Modular Arithmetic, Grades 8 & 9

Blacksburg Math Circle

Warm-up Problem.
Let \( a_1 = 7 \) and \( a_2 = 11 \). We fix the divisor to be \( d = 5 \) in this problem.

(a) Compute the remainder \( r_1 \) of \( a_1 \). Compute the remainder \( r_2 \) of \( a_2 \) as well.
(b) Is the remainder of \( a_1 + a_2 \) equal to \( r_1 + r_2 \)?
(c) For other choices of \( a_1 \) and \( a_2 \), do you think the remainder of \( a_1 + a_2 \) is always equal to \( r_1 + r_2 \)? If not, can you find a relation between \( a_1 + a_2 \) and \( r_1 + r_2 \)?
(d) Is the remainder of \( a_1 a_2 \) equal to \( r_1 r_2 \)?
(e) For other choices of \( a_1 \) and \( a_2 \), do you think the remainder of \( a_1 a_2 \) is always equal to \( r_1 r_2 \)? If not, can you find a relation between \( a_1 a_2 \) and \( r_1 r_2 \)?

As you can see above, a dividend \( a \) and its remainder \( r \) when divided by a divisor \( d \) behave in the same way when you carry out basic arithmetic operations like addition and multiplication (subtraction is also fine) followed by taking a remainder, which is called “modular arithmetic.” Modular arithmetic may seem to be unusual, but it turns out that people use it on a daily basis. (Do you see how? Hint: \( d = 12 \).)

The fact that \( a = 7 \) and \( r = 2 \) behave in the same way in modular arithmetic with \( d = 5 \) is denoted as \( 7 \equiv 2 \pmod{5} \) and pronounced as “7 is congruent to 2 modulo 5” where \( d = 5 \) is called a modulus. In general, we write

\[
a \equiv b \pmod{d}
\]

if \( a - b \) is divisible by \( d \) (i.e. \( a - b \) is an integer multiple of \( d \)). You are not restricted to have a remainder on the right or use positive numbers. The statement \( 7 \equiv -3 \pmod{5} \) is true because \( 7 - (-3) = 10 \) is divisible by 5.

In the following problems, you will discover some properties and uses of modular arithmetic. Enjoy!

**Problem 1.**
What is the remainder of \( 2^{50} \pmod{5} \)? How about \( 3^{2016} \pmod{7} \)?

**Problem 2.**
Find a positive integer \( n \) such that \( x \equiv 2 \pmod{3} \) and \( x \equiv 3 \pmod{4} \). Can you list all such positive integers less than 50?

**Problem 3.**
Find a positive integer \( n \) such that \( x \equiv 1 \pmod{4} \), \( x \equiv 3 \pmod{5} \), and \( x \equiv 3 \pmod{7} \).

**Problem 4.**
Let \( d_1 = 3 \) and \( d_2 = 5 \). Let \( n \) be an integer that has the same remainder \( r \) mod \( d_1 \) and \( d_2 \).
(a) For \( n = 16 \) (what is \( r \)?), compute the remainder of \( n \pmod{d_1 d_2} \).
(b) For \( n = 32 \) (what is \( r \)?), compute the remainder of \( n \pmod{d_1 d_2} \).
(c) Based on your observations, formulate a conjecture.
(d) Prove your conjecture.
(e) Do you think your conjecture holds for other choices of \(d_1\) and \(d_2\) (e.g. \(d_1 = 4\) and \(d_2 = 6\))? Can you identify a condition on \(d_1\) and \(d_2\) for your conjecture to be true?

**Problem 5.**
Let \(n\) be an integer that is not divisible by 3.
(a) For \(n = 4\), compute the remainder of \(n^2 - 1 \pmod{3}\).
(b) For \(n = 10\), compute the remainder of \(n^2 - 1 \pmod{3}\).
(c) Try a few more examples. Based on your observations, formulate a conjecture.
(d) Prove your conjecture.

**Problem 6.**
Let \(n\) be an odd integer.
(a) For \(n = 3\), compute the remainder of \(n^2 \pmod{8}\).
(b) For \(n = 13\), compute the remainder of \(n^2 \pmod{8}\).
(c) Try a few more examples. Based on your observations, formulate a conjecture.
(d) Prove your conjecture.

*Problem 7.
Let \(n\) be an odd integer.
(a) For \(n = 3\), compute the remainder of \(n(n + 2) \pmod{16}\).
(b) For \(n = 13\), compute the remainder of \(n(n + 2) \pmod{16}\).
(c) Try a few more examples. Based on your observations, formulate a conjecture.
(d) Prove your conjecture.

**Problem 8.**
Let \(n\) be an odd integer.
(a) For \(n = 5\), compute the remainder of \(1 + 2 + \cdots + n \pmod{n}\).
(b) For \(n = 7\), compute the remainder of \(1 + 2 + \cdots + n \pmod{n}\).
(c) What is your conjecture?
(d) Prove your conjecture.

**Problem 9.**
Let \(n\) be an even integer.
(a) For \(n = 4\), compute the remainder of \(1 + 2 + \cdots + n \pmod{n}\).
(b) For \(n = 6\), compute the remainder of \(1 + 2 + \cdots + n \pmod{n}\).
(c) What is your conjecture?
(d) Prove your conjecture.