

CS 135

Introduction to Modular Arithmetic

Professor Bloom

February 10, 2009

1 The arithmetic operations

The **arithmetic operations** on \mathbb{N} are the familiar $x + y$, $x \times y$, $x - y$, x/y . Wait, (you say), $2 - 5$ is not a member of \mathbb{N} . Right. $2/5$ isn't either. So what do you mean (you ask) by including subtraction and division?

We admit that subtraction and division when restricted to \mathbb{N} are only PARTIAL functions, i.e., for certain arguments they are not defined.

Except that we have used the notation x/y for “integer division”, the largest integer q such that $y \times q \leq x$. Thus, if $q = x/y$,

$$\begin{aligned}q \times y &\leq x \\(q + 1) \times y &> x.\end{aligned}$$

Exercise. What is an analogous way to define “integer subtraction”?

1.1 Modular arithmetic

Remember the **fundamental theorem of division**: if $n, m > 0$ are integers, then there are unique integers q, r such that

$$\begin{aligned}n &= qm + r \quad \text{and} \\0 &\leq r < m.\end{aligned}$$

r is $n \bmod m$ and q is (quotient n m).

If $r = 0$, we say m **divides** n and write $m|n$.

Let

$$\mathbb{Z}_m = \{0, 1, \dots, m - 1\}$$

be the “integers mod m ”. On \mathbb{Z}_m we have at least three of the arithmetic operations totally defined.

addition For $x, y \in \mathbb{Z}_m$, we **define**

$$x +_m y := (x + y) \bmod m.$$

For example, $2 +_5 4 = 1$.

multiplication For $x, y \in \mathbb{Z}_m$, we **define**

$$x \times_m y := (x \times y) \bmod m.$$

For example, $2 \times_5 4 = 3$.

unary minus For $x \in \mathbb{Z}_m$, we **define** $-_m x$ as that unique $y \in \mathbb{Z}_m$ such that $x +_m y = 0$. In fact,

$$-_m x = \begin{cases} 0 & \text{if } x = 0 \\ m - x & \text{otherwise.} \end{cases}$$

subtraction For $x, y \in \mathbb{Z}_m$, we **define** $x -_m y$ as $x +_m (-_m y)$. For example, $2 -_5 4 = 3$. Thus, $x -_m y = z$ iff $x = y +_m z$.

What properties do these operations have? *Answer, in brief.* The same properties that the corresponding operations on the integers have. For example,

$$\begin{aligned} x +_m y &= y +_m x \\ (x +_m y) +_m z &= x +_m (y +_m z) \\ x +_m 0 &= x \\ x \times_m y &= y \times_m x \\ (x \times_m y) \times_m z &= x \times_m (y \times_m z) \\ x \times_m 1 &= x \\ x \times_m (y +_m z) &= (x \times_m y) +_m (x \times_m z). \end{aligned}$$

Notation

From now on, we *do not use the subscript m on the mod m arithmetic operations.*

1.2 Division

How about division? The answer depends on m . For example, we would like division mod m to satisfy the following property.

$$x/y = z \iff x = yz,$$

where all operations are mod m . Now, modulo 5, for example, we have a total division operation on the nonzero elements. Thus, $x/1 = x$, for all $1 \leq x < m$, since $1 \times x = x$, and $x/x = 1$, for the same reason.

Example: for $m = 5$:

Division mod 5.

x	y	x/y
1	2	3
2	2	1
2	3	4
2	4	3
3	2	4
3	3	1
3	4	2
4	2	2
4	3	3
4	4	1

But, for $m = 4$, division is only partial.

Division mod r

x	y	x/y
1	2	?
2	2	1
2	3	2
3	2	?
3	3	1

Why the question marks? There is no $x \in \mathbb{N}_4$ such that $2x \equiv 1 \pmod{4}$; and there is no x such that $2x \equiv 3 \pmod{4}$. Indeed, $2 \times 2 = 0$, $2 \times 1 = 2 \times 3 = 2$.

How can we understand these two cases?

2 Exercises

For each of the true/false questions, explain your answer. If false, provide a counter example; if true, give an argument for why it is true.

1. For integers a, b , **write $a|b$ if a divides b , i.e., if $b = qa$, for some integer q .** Prove: if $a|b$ and $a|c$, then $a|(b + c)$ and $a|(b - c)$.
2. True or false. If $a|(b + c)$ then $a|b$ and $a|c$.
3. True or false. If $a|b$ then $a|bc$, for all integers c .
4. True or false. If $a|b$ and $b|c$ then $a|c$.
5. True or false. If $a|b$ and $b|a$ then $a = b$.
6. True or false. If $a, b, c \geq 0$ and $a|b$ and $b|a$ then $a = b$.
7. For which integers a is the following true? $a|0$.
8. For which integers a is the following true? $0|a$.
9. For which integers a is the following true? $a|1$.
10. For which integers a is the following true? $1|a$.
11. Suppose a, b are nonnegative. Show that there is an integer c with the following properties.
 - $a|c$ and $b|c$
 - if $d > 0$ is any integer such that $a|d$ and $b|d$ then $c|d$.Give a description of c in the case that $a = 2$ and $b = 3$.
12. Suppose a, b are nonnegative. Show that there is an integer c with the following properties.
 - $c|a$ and $c|b$
 - if $d > 0$ is any integer such that $d|a$ and $d|b$ then $d|c$.Give a description of c in the case that $a = 2$ and $b = 3$.