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 $n > 2$.

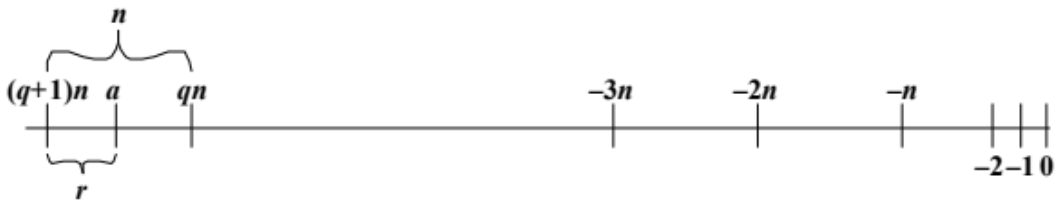
Um contra exemplo com o S_3 seria:

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

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

Essa é a definição de congruência apresentada no livro.

b. $a \equiv b \pmod{n}$ **and** $b \equiv c \pmod{n}$ **imply** $a \equiv c \pmod{n}$

As duas primeiras significam:

$$a - b = nk$$
$$b - c = nm$$

Então substituindo:

$$a - c = (a - b) + (b - c) = n(k + m)$$

13. (4.12) Prove the following:

a. $[(a \bmod n) - (b \bmod n)] \bmod n \equiv (a - b) \bmod n$

Considere o seguinte:

$$c = a \bmod n$$
$$d = b \bmod n$$

Então:

$$c = a + kn$$
$$d = b + mn$$
$$c - d = (a - b) + (k - m) \times n$$
$$(c - d) = (a - b) \bmod n$$

b. $[(a \bmod n) \times (b \bmod n)] \bmod n \equiv (a \times b) \bmod n$

Com as definições de c e d da alternativa anterior:

$$cd = ab + n \times (kb + ma + kmn)$$
$$cd = (a \times b) \bmod n$$

14. (4.9) In Section 4.3, we define the congruence relationship as follows: Two integers a and b are said to be congruent modulo n if $(a \mod n) = (b \mod n)$. We then proved that $a \equiv b (mod\ n)$ if $n|(a-b)$. Some texts on number theory use this latter relationship as the definition of congruence: Two integers a and b are said to be congruent modulo n if $n|(a-b)$. Using this latter definition as the starting point, prove that, if $(a \mod n) = (b \mod n)$, then n divides $(a-b)$.

Qualquer inteiro a pode ser escrito como $a = qn + r$ onde q é algum inteiro e r é um número entre $0, 1, 2, \ldots, n-1$. Usando a segunda definição, não há dois restos na lista citada que são congruente módulo n, porque a diferença entre eles é menor que n e portando n não divide essa diferença. Portando, esses dois números devem ter restos diferentes. Então é possível concluir que n divide $(a-b)$ se e somente se a e b são números que possuem o mesmo resto quando dividido por n.

15. (4.14) Show that an integer N is congruent modulo 9 to the sum of its decimal digits. For example, $475 \equiv 4+7+5 \equiv 16 \equiv 1+6 \equiv 7 \pmod 9$. This is the basis for the familiar procedure of "casting out 9's" when checking computations in arithmetic

Temos:

$1 \equiv 1 (mod\ 9)$
$10 \equiv 1 (mod\ 9)$
$10^2 \equiv 10(10) \equiv 1(1) (mod\ 9)$
$10^{n-1} \equiv 1 (mod\ 9)$

Se escrever $N = a_0 + a_1 10^1 + \cdots + a_{n-1} 10^{n-1}$. Então $N \equiv a_0 + a_1 + \cdots + a_{n-1} (mod\ 9)$.

16. (4.27) Determine the multiplicative inverse of $x^3 + x + 1$ in GF(2^4) with $m(x) = x^4 + x + 1$.

$x^2 + 1$

Power REP	Polynomial REP	Binary REP	Decimal (Hex) RPEP
0	0	0000	0
g^0	1	0001	1
g^1	g	0010	2
g^2	g^2	0100	4
g^3	g^3	1000	8
g^4	$g+1$	0011	3
g^5	g^2+g	0110	6
g^6	g^3+g^2	1100	12
g^7	g^3+g+1	1011	11
g^8	g^2+1	0101	5
g^9	g^3+g	1010	10
g^{10}	g^2+g+1	0111	7
g^{11}	g^3+g^2+1	1110	14
g^{12}	g^3+g^2+g+1	1111	15
g^{13}	g^3+g^2+1	1101	13
g^{14}	g^3+1	1001	9

17. (4.28) Develop a table similar to Table 4.9 for GF(2^4) with $m(x) = x^4 + x + 1$.

18. (4.23) For polynomial arithmetic with coefficients in Z_{10}, perform the following calculations.

a. $(7x + 2) - (x^2 + 5)$:

$9x^2 + 7x + 7$

a. $(6x^2 + x + 3) \times (5x^2 + 2)$:

$5x^3 + 7x^2 + 2x + 6$

19. (4.22) Demonstrate whether each of these statements is true or false for polynomials over a field.

a. The product of monic polynomials is monic.

True. O único termo que não é zero no resultado terá valor igual a 1.

b. The product of polynomials of degrees m and n has degree $m + n$.

True. Temos $c_{n+m} = a_n b_m \neq 0$.

c. The sum of polynomials of degrees m and n has degree $max[m, n]$.

True quando $m \neq n$, mas false no geral quando $m = n$, por causa que os coeficientes com maiores graus podem se cancelar.

20. (4.19) Using the extended Euclidean algorithm, find the multiplicative inverse of

a. 1234 *mod* 4321**:**

1234

b. 1234 *mod* 4321**:**

$gcd(40902, 24240) = 34 \neq 1$.

c. 550 *mod* 1769**:**

550