Teoria dos números e corpos finitos

Lucas João Martins

1. (4.6) For each of the following equations, find an integer x that satisfies the equation.

a. $5x \equiv 4 \pmod{3}$

$x = 2$
$5 \times 2 = 10$
$10 - 4 = 6 = 3 \times 2$

b. $7x \equiv 6 \pmod{5}$

$x = 3$
$7 \times 3 = 21$
$21 - 6 = 15 = 5 \times 3$

c. $9x \equiv 8 \pmod{7}$

$x = 4$
$9 \times 4 = 36$
$36 - 8 = 28 = 7 \times 4$

2. (4.7) In this text, we assume that the modulus is a positive integer. But the definition of the expression $a \mod n$ also makes perfect sense if n is negative. Determine the following:

Usando $a \mod n = a - \lfloor a/n \rfloor \times n$.

a. $5 \mod 3$

2

b. $5 \mod -3$

$$
\begin{aligned}
&5 - \lfloor 5/-3 \rfloor \times -3 \\
&5 - (-2 \times -3) \\
&5 - 6 \\
&-1
\end{aligned}
$$

c. $-5 \mod 3$

$$
\begin{aligned}
&-5 - \lfloor -5/3 \rfloor \times 3 \\
&-5 - (-2 \times 3) \\
&-5 + 6 \\
&1
\end{aligned}
$$

d. $-5 \mod -3$

$$
\begin{aligned}
&-5 - \lfloor -5/-3 \rfloor \times -3 \\
&-5 - (1 \times -3) \\
&-5 + 3 \\
&-2
\end{aligned}
$$

3. (4.8) A modulus of 0 does not fit the definition but is defined by convention as follows: $a \mod 0 = a$. With this definition in mind, what does the following expression mean: $a \equiv b \pmod 0$?

Significa que a e b são iguais.

4. (4.1) For the group S_n of all permutations of n distinct symbols:

a. what is the number of elements in S_n?

$n!$

b. show that S_n is not abelian for $n > 2$.

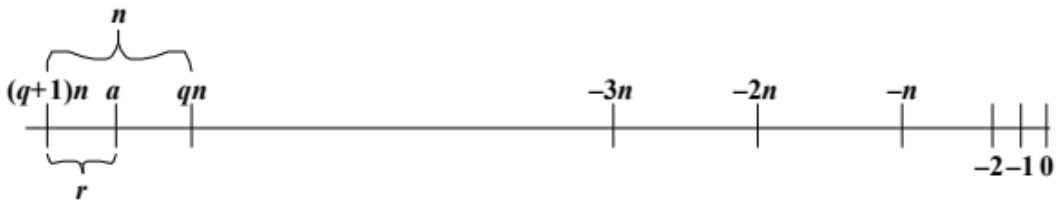
Um contra exemplo com o S_3 seria:

$$\{3,2,1\} \cdot \{1,3,2\} = \{2,3,1\}$$
$$\{1,3,2\} \cdot \{3,2,1\} = \{3,1,2\}$$

5. (4.4) Reformulate Equation (4.1), removing the restriction that a is a nonnegative integer. That is, let a be any integer.

A equação continua a mesma.

6. (4.5) Draw a figure similar to Figure 4.1 for $a < 0$.



7. (4.13) Find the multiplicative inverse of each nonzero element in Z_5.

Para todo $a \in Z_5$, precisamos encontrar um $b \in Z_5$ onde $ab \equiv 1 \pmod 5$

$1 \to 1$
$2 \to 3$
$3 \to 2$
$4 \to 4$

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

×	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

w	$-w$	w^{-1}
0	0	—
1	4	1
2	3	3
3	2	2
4	1	4

8. (4.20) Develop a set of tables similar to Table 4.3 for GF(5).

9. (4.10) What is the smallest positive integer that has exactly k divisors, for $1 \leq k \leq 6$?

$k = 1 \rightarrow 1 \rightarrow \{1\}$
$k = 2 \rightarrow 2 \rightarrow \{1, 2\}$
$k = 3 \rightarrow 4 \rightarrow \{1, 2, 4\}$
$k = 4 \rightarrow 6 \rightarrow \{1, 2, 3, 6\}$
$k = 5 \rightarrow 16 \rightarrow \{1, 2, 4, 8, 16\}$
$k = 6 \rightarrow 12 \rightarrow \{1, 2, 3, 4, 6, 12\}$

10. (4.2) Does the set of residue classes (mod 3) form a group

Considere as seguintes tabelas de multiplicação e adição para responder as perguntas:

Tabela 1: Adição

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

Tabela 2: Multiplicação

x	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

a. with respect to modular addition?

Sim, o elemento identidade é 0 e a inversa de 0, 1, 2 são respectivamente 0, 2, 1.

b. with respect to modular multiplication?

Não, o elemento identidade é 1, mas 0 não possui inversa.

11. (4.3) Consider the set $S = \{a, b\}$ with addition and multiplication defined by the following tables. Is S a ring? Justify your answer.

+	a	b
a	a	b
b	b	a

×	a	b
a	a	a
b	a	b

S é um anel por causa dos seguintes motivos:

- a soma de qualquer dois elementos em S resulta em um elemento também em S
- ele é associativo sobre a adição
- a é a identidade da adição
- a inversa aditiva de a e b são b e a respectivamente
- ele é comutativo sobre a adição
- o produto de qualquer dois elementos em S resulta em um elemento também em S

- ele é associativo sobre o produto
- ele é distributivo sobre as duas operações

12. (4.11) Prove the following:

a. $a \equiv b \pmod{n}$ **implies** $b \equiv a \pmod{n}$

13. (4.12)

14. (4.9)

15. (4.14)

16. (4.27)

17. (4.28)

18. (4.23)

19. (4.22)

20. (4.19)