Modular Arithmetic

Notes

You can think of arithmetic mod n as working on a clock with ______________.
For any numbers a and n, $a \mod n$ is ____________________________.

To find the mod n multiplicative inverse, we look for the number a^{-1} between 1 and $n-1$ such that _______________________.

In symbols, the addition property of modular arithmetic is

In symbols, the multiplication property of modular arithmetic is

The above properties mean that when you are doing modular arithmetic you can reduce mod n either before or after you perform the operations!

Reducing Modulo n

1. Reduce each of the following.

   (a) $13 \mod 7 \equiv$ _______
   (b) $16 \mod 4 \equiv$ _______
   (c) $-12 \mod 9 \equiv$ _______
   (d) $32 \mod 28 \equiv$ _______
   (e) $50000 \mod 2 \equiv$ _______
   (f) $765 \mod 2 \equiv$ _______
   (g) $39 \mod 12 \equiv$ _______
   (h) $-8 \mod 3 \equiv$ _______
   (i) $55 \mod 11 \equiv$ _______

2. Circle any of the letters from question 1 where the given number was divisible by the modulus. What do you notice about these problems? Explain why this makes sense.

   ____
   ____
   ____

Modular Arithmetic

1. Compute the following.

   (a) $3 + 6 \mod 7 \equiv$ ______
   (b) $3 - 6 \mod 7 \equiv$ ______
   (c) $15 + 4 \mod 9 \equiv$ ______
   (d) $5 - 22 \mod 28 \equiv$ ______
   (e) $12 \cdot 3 \mod 2 \equiv$ ______
   (f) $5 \cdot 2 \mod 12 \equiv$ ______
   (g) $77 \cdot 75 \mod 76 \equiv$ ______
   (h) $2345678 \cdot 8765432 \mod 2 \equiv$ ______
   (i) $3 + 16 - 21 \mod 7 \equiv$ ______
   (j) $5 + 9 + 7 + 6 + 4 + 30 + 13 \mod 3 \equiv$ ______
   (k) $5 \cdot (77 - 301 + 4567) \mod 5 \equiv$ ______
   (l) $7 \cdot 3 \cdot 5 \mod 10 \equiv$ ______
   (m) $2^4 \mod 3 \equiv$ ______
   (n) $3^3 \mod 25 \equiv$ ______
   (o) $9^{10} \mod 8 \equiv$ ______
   (p) $3^{-1} \mod 7 \equiv$ ______
   (q) $7^{-1} \mod 9 \equiv$ ______
   (r) $7 \div 4 \mod 11 \equiv$ ______
   (s) $8 \div 4 \mod 15 \equiv$ ______

2. Fill in the "Number 1", "Number 2", and "Modulus" blanks below to create your own modular equations. Then fill in the "Answer" blank to complete the equation. If you're doing this with a friend, feel free to make up questions for each other!

   (a) ________ $+$ ________ $\equiv$ ________ mod ________
   (b) ________ $-$ ________ $\equiv$ ________ mod ________
   (c) ________ $\cdot$ ________ $\equiv$ ________ mod ________

3. Show that 6 does not have a multiplicative inverse mod 8 by checking all possibilities.

4. (Challenge problem) Try to come up with a general rule for when a number a does not have a multiplicative inverse mod n.