

1. More definitions

Modulus

“In computing, the modulo operation finds the remainder after division of one number by another (sometimes called modulus).

Given two positive numbers, a (the dividend) and n (the divisor), $a \bmod n$ (abbreviated as $a \bmod n$) is the remainder of the Euclidean division of a by n .”^a

$$\begin{array}{r} 4r1 \\ 2 \overline{)9} \\ \underline{-8} \\ 1 \end{array}$$

$$9 \bmod 2 = 1$$

If we're dividing a by b , the result is a quotient q . If we're calculating $a \bmod b$, the result is the remainder r .

We can also write this out as:

$a = b \cdot q + r$, where $0 \leq r < b$, and q and r are the only two integers that will satisfy the equation.

^aFrom https://en.wikipedia.org/wiki/Modulo_operation

Rational numbers

In mathematics, a rational number is any number that can be expressed as the quotient or fraction p/q of two integers, a numerator p and a non-zero denominator q .^[1] Since q may be equal to 1, every integer is a rational number.^a

The set of rational numbers is written as \mathbb{Q} .

^aFrom https://en.wikipedia.org/wiki/Rational_number

Question 1

Prove the following

Example: Solve $13 \bmod 5$

$$13 / 5 = 2, \quad 13 \bmod 5 = 3, \quad 13 = 5 \cdot 2 + 3$$

- a. $9 \bmod 7$ $(13 = 15 \cdot q + r...)$
 - b. $5 \bmod 2$
 - c. $15 \bmod 3$
 - d. $-7 \bmod 2$
-

Question 2

Prove the following propositions:

- a. If a divides b and a divides c , then a divides $b + c$.¹

Start with: $b = ak$ and $c = aj$ and calculate $b + c$.

- b. If a divides b and c divides d , then ac divides bd .²

Start with: $b = ak, d = cj$ and calculate bd .

¹From Discrete Mathematics by Ensley and Crawley

²From Discrete Mathematics by Ensley and Crawley