Applications of Fermat’s Little Theorem and Congruences

Definition:
Let \( m \) be a positive integer. Then integers \( a \) and \( b \) are congruent modulo \( m \), denoted by
\[
a \equiv b \mod m,
\]
if \( m \mid (a - b) \).

Example:
\[
3 \equiv 1 \mod 2, \quad 6 \equiv 4 \mod 2, \quad -14 \equiv 0 \mod 7, \quad 25 \equiv 16 \mod 9, \quad 43 \equiv -27 \mod 35.
\]

Properties:
Let \( m \) be a positive integer and let \( a, b, c, d \) be integers. Then
1. \( a \equiv a \mod m \)
2. If \( a \equiv b \mod m \), then \( b \equiv a \mod m \).
3. If \( a \equiv b \mod m \) and \( b \equiv c \mod m \), then \( a \equiv c \mod m \).
4. (a) If \( a \equiv qm + r \mod m \), then \( a \equiv r \mod m \).
   (b) Every integer \( a \) is congruent mod \( m \) to exactly one of \( 0, 1, \ldots, m - 1 \).
5. If \( a \equiv b \mod m \) and \( c \equiv d \mod m \), then
\[
a \pm c \equiv b \pm d \mod m \quad \text{and} \quad ac \equiv bd \mod m.
\]
5'. If \( a \equiv b \mod m \), then
\[
a \pm c \equiv b \pm c \mod m \quad \text{and} \quad ac \equiv bc \mod m.
\]
5''. If \( a \equiv b \mod m \), then
\[
a^n \equiv b^n \mod m \quad \text{for any} \ n \in \mathbb{Z}^+.
\]
6. If \((c, m) = 1\) and \( ac \equiv bc \mod m \), then \( a \equiv b \mod m \).

Theorem (Fermat’s Little Theorem): Let \( p \) be a prime. Then
\[
n^p \equiv n \mod p
\]
for any integer \( n \geq 1 \).

Corollary: Let \( p \) be a prime. Then
\[
n^{p-1} \equiv 1 \mod p
\]
for any integer \( n \geq 1 \) with \((n, p) = 1\).
1. Find all solutions to each of the following congruences:
   (i) \( 2x \equiv 1 \mod 3 \).
   (ii) \( 3x \equiv 4 \mod 8 \).
   (iii) \( 6x \equiv 3 \mod 15 \).
   (iv) \( 8x \equiv 7 \mod 18 \).
   (v) \( 9x + 23 \equiv 28 \mod 25 \).

2. What is the last digit of \( 4321^{4321} \)?

3. Prove that there is no perfect square \( a^2 \) which is congruent to 2 mod 4.

4. Prove that there is no perfect square \( a^2 \) whose last digit is 2.

5. Prove that 888...882 is not a perfect square.

6*. Prove that there is no perfect square \( a^2 \) whose last digits are 85.

7. Prove that the following equations have no solutions in integer numbers:
   (i) \( x^2 - 3y = 5 \)
   (ii) \( 3x^2 - 4y = 5 \)
   (iii) \( x^2 - y^2 = 2002 \)

8. Prove that \( 10 \mid 11^{10} - 1 \).

9*. Prove that \( 300 \mid 11^{10} - 1 \).

10. Prove that \( 17 \mid a^{80} - 1 \) for any \( a \in \mathbb{Z}^+ \) with \( (a, 17) = 1 \).

11*. What is the remainder after dividing \( 3^{50} \) by 7?
**THEOREM AND EXAMPLES**

**Theorem:** If \((a, m) = 1\), then, for every integer \(b\), the congruence

\[ ax \equiv b \mod m \]  

(1)

has exactly one solution

\[ x \equiv bs \mod m, \]  

(2)

where \(s\) is such a number that

\[ as \equiv 1 \mod m. \]  

(3)

**Proof (Sketch):** We show that (2) is the solution of (1). In fact, if we multiply (2) by \(a\) and (3) by \(b\) (we can do that by property 5'), we get

\[ ax \equiv abs \mod m \quad \text{and} \quad bsa \equiv b \mod m, \]

which imply (1) by property 3. ■

**Example 1:** Find all solutions of the following congruence

\[ 2x \equiv 5 \mod 7. \]

**Solution:** We first note that \((2, 7) = 1\). Therefore we can apply the theorem above. Since \(2 \cdot 4 \equiv 1 \mod 7\), we get

\[ x \equiv 5 \cdot 4 \equiv 6 \mod 7. \]

**Example 2:** Find all solutions of the following congruence

\[ 2x \equiv 5 \mod 8. \]

**Solution:** Since \((2, 8) = 2\), we can’t apply the theorem above directly. We now note that \(2x \equiv 5 \mod 8\) is equivalent to \(2x - 8y = 5\), which is impossible, since the left-hand side is divisible by 2, whereas the right-hand side is not. So, this equation has no solutions.

**Example 3:** Find all solutions of the following congruence

\[ 4x \equiv 2 \mod 6. \]

**Solution:** Since \((4, 6) = 2\), we can’t apply the theorem above directly again. However, canceling out 2 (think about that!), we obtain

\[ 2x \equiv 1 \mod 3. \]

Note that \((2, 3) = 1\). Therefore we can apply the theorem above to the new equation. Since \(2 \cdot 2 \equiv 1 \mod 3\), we get

\[ x \equiv 1 \cdot 2 \equiv 2 \mod 3. \]

**Example 4:** What is the last digit of \(345271^{79399}\)?

**Solution:** It is obvious that \(345271 \equiv 1 \mod 10\), therefore by property 5' we have

\[ 345271^{79399} \equiv 1^{79399} \equiv 1 \mod 10. \]

This means that the last digit of \(345271^{79399}\) is 1.
Example 5: Prove that there is no integer number $a$ such that $a^4$ is congruent to 3 mod 4.

Solution: By the property 4(a) each integer number is congruent to 0, 1, 2, or 3 mod 4. Consider all these cases and use property 5′:

- If $a \equiv 0 \text{ mod } 4$, then $a^4 \equiv 0^4 \equiv 0 \text{ mod } 4$.
- If $a \equiv 1 \text{ mod } 4$, then $a^4 \equiv 1^4 \equiv 1 \text{ mod } 4$.
- If $a \equiv 2 \text{ mod } 4$, then $a^4 \equiv 2^4 \equiv 0 \text{ mod } 4$.
- If $a \equiv 3 \text{ mod } 4$, then $a^4 \equiv 3^4 \equiv 1 \text{ mod } 4$.

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

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

Solution: By the property 4(a) each integer number is congruent to 0, 1, 2, . . . , 8 or 9 mod 10. Consider all these cases and use property 5′′:

- If $a \equiv 0 \text{ mod } 10$, then $a^2 \equiv 0^2 \equiv 0 \text{ mod } 10$.
- If $a \equiv 1 \text{ mod } 10$, then $a^2 \equiv 1^2 \equiv 1 \text{ mod } 10$.
- If $a \equiv 2 \text{ mod } 10$, then $a^2 \equiv 2^2 \equiv 4 \text{ mod } 10$.
- If $a \equiv 3 \text{ mod } 10$, then $a^2 \equiv 3^2 \equiv 9 \text{ mod } 10$.
- If $a \equiv 4 \text{ mod } 10$, then $a^2 \equiv 4^2 \equiv 6 \text{ mod } 10$.
- If $a \equiv 5 \text{ mod } 10$, then $a^2 \equiv 5^2 \equiv 5 \text{ mod } 10$.
- If $a \equiv 6 \text{ mod } 10$, then $a^2 \equiv 6^2 \equiv 6 \text{ mod } 10$.
- If $a \equiv 7 \text{ mod } 10$, then $a^2 \equiv 7^2 \equiv 9 \text{ mod } 10$.
- If $a \equiv 8 \text{ mod } 10$, then $a^2 \equiv 8^2 \equiv 4 \text{ mod } 10$.
- If $a \equiv 9 \text{ mod } 10$, then $a^2 \equiv 9^2 \equiv 1 \text{ mod } 10$.

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

Example 7: Prove that 444444444444444444443 is not a perfect square.

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

Example 8: Prove that the equation $x^4 - 4y = 3$ has no solutions in integer numbers.

Solution: Rewrite this equation as $x^4 = 4y + 3$, which means that $x^4 \equiv 3 \text{ mod } 4$, which is impossible by Example 5.

Example 9: Prove that $10 | 101^{2003} - 1$.

Solution: We have

\[
101 \equiv 1 \text{ mod } 10,
\]

therefore by property 5′′ we get

\[
101^{2003} \equiv 1^{2003} \equiv 1 \text{ mod } 10,
\]

which means that $10 | 101^{2003} - 1$.

Example 10: Prove that $23 | a^{154} - 1$ for any $a \in \mathbb{Z}^+$ with $(a, 23) = 1$.

Solution: By Fermat’s Little theorem we have

\[
a^{22} \equiv 1 \text{ mod } 23,
\]

therefore by property 5′′ we get

\[
a^{22 \cdot 7} \equiv 1^7 \equiv 1 \text{ mod } 23,
\]

and the result follows.
SOLUTIONS

Problem 1(i): Find all solutions of the congruence $2x \equiv 1 \pmod{3}$.
Solution: We first note that $(2, 3) = 1$. Therefore we can apply the theorem above. Since $2 \cdot 2 \equiv 1 \pmod{3}$, we get $x \equiv 1 \cdot 2 \equiv 2 \pmod{3}$.

Problem 1(ii): Find all solutions of the congruence $3x \equiv 4 \pmod{8}$.
Solution: We first note that $(3, 8) = 1$. Therefore we can apply the theorem above. Since $3 \cdot 3 \equiv 1 \pmod{8}$, we get $x \equiv 4 \cdot 3 \equiv 12 \equiv 4 \pmod{8}$.

Problem 1(iii): Find all solutions of the congruence $6x \equiv 3 \pmod{15}$.
Solution: Since $(6, 15) = 3$, we can’t apply the theorem above directly again. However, canceling out 3, we obtain $2x \equiv 1 \pmod{5}$. Note that $(2, 5) = 1$. Therefore we can apply the theorem above to the new equation. Since $2 \cdot 3 \equiv 1 \pmod{5}$, we get $x \equiv 1 \cdot 3 \equiv 3 \pmod{5}$.

Problem 1(iv): Find all solutions of the congruence $8x \equiv 7 \pmod{18}$.
Solution: Since $(8, 18) = 2$, we can’t apply the theorem above directly. We now note that $8x \equiv 7 \pmod{18}$ is equivalent to $8x - 18y = 7$, which is impossible, since the left-hand side is divisible by 2, whereas the right-hand side is not. So, this equation has no solutions.

Problem 1(v): Find all solutions of the congruence $9x + 23 \equiv 28 \pmod{25}$.
Solution: We first rewrite this congruence as $9x \equiv 5 \pmod{25}$. Note that $(9, 25) = 1$. Therefore we can apply the theorem above. Since $9 \cdot 14 \equiv 1 \pmod{25}$, we get $x \equiv 5 \cdot 14 \equiv 70 \equiv 20 \pmod{25}$.

Problem 2: What is the last digit of $4321^{4321}$?
Solution: It is obvious that $4321 \equiv 1 \pmod{10}$, therefore by property 5” we have $4321^{4321} \equiv 1^{4321} \equiv 1 \pmod{10}$. This means that the last digit is 1.

Problem 3: Prove that there is no perfect square $a^2$ which is congruent to 2 mod 4.
Solution: By the property 4(a) each integer number is congruent to 0, 1, 2, or 3 mod 4. Consider all these cases and use property 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 mod 4. Therefore $a^2 \not\equiv 2 \pmod{4}$.

Problem 4: Prove that there is no perfect square $a^2$ whose last digit is 2.
Solution: By the property 4(a) each integer number is congruent to 0, 1, 2, ..., 8 or 9 mod 10. Consider all these cases and use property 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 mod 10. Therefore $a^2 \not\equiv 2 \pmod{10}$, and the result follows.
Problem 5: Prove that $888 \ldots 882$ is not a perfect square.
Solution 1: We have $888 \ldots 882 = 4k + 2$. Therefore it is congruent to $2$ mod $4$ by property 4(a), which is impossible by Problem 3.
Solution 2: The last digit is $2$, which is impossible by Problem 4.

Problem 6*: Prove that there is no perfect square $a^2$ whose last digits are $85$.
Solution: It follows from problem 4 that $a^2 \equiv 5$ mod $10$ only if $a \equiv 5$ mod $10$. Therefore $a^2 \equiv 85$ mod $100$ only if $a \equiv 5, 15, 25, \ldots, 95$ mod $100$. If we consider all these cases and use property $5''$ the same manner as in problem 4, we will see that $a^2 \equiv 25$ mod $100$. Therefore $a^2 \neq 85$ mod $100$, and the result follows.

Problem 7(i): Prove that the equation $x^2 - 3y = 5$ has no solutions in integer numbers.
Solution: Rewrite this equation as $x^2 = 3y + 5$, which means that $x^2 \equiv 3 \equiv 2$ mod $3$. By the property 4(a) each integer number is congruent to $0$, $1$, or $2$ mod $3$. Consider all these cases and use property $5''$:
- If $a \equiv 0$ mod $3$, then $a^2 \equiv 0^2 \equiv 0$ mod $3$.
- If $a \equiv 1$ mod $3$, then $a^2 \equiv 1^2 \equiv 1$ mod $3$.
- If $a \equiv 2$ mod $3$, then $a^2 \equiv 2^2 \equiv 1$ mod $3$.
So, $a^2 \equiv 0$ or $1$ mod $3$. Therefore $a^2 \neq 2$ mod $3$.

Problem 7(ii): Prove that the equation $3x^2 - 4y = 5$ has no solutions in integer numbers.
Solution: Rewrite this equation as $3x^2 = 4y + 5$, which means that $3x^2 \equiv 5 \equiv 1$ mod $4$. On the other hand, by Problem 3 we have $x^2 \equiv 0$ or $1$ mod $4$, hence $3x^2 \equiv 0$ or $3$ mod $4$. Therefore $x^2 \neq 1$ mod $4$.

Problem 7(iii): Prove that the equation $x^2 - y^2 = 2002$ has no solutions in integer numbers.
Solution: By Problem 3 we have $x^2 \equiv 0$ or $1$ mod $4$, hence $x^2 - y^2 \equiv 0, 1$ or $-1$ mod $4$. On the other hand, $2002 \equiv 2$ mod $4$. Therefore $x^2 - y^2 \neq 2002$ mod $4$.

Problem 8: Prove that $10 \mid 11^{10} - 1$.
Solution: We have $11 \equiv 1$ mod $10$, therefore by property $5''$ we get $11^{10} \equiv 1^{10} \equiv 1$ mod $10$, which means that $10 \mid 11^{10} - 1$.

Problem 9*: Prove that $300 \mid 11^{10} - 1$.
Solution: We have
\[
11^{10} - 1 = (11^5 + 1)(11^5 - 1) = (11^5 + 1)(11 - 1)(11^4 + 11^3 + 11^2 + 11 + 1).
\]
Since $11 \equiv 1$ mod $10$, by property $5''$ we get $11^n \equiv 1$ mod $10$. Therefore by property $5$ we obtain
\[
11^4 + 11^3 + 11^2 + 11 + 1 \equiv 5 \text{ mod } 10.
\]
Note that $11^5 + 1$ is divisible by $2$ and $11 - 1$ is divisible by $10$. Therefore the right-hand side of (*) is divisible by $2 \cdot 10 \cdot 5 = 100$. On the other hand, by Fermat’s Little Theorem, $11^{10} - 1$ is divisible by $3$. Since $(3, 100) = 1$, the whole expression is divisible by $300$.

Problem 10: Prove that $17 \mid a^{80} - 1$ for any $a \in \mathbb{Z}^+$ with $(a, 17) = 1$.
Solution: By Fermat’s Little theorem we have $a^{16} \equiv 1$ mod $17$, therefore by property $5''$ we get $a^{16 \cdot 5} \equiv 1^5 \equiv 1$ mod $17$, and the result follows.

Problem 11: What is the remainder after dividing $3^{50}$ by $7$?
Solution: By Fermat’s Little theorem we have $3^6 \equiv 1$ mod $7$, therefore by property $5''$ we get $3^{6 \cdot 8} \equiv 1^8 \equiv 1$ mod $7$, therefore $3^{50} \equiv 9 \equiv 2$ mod $7$. 

6