Modular Arithmetic

Fix a positive integer m.

For any two integers a and b, we say a is **congruent** to b **modulo *m*,** denoted by $a \equiv b$ **(mod *m*)**, if m divides the difference $a - b$ evenly.

Intuitively, $a \equiv b$ **(mod *m*)** if a and b have the same remainder when each is divided by m.

For example, $7 \equiv 3 \pmod 4$, $11 \equiv 1 \pmod 5$, $5 \equiv -2 \pmod 7$, $8 \equiv 0 \pmod 8$.

Of course, $a \equiv a \pmod m$ for any $m > 0$.

Here are some nice properties:

- $a \equiv b \pmod m$, $c \equiv d \pmod m \Rightarrow a + c \equiv b + d \pmod m$
- $a \equiv b \pmod m$, $c \equiv d \pmod m \Rightarrow a - c \equiv b - d \pmod m$
- $a \equiv b \pmod m$, $c \equiv d \pmod m \Rightarrow ac \equiv bd \pmod m$
- $a \equiv b \pmod m \Rightarrow a^k \equiv b^k \pmod m$ for all integers $k > 0$

Example: $7 \equiv 3 \pmod 4$, $1 \equiv 9 \pmod 4 \Rightarrow 8 \equiv 12$, $6 \equiv -6$, $7 \equiv 27 \pmod 4$

****

Exercises:

$2006 \equiv$?? (mod 2), ?? (mod 3), ?? (mod 5), ?? (mod 10), ??

$-2006 \equiv$?? (mod 2), ?? (mod 3), ?? (mod 5), ?? (mod 10), ??

****

Q: What is the advantage of using modular arithmetic?
A: To work with smaller numbers.

Application #1: An integer > 0 is divisible by 3 if this integer's digit sum is divisible by 3.
Here is an illustration by using modular arithmetic.

$123456 = 1 \cdot 100000 + 2 \cdot 10000 + 3 \cdot 1000 + 4 \cdot 100 + 5 \cdot 10 + 6$
$\equiv 1 \cdot 1 + 2 \cdot 1 + 3 \cdot 1 + 4 \cdot 1 + 5 \cdot 1 + 6 \equiv 1 + 2 + 3 + 4 + 5 + 6 \pmod 3$

Therefore, 123456 is divisible by 3 $\Leftrightarrow$ $123456 \equiv 0 \pmod 3$
$\Leftrightarrow 1 + 2 + 3 + 4 + 5 + 6 \equiv 0 \pmod 3$ $\Leftrightarrow$ the digit sum of 123456 is divisible by 3

****

Exercise: Use the divisibility test to determine if 123456789 is divisible by 3.

****

Application #2: An integer > 0 is divisible by 9 if this integer's digit sum is divisible by 9.

Here is an illustration by using modular arithmetic.

$123453 = 1\cdot100000 + 2\cdot10000 + 3\cdot1000 + 4\cdot100 + 5\cdot10 + 3$
$\equiv 1\cdot1 + 2\cdot1 + 3\cdot1 + 4\cdot1 + 5\cdot1 + 3 \pmod 9 \equiv 1 + 2 + 3 + 4 + 5 + 3 \pmod 9$

Therefore, 123453 is divisible by 9 $\Leftrightarrow$ $123453 \equiv 0 \pmod 9$
$\Leftrightarrow 1 + 2 + 3 + 4 + 5 + 3 \equiv 0 \pmod 9$ $\Leftrightarrow$ the digit sum of 123453 is divisible by 9

****

Exercise: Use the divisibility test to determine if 123456789 is divisible by 9.

****

Application #3: An integer > 0 is divisible by 11 if the alternating sum of this integer's digits is divisible by 11.

$123453 = 1\cdot100000 + 2\cdot10000 + 3\cdot1000 + 4\cdot100 + 5\cdot10 + 3$
$\equiv 1\cdot10^5 + 2\cdot10^4 + 3\cdot10^3 + 4\cdot10^2 + 5\cdot10^1 + 3$
$\equiv 1(-1)^5 + 2(-1)^4 + 3(-1)^3 + 4(-1)^3 + 5(-1)^1 + 3 \pmod{11}$
$\equiv -1 + 2 - 3 + 4 - 5 + 3 \equiv 0 \pmod{11}$

****

Exercise: Use the divisibility test to determine if 123456789 is divisible by 11.

****

Application #4: If (a, b, c) is a Pythagorean triple, i.e., $a^2 + b^2 = c^2$, such that a, b, and c can not be divided by any integer greater than 1, then one of a and b must be odd and the other must be even. (Familiar Pythagorean triples: (3. 4. 5), (5, 12, 13), (7, 24, 25), (8, 15, 17))

It is much easer to see why a and b can't be both even – otherwise, c will also be even. This is imply that a, b, and c will all be divisible by 2, a contradiction.

Assuming that both a and b are odd. Then, $a \equiv 1, 3 \pmod 4$, $b \equiv 1, 3 \pmod 4$.
$\Rightarrow a^2 \equiv 1$, $b^2 \equiv 1 \pmod 4$ $\Rightarrow$ $c^2 = a^2 + b^2 \equiv 2 \pmod 4$.

However, $c \equiv 0, 1, 2, 3 \pmod 4 \Rightarrow c^2 \equiv 0, 1 \pmod 4$. $\rightarrow\leftarrow$

****

Exercise: Show that $(m^2 - n^2, 2mn, m^2 + n^2)$ is a Pythagorean triple for any $m, n > 0$. Find a Pythagorean triple (117, ___, ___).

****

Application #5: Does the equation $6a^2 - 5b = 3$ have any integer solutions?

No, because $6a^2 - 5b \equiv 6a^2 \pmod 5 \equiv a^2 \pmod 5 \equiv 0, 1, 4 \neq 3 \pmod 5$.

****

Exercise: Show that the equation $7a^2 - 3b = 2$ has no integer solutions.

****

Application #6: Finding the last few digits of an integer.

The last digit of $2006^3 \equiv 6^3 \equiv 6 \cdot 6 \cdot 6 \equiv 6 \pmod{10}$.
The last two digits of $923^4 \equiv 23^4 \equiv (23)^2(23)^2 \equiv (29)(29) \equiv 41 \pmod{100}$.
The last three digits of $1234998^{10} \equiv (-2)^{10} \equiv 2^{10} \equiv 1024 \equiv 24 \pmod{1000}$

****

Exercises:

- Find the last digit of 919^5.
- Find the last two digits of 2006^4.
- Find the last three digits of 959697^5.

****

Application #7: Finding the last few digits of large powers of integers.

The last digit: Note that $k^4 \equiv 1 \pmod{10}$ for all $k = 1, 3, 7, 9$.
Therefore, $923^{2006} \equiv 3^{2006} \equiv 3^{2004} \cdot 3^2 \equiv 1 \cdot 9 \equiv 9 \pmod{10}$.

The last two digits: Note that $k^{40} \equiv 1 \pmod{10}$ for all $1 \leq k \leq 99$ and $(k, 100) = 1$
Therefore, $923^{2006} \equiv 23^{2006} \equiv 23^{2000} \cdot 23^6 \equiv 1 \cdot 148035889 \equiv 89 \pmod{100}$

The last three digits: Note that $k^{400} \equiv 1 \pmod{10}$ for all $1 \leq k \leq 999$ and $(k, 1000) = 1$
Therefore, $923^{2006} \equiv 923^{2006} \equiv 923^{2000} \cdot 923^6 \equiv (-77)^6 \equiv 77^6 \equiv 208422380089 \equiv 89 \pmod{1000}$

****

Exercises:

- Find the last digit of 917^{50001}.
- Find the last two digits of 1234567^{50002}.
- Find the last three digits of 123456789^{50003}.

****