Modelagem Matemática no Ensino

Aula 06

1. Criptografia e Codificação
2. Atividade: Sistema Binário
3. Trabalho 01 - Entrega: 19/08

Profa. Karla Lima
FACET/UFGD

1 Criptografia e Codificação

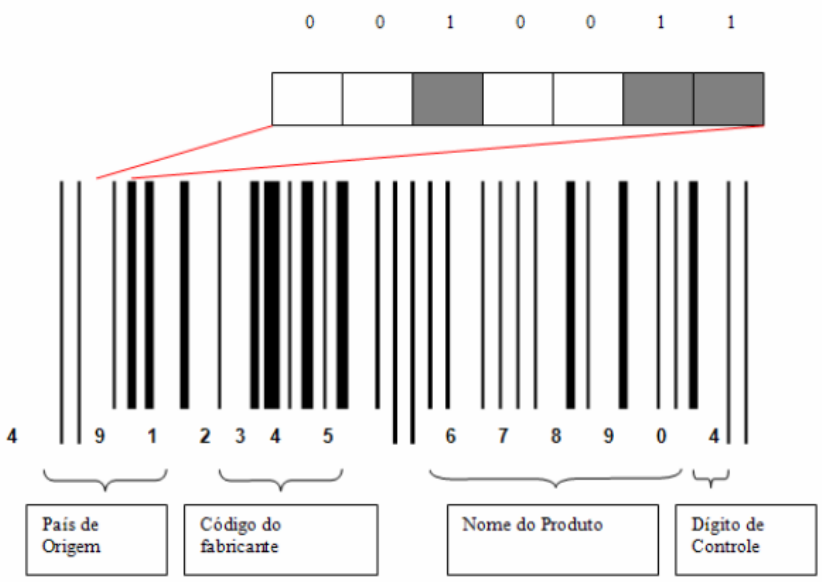
- Para codificarmos ou decodificarmos uma mensagem necessitamos de informações confidenciais denominadas chave.
- A criptoanálise estuda formas de decodificar uma mensagem sem se conhecer, de antemão, a chave. Ela reconstrói, a partir da mensagem codificada, a mensagem no seu formato original, com a ajuda de métodos matemáticos.
- Dizemos que a criptoanálise é responsável por quebrar o código da mensagem codificada, o que permite transformar dados ou mensagens em alguma forma legível.
- A criptografia, por outro lado, é utilizada para proteger informações e manter o sigilo de dados confidenciais.
- A criptografia utiliza métodos para a produção e distribuição segura de chaves e estuda algoritmos que permitem transformar mensagens claras em formas de comunicação só inteligíveis pelos emissores e pelos receptores envolvidos no processo.

  - **Criptograma:** Mensagem cujo conteúdo foi obtido a partir de uma técnica de criptografia.
  - **Ciframento:** Técnica de criptografia para obter um criptograma a partir de uma mensagem.
  - **Deciframento:** Técnica de criptografia para obter a mensagem original a partir de uma criptograma.

- Na ciência da criptografia estudam-se os códigos e as cifras.
- No estudo de códigos em geral não há a intenção de se esconder a informação, como, por exemplo, nos códigos de barra, hoje em dia amplamente utilizados.

1.1 Código de Barras

- Ultimamente todos os produtos vendidos em supermercados são identificados com códigos de barras, formados por uma sequência alternada de linhas brancas e pretas.
- Nestas barras estão contidas informações sobre o fabricante, preço e origem.



- A vantagem das barras é que elas podem ser identificadas rapidamente, e sem risco de erros, por aparelhos portáteis de leitura óptica, como os usados pelos caixas de supermercado.
- Mas o que realmente importa para identificar o produto é sua sequência numérica, que também pode ser digitada manualmente pelos caixas. Esse

número funciona como uma espécie de RG do produto, ou seja, não existem dois produtos diferentes com o mesmo número.

- As barras pretas e brancas são convertidas, por meio de uma leitora ótica, em dígitos **binários** que podem ser entendidos pelo computador.
- A linha preta corresponde ao binário 1 e a linha branca ao binário 0.
- Cada grupo de sete linhas representa um número que aparece imediatamente abaixo do código, mas não é em geral a representação binária deste número.
- As barras mais compridas têm a função apenas de separar as demais e as listras brancas e pretas que aparecem alternadamente podem ser de oito tipos: fina branca (0), média branca (00), grossa branca (000), muito grossa branca (0000), fina preta (1), média preta (11), grossa preta (111) e muito grossa preta (1111).

1.2 CPF: Cadastro de Pessoa Física

O cadastro das pessoas físicas tem o seguinte formato:

$$X_1\,X_2\,X_3\,X_4\,X_5\,X_6\,X_7\,X_8\,R - C_1\,C_2$$

- Os oito primeiros números constituem o número básico de inscrição da pessoa física no Cadastro Individual do Contribuinte.
- O nono algarismo, indicado pela letra R, indica a região fiscal onde foi efetuada a inscrição.
- O dígito C_1 é um número verificador do número formado pelos nove algarismos anteriores (calculado tomando o resto por 11).
- C_2 é o dígito de controle que verifica a exatidão dos dez algarismos anteriores (usando também o resto por 11).

Cálculo de C_1:

Figura 1: fonte

- Cada um dos nove algarismos, a partir da direita, é multiplicado sucessivamente por $2, 3, 4, 5, 6, 7, 8, 9, 10$ e os produtos resultantes são somados.
- A soma obtida é então dividida por 11 e C_1 será o quanto falta para 11 do resto desta divisão.
- Se este complemento for maior ou igual a 10, toma- se o valor 0.
- Colocamos o valor encontrado de C_1 na sua devida posição para iniciar o cálculo de C_2 .

Cálculo de C_2:

- Cada um dos dez algarismos, a partir da direita, é multiplicado sucessivamente por $2, 3, 4, 5, 6, 7, 8, 9, 10, 11$ e os produtos resultantes são somados.

- A soma obtida é então dividida por 11 e C_2 será o quanto falta para 11 do resto desta divisão.
- Se este complemento for maior ou igual a 10, toma- se o valor 0.

Exercício 1 *Crie um CPF, detalhando a escolha da região fiscal e a obtenção dos dígitos de controle.*

2 Atividade: Sistema Binário

Apresenta-se os 5 calendários abaixo e pede-se que alguém indique em quais dos calendários a data de seu nascimento aparece sublinhada.

Um sim um não

dom	seg	ter	qua	qui	sex	sab
			1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30	31	

De dois em dois

dom	seg	ter	qua	qui	sex	sab
			1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30	31	

De quatro em quatro

dom	seg	ter	qua	qui	sex	sab
			1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30	31	

De oito em oito

dom	seg	ter	qua	qui	sex	sab
			1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30	31	

Meio mês sim meio não

dom	seg	ter	qua	qui	sex	sab
			1	2	3	4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30	31	

Figura 2: fonte

- Os primeiros dias grifados, nos cinco calendários, são as cinco primeiras potências de 2: $2^0 = 1, 2^1 = 2, 2^2 = 4, 2^3 = 8$ e $2^4 = 16$.
- Cada inteiro positivo pode ser expressado, de uma única maneiro, como uma potência de 2 ou como soma de potências de 2 distintas entre si.

Exercício 2 *Verifique cada uma das afirmações a seguir:*

a) *Cada número de* 1 *a* 31 *pode ser escrito com as potências de* 2 *citadas acima.*

b) *No primeiro calendário, os números sublinhados são representados por somas de potências de* 2 *em que o número* $1 = 2^0$ *participa.*

c) *O segundo calendário mostra grifados os números expressados por tais somas em que o número* 2 *participa.*

d) *O terceiro calendário mostra, grifados, os números expressados por somas tendo a participação da potência* 2^2.

e) *O quarto calendário mostra, grifados, os números expressados por somas tendo a participação da potência* 2^3.

f) *Por fim, no quinto calendário, os números sublinhados são representados por somas de potências de* 2 *em que o número* 2^4 *participa.*

Exercício 3 *Com as afirmações acima, porque devemos somar o primeiro número grifado de cada calendário indicado pelo participante, a fim de adivinhar o dia em que ele nasceu?*

3 Trabalho 01 - Entrega: 19/08

Vamos utilizar cartões perfurados para trabalhar com números de 0 a 31, utilizando-se a base 2. Esses números podem ser escritos com apenas 5 dígitos, como visto no Exercício 2.

Cada buraco representará o número 1 e cada fenda o número 0.

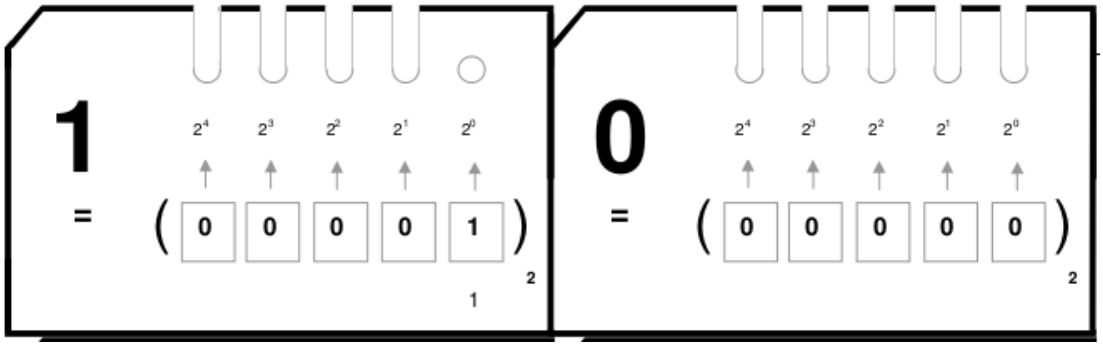


Figura 3: fonte

Faça um maço com as cartas. Se você colocar um palito (ou um canudo ou um clipe) por alguns dos buracos do maço, e levantá-lo, algumas cartas cairão e outras ficarão presas no palito. Repetindo organizadamente este procedimento você poderá realizar várias operações com os números binários de 0 a 31.

3.1 Atividade do dia 05/08

Descreva uma maneira de:

1. Separar as cartas pares das ímpares.
2. Colocar as cartas em ordem crescente, depois de embaralhadas.
3. Localizar qualquer número de 0 a 31 com a colocação do palito e levantamento do maço 5 vezes.

Justifique os passos dados em cada truque.

3.2 Atividade do dia 12/08

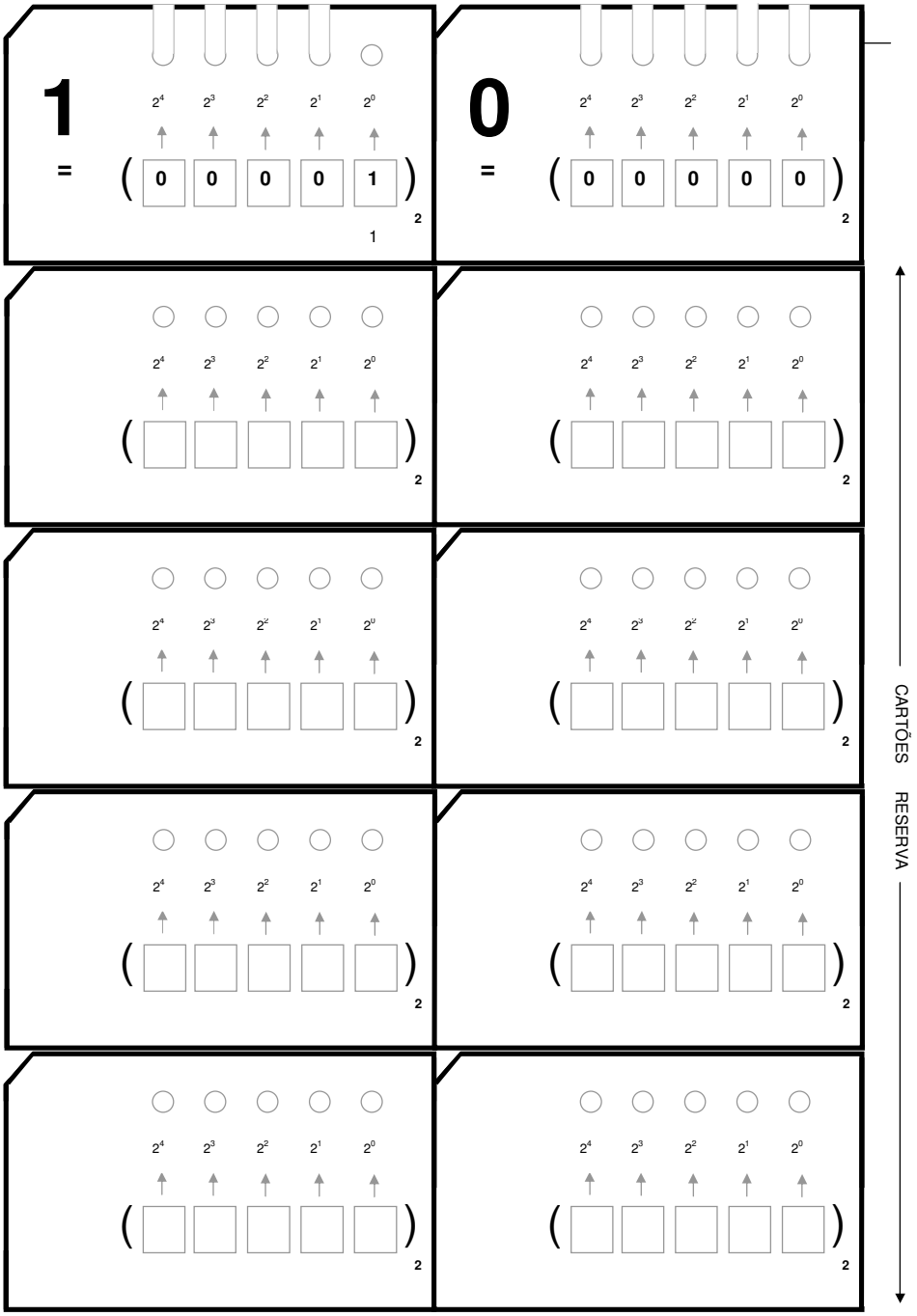
1. Construção dos material.

2. Discussão sobre as soluções encontradas no dia 05/08.

3.3 Atividade do dia 19/08

1. Entrega do relatório de atividades, disponibilizado no dia 12/08.

2. Aula Normal.


1
=
0
=
CARTÕES
RESERVA