction to Congruences

DEFINITION: Let m be a positive integer. Then integers a and b are **congruent modulo** m, denoted by

$$a \equiv b \pmod{m}$$

if $m \mid (a - b)$.

EXAMPLE:

$3 \equiv 1 \pmod{2}$, $6 \equiv 4 \pmod{2}$, $-14 \equiv 0 \pmod{7}$, $25 \equiv 16 \pmod{9}$, $43 \equiv -27 \pmod{35}$

THEOREM 1: If a and b are integers, then $a \equiv b \pmod{m}$ if and only if there is an integer k such that $a = b + km$.

Proof: If $a \equiv b \pmod{m}$, then $m \mid (a-b)$. This means that there is an integer k with $km = a-b$, so that $a = b + km$.

Conversely, if there is an integer k with $a = b + km$, then $km = a - b$. Hence, $m \mid (a - b)$, and consequently, $a \equiv b \pmod{m}$. ■

EXAMPLE: We have $19 \equiv -2 \pmod{7}$ and $19 = -2 + 3 \cdot 7$.

THEOREM 2: Let m be a positive integer. Congruences modulo m satisfy the following properties:

(i) *Reflexive property.* If a is an integer, then $a \equiv a \pmod{m}$.

(ii) *Symmetric property.* If a and b are integers such that $a \equiv b \pmod{m}$, then $b \equiv a \pmod{m}$.

(iii) *Transitive property.* If a, b, and c are integers with $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$, then $a \equiv c \pmod{m}$.

Proof:

(i) We see that $a \equiv a \pmod{m}$, because $m \mid (a - a) = 0$.

(ii) If $a \equiv b \pmod{m}$, then $m \mid (a - b)$. Hence, there is an integer k such that $km = a - b$. This shows that $(-k)m = b - a$, so that $m \mid (b - a)$. Consequently, $b \equiv a \pmod{m}$.

(iii) If $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$, then $m \mid (a - b)$ and $m \mid (b - c)$. Since

$$a - c = (a - b) + (b - c)$$

it follows that $m \mid (a - c)$ by Theorem 2 from Section 1.5. Therefore, $a \equiv c \pmod{m}$. ■

REMARK: By Theorem 2, we see that the set of integers is divided into m different sets called *congruence classes modulo* m, each containing integers which are mutually congruent modulo m. Note that when $m = 2$, this gives us the two classes of even and odd integers.

EXAMPLE: The three congruence classes modulo 3 are given by

$$\ldots \equiv -9 \equiv -6 \equiv -3 \equiv 0 \equiv 3 \equiv 6 \equiv 9 \pmod{3}$$

$$\ldots \equiv -8 \equiv -5 \equiv -2 \equiv 1 \equiv 4 \equiv 7 \equiv 10 \pmod{3}$$

$$\ldots \equiv -7 \equiv -4 \equiv -1 \equiv 2 \equiv 5 \equiv 8 \equiv 11 \pmod{3}$$

DEFINITION: A **complete system of residues modulo** m is a set of integers such that every integer is congruent modulo m to exactly one integer of the set.

EXAMPLE: The Division Algorithm shows that the set of integers $0, 1, 2, \ldots, m-1$ is a complete system of residues modulo m.

LEMMA: A set of m incongruent integers modulo m forms a complete set of residues modulo m.

THEOREM 3: If $r_1, r_2, \ldots, r_m$ is a complete system of residues modulo m, and if a is a positive integer with $(a, m) = 1$, then

$$ar_1 + b, \quad ar_2 + b, \ldots ar_m + b$$

is a complete system of residues modulo m for any integer b.

THEOREM 4: If a, b, c, d, and m are integers such that $m > 0$, $a \equiv b \pmod{m}$, and $c \equiv d \pmod{m}$, then

(i) $a + c \equiv b + d \pmod{m}$

(ii) $a - c \equiv b - d \pmod{m}$

(iii) $ac \equiv bd \pmod{m}$

Proof: Since $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, we know that $m \mid (a - b)$ and $m \mid (c - d)$.

To prove (i), note that

$$(a + c) - (b + d) = (a - b) + (c - d)$$

Hence

$$m \mid [(a + c) - (b + d)]$$

by Theorem 2 from Section 1.5. Therefore, $a + c \equiv b + d \pmod{m}$.

To prove (ii), note that

$$(a - c) - (b - d) = (a - b) - (c - d)$$

Hence

$$m \mid [(a - c) - (b - d)]$$

by Theorem 2 from Section 1.5. Therefore, $a - c \equiv b - d \pmod{m}$.

To prove (iii), note that

$$ac - bd = ac - bc + bc - bd = c(a - b) + b(c - d)$$

Hence

$$m \mid [(ac - bd)]$$

by Theorem 2 from Section 1.5. Therefore, $ac \equiv bd \pmod{m}$. ■

EXAMPLE: Because $13 \equiv 3 \pmod{5}$ and $7 \equiv 2 \pmod{5}$, using the Theorem above we see that

$$\begin{array}{lcl} 13 + 7 \equiv 3 + 2 \pmod{5} & & 20 \equiv 5 \pmod{5} \\ 13 - 7 \equiv 3 - 2 \pmod{5} & \Longrightarrow & 6 \equiv 1 \pmod{5} \\ 13 \cdot 7 \equiv 3 \cdot 2 \pmod{5} & & 91 \equiv 6 \pmod{5} \end{array}$$

COROLLARY: If a, b, c, and m are integers, with $m > 0$, such that $a \equiv b \pmod{m}$, then

(i) $a + c \equiv b + c \pmod{m}$

(ii) $a - c \equiv b - c \pmod{m}$

(iii) $ac \equiv bc \pmod{m}$

Proof: The result immediately follows from the Theorem above with $d = c$. ■

EXAMPLE: Because $19 \equiv 3 \pmod{8}$, using the Corollary above we see that

$$\begin{array}{rcl} 19 + 7 \equiv 3 + 7 \pmod{8} & & 26 \equiv 10 \pmod{8} \\ 19 - 4 \equiv 3 - 4 \pmod{8} & \Longrightarrow & 15 \equiv -1 \pmod{8} \\ 19 \cdot 2 \equiv 3 \cdot 2 \pmod{8} & & 38 \equiv 6 \pmod{8} \end{array}$$

THEOREM 5: If a, b, k, and m are integers such that $k > 0,\ m > 0$, and $a \equiv b \pmod{m}$, then $a^k \equiv b^k \pmod{m}$.

Proof: Because $a \equiv b \pmod{m}$, we have $m \mid (a - b)$, and because

$$a^k - b^k = (a - b)(a^{k-1} + a^{k-2}b + \ldots + ab^{k-2} + b^{k-1})$$

we see that $(a - b) \mid (a^k - b^k)$. Therefore, by Theorem 1 from Section 1.5 it follows that $m \mid (a^k - b^k)$. Hence, $a^k \equiv b^k \pmod{m}$. ■

EXAMPLE: Because $7 \equiv 2 \pmod{5}$, the Theorem above tells us that

$$7^3 \equiv 2^3 \ (\bmod\ 5) \qquad \Longrightarrow \qquad 343 \equiv 8 \ (\bmod\ 5)$$

THEOREM 6: If $a \equiv b \pmod{m_1},\ a \equiv b \pmod{m_2}, \ldots, a \equiv b \pmod{m_k}$, where $a, b, m_1, m_2, \ldots, m_k$ are integers with $m_1, m_2, \ldots, m_k$ positive, then

$$a \equiv b \pmod{[m_1, m_2, \ldots, m_k]}$$

where $[m_1, m_2, \ldots, m_k]$ denotes the least common multiple of $m_1, m_2, \ldots, m_k$.

COROLLARY: If $a \equiv b \pmod{m_1},\ a \equiv b \pmod{m_2}, \ldots, a \equiv b \pmod{m_k}$, where a and b are integers and $m_1, m_2, \ldots, m_k$ are pairwise relatively prime positive integers, then

$$a \equiv b \pmod{m_1, m_2, \ldots, m_k}$$

THEOREM 7: If a, b, c, and m are integers such that $m > 0,\ d = (c, m)$, and $ac \equiv bc \pmod{m}$, then $a \equiv b \pmod{m/d}$.

Proof: If $ac \equiv bc \pmod{m}$, we know that

$$m \mid (ac - bc) = c(a - b)$$

Hence, there is an integer k with

$$c(a - b) = km$$

By dividing both sides by d, we have

$$(c/d)(a-b) = k(m/d)$$

Because $(m/d, c/d) = 1$, by Theorem 1 from Section 3.5 it follows that

$$m/d \mid (a-b)$$

Hence, $a \equiv b \pmod{m/d}$. ■

EXAMPLE: Because $50 \equiv 20 \pmod{15}$ and $(10, 15) = 5$, we see that

$$50/10 \equiv 20/10 \pmod{15/5} \qquad \text{or} \qquad 5 \equiv 2 \pmod{3}$$

COROLLARY: If a, b, c, and m are integers such that $m > 0$, $(c, m) = 1$, and $ac \equiv bc \pmod{m}$, then $a \equiv b \pmod{m}$.

EXAMPLE: Because $42 \equiv 7 \pmod{5}$ and $(5, 7) = 1$, we can conclude that $42/7 \equiv 7/7 \pmod{5}$, or that $6 \equiv 1 \pmod{5}$.

Appendix

PROBLEM 1: Prove that

(a) $10 \mid (11^{10} - 1)$ (b) $10 \mid (101^{2003} - 1)$

Solution:

(a) We have $11 \equiv 1 \bmod 10$ therefore by Theorem 5 we get $11^{10} \equiv 1^{10} \equiv 1 \pmod{10}$ which means that $10 \mid (11^{10} - 1)$.

(b) We have

$$101 \equiv 1 \bmod 10$$

therefore by Theorem 5 we get

$$101^{2003} \equiv 1^{2003} \equiv 1 \pmod{10}$$

which means that $10 \mid (101^{2003} - 1)$.

PROBLEM 2: Find the last digit of

(a) 4321^{4321} (b) 345271^{79399}

Solution:

(a) It is obvious that $4321 \equiv 1 \pmod{10}$ therefore by Theorem 5 we have

$$4321^{4321} \equiv 1^{4321} \equiv 1 \pmod{10}$$

This means that the last digit is 1.

(b) Similarly, since $345271 \equiv 1 \pmod{10}$, by Theorem 5 we have

$$345271^{79399} \equiv 1^{79399} \equiv 1 \pmod{10}$$

This means that the last digit of 345271^{79399} is 1.

PROBLEM 3: Prove that there is no perfect square a^2 which is congruent to 2 modulo 3.

Solution: By the Division Algorithm, each integer number is congruent to $0, 1$, or 2 modulo 3. Consider all these cases and use Theorem 5:

If $a \equiv 0 \pmod 3$ then $a^2 \equiv 0^2 \equiv 0 \pmod 3$
If $a \equiv 1 \pmod 3$ then $a^2 \equiv 1^2 \equiv 1 \pmod 3$
If $a \equiv 2 \pmod 3$ then $a^2 \equiv 2^2 \equiv 1 \pmod 3$

So, $a^2 \equiv 0$ or 1 mod 3. Therefore $a^2 \not\equiv 2 \pmod 3$.

PROBLEM 4: Prove that there is no perfect square a^2 which is congruent to 2 or 3 modulo 4.

Solution: By the Division Algorithm, each integer number is congruent to $0, 1, 2$, or 3 modulo 4. Consider all these cases and use Theorem 5:

If $a \equiv 0 \pmod 4$ then $a^2 \equiv 0^2 \equiv 0 \pmod 4$
If $a \equiv 1 \pmod 4$ then $a^2 \equiv 1^2 \equiv 1 \pmod 4$
If $a \equiv 2 \pmod 4$ then $a^2 \equiv 2^2 \equiv 0 \pmod 4$
If $a \equiv 3 \pmod 4$ then $a^2 \equiv 3^2 \equiv 1 \pmod 4$

So, $a^2 \equiv 0$ or 1 modulo 4. Therefore $a^2 \not\equiv 2$ or 3 $\pmod 4$.

PROBLEM 5: Prove that there is no integer number a such that $a^4 \equiv 3 \pmod 4$.

Solution: By the Division Algorithm, each integer number is congruent to $0, 1, 2$, or 3 modulo 4. Consider all these cases and use Theorem 5:

If $a \equiv 0 \pmod 4$ then $a^4 \equiv 0^4 \equiv 0 \pmod 4$
If $a \equiv 1 \pmod 4$ then $a^4 \equiv 1^4 \equiv 1 \pmod 4$
If $a \equiv 2 \pmod 4$ then $a^4 \equiv 2^4 \equiv 0 \pmod 4$
If $a \equiv 3 \pmod 4$ then $a^4 \equiv 3^4 \equiv 1 \pmod 4$

So, $a^4 \equiv 0$ or 1 mod 4. Therefore $a^4 \not\equiv 3 \pmod 4$.

PROBLEM 6: Prove that there is no perfect square a^2 whose last digit is 3.

Solution: By the Division Algorithm, each integer number is congruent to $0, 1, 2, \ldots, 8$ or 9 modulo 10. Consider all these cases and use Theorem 5:

If $a \equiv 0 \pmod{10}$ then $a^2 \equiv 0^2 \equiv 0 \pmod{10}$
If $a \equiv 1 \pmod{10}$ then $a^2 \equiv 1^2 \equiv 1 \pmod{10}$
If $a \equiv 2 \pmod{10}$ then $a^2 \equiv 2^2 \equiv 4 \pmod{10}$
If $a \equiv 3 \pmod{10}$ then $a^2 \equiv 3^2 \equiv 9 \pmod{10}$
If $a \equiv 4 \pmod{10}$ then $a^2 \equiv 4^2 \equiv 6 \pmod{10}$
If $a \equiv 5 \pmod{10}$ then $a^2 \equiv 5^2 \equiv 5 \pmod{10}$
If $a \equiv 6 \pmod{10}$ then $a^2 \equiv 6^2 \equiv 6 \pmod{10}$
If $a \equiv 7 \pmod{10}$ then $a^2 \equiv 7^2 \equiv 9 \pmod{10}$
If $a \equiv 8 \pmod{10}$ then $a^2 \equiv 8^2 \equiv 4 \pmod{10}$
If $a \equiv 9 \pmod{10}$ then $a^2 \equiv 9^2 \equiv 1 \pmod{10}$

So, $a^2 \equiv 0, 1, 4, 5, 6$ or 9 modulo 10. Therefore $a^2 \not\equiv 3 \pmod{10}$, and the result follows.

PROBLEM 7: Prove that 444444444444444443 is not a perfect square.

Solution 1: 444444444444444443 is congruent to 3 modulo 4, which is impossible by Problem 4.

Solution 2: The last digit is 3, which is impossible by Problem 6.

PROBLEM 8: Prove that $888\ldots882$ is not a perfect square.

Solution 1: $888\ldots882$ is congruent to 2 modulo 4, which is impossible by Problem 4.

Solution 2: The last digit is 2, which is impossible by Problem 6.

PROBLEM 9: Prove that there is no perfect square a^2 whose last digits are 85.

Solution: It follows from Problem 6 that $a^2 \equiv 5$ mod 10 only if $a \equiv 5 \pmod{10}$. Therefore $a^2 \equiv 85 \pmod{100}$ only if $a \equiv 5, 15, 25, \ldots, 95 \pmod{100}$. If we consider all these cases and use Theorem 5 is the same manner as in Problem 6, we will see that $a^2 \equiv 25 \pmod{100}$. Therefore $a^2 \not\equiv 85 \pmod{100}$, and the result follows.

PROBLEM 10: Prove that the following equations have no solutions in integer numbers.

(a) $x^2 - 3y = 5$ (b) $3x^2 - 4y = 5$ (c) $x^4 - 4y = 3$ (d) $x^2 - y^2 = 2002$

Solution:

(a) Rewrite this equation as $x^2 = 3y + 5$, which means that $x^2 \equiv 5 \equiv 2 \pmod 3$. This is impossible by Problem 3.

(b) Rewrite this equation as $3x^2 = 4y+5$, which means that $3x^2 \equiv 5 \equiv 1 \pmod 4$. On the other hand, by Problem 4 we have $x^2 \equiv 0$ or $1 \pmod 4$, hence $3x^2 \equiv 0$ or $3 \pmod 4$ by Theorem 4 or its Corollary. Therefore $x^2 \not\equiv 1 \pmod 4$.

(c) Rewrite this equation as $x^4 = 4y + 3$, which means that $x^4 \equiv 3 \pmod 4$. This is impossible by Problem 5.

(d) By Problem 4, we have $x^2 \equiv 0$ or $1 \pmod 4$, hence $x^2 - y^2 \equiv 0, 1$ or $-1 \pmod 4$. On the other hand, $2002 \equiv 2 \pmod 4$. Therefore $x^2 - y^2 \not\equiv 2002 \pmod 4$.