UNIVERSIDADE FEDERAL DO RIO DE JANEIRO

MESTRADO PROFISSIONAL EM MATEMÁTICA EM REDE NACIONAL - PROFMAT

Criptografia Kid-RSA adaptada: uma abordagem didática no estudo das operações de multiplicação e divisão

RENATA SANTOS LOPES CEREJA

RIO DE JANEIRO - RJ

Agosto de 2018

PROFMAT

RENATA SANTOS LOPES CEREJA

Criptografia Kid-RSA adaptada: uma abordagem didática no estudo das operações de multiplicação e divisão

Dissertação submetida ao Curso de Pós-graduação stricto sensu de Mestrado Profissional em Matemática em Rede Nacional (PROFMAT) para aprimoramento da formação profissional de professores da educação básica, pela Universidade Federal do Rio de Janeiro, como requisito parcial à obtenção do Grau de Mestre.

Orientadora: Prof.ª Dr.ª Maria Aguireiras Alvarez de Freitas.

Rio de Janeiro – RJ

2018

CIP - Catalogação na Publicação

C414c

Cereja, Renata Santos Lopes
Criptografia Kid-RSA adaptada: uma abordagem didática no estudo das operações de multiplicação e divisão / Renata Santos Lopes Cereja. -- Rio de Janeiro, 2018.
84 f.

Orientadora: Maria Aguireiras Alvarez de Freitas.
Dissertação (mestrado) - Universidade Federal do Rio de Janeiro, Instituto de Matemática, Programa de Pós-Graduação em Ensino de Matemática, 2018.

1. Criptografia. 2. Multiplicação. 3. Divisão. 4. Ensino Fundamental. 5. kid-RSA adaptada. I. Freitas, Maria Aguireiras Alvarez de, orient. II. Título.

Elaborado pelo Sistema de Geração Automática da UFRJ com os dados fornecidos pelo(a) autor(a).

Renata Santos Lopes Cereja

Criptografia Kid-RSA adaptada: uma abordagem didática no estudo das operações de multiplicação e divisão

Dissertação submetida ao corpo docente do Programa de Mestrado Profissional em Matemática em Rede Nacional – PROFMAT da Universidade Federal do Rio de Janeiro como parte dos requisitos necessários para obtenção do grau de Mestre em Matemática.

Aprovada em 30/08/2018

Maria Aguieiras Alvarez de Freitas, D.Sc.
Instituto de Matemática – UFRJ

Marisa Beatriz Bezerra Leal, D.Sc.
Instituto de Matemática – UFRJ

Renata Raposo Del-Vecchio, D.Sc.
Instituto de Matemática e Estatística - UFF

AGRADECIMENTOS

Agradeço a Deus por conseguir chegar até aqui, pois ele colocou anjos na minha vida que me ajudaram durante todo percurso do mestrado.

Aos meus pais, que sempre me incentivaram a estudar e alçar voos mais altos, que sempre acreditaram no meu potencial desde pequena e investiram para que eu tivesse o melhor estudo.

Ao meu noivo, que, assim como meus pais, vivenciou todo o processo, desde a prova de seleção até este momento, escutando todas as minhas preocupações e dizendo que eu daria conta de tudo.

Agradeço à Viviana e à Vanessa, diretoras das escolas em que apliquei a atividade relatada neste trabalho. Agradeço também a toda à equipe de coordenação de ambas as escolas. Sem a parceria que encontro nessas escolas, nada disto seria possível. Agradeço também à Michele, funcionária e amiga da escola municipal que trabalho, por sempre se preocupar em saber se estava dando tudo certo e ficar sempre na torcida positiva.

Ao Professor Dr. Coutinho (Collier), por ter me apresentado ao mundo da criptografia quando ainda estava na graduação e por ter plantado a semente de que era possível apresentar a criptografia em sala de aula, me indicando um autor, cujo artigo inspirou parte deste trabalho.

Agradeço à minha orientadora, por me ajudar na parte mais difícil para mim deste mestrado.

Por fim, agradeço a todos que de alguma forma me apoiaram e estiveram junto comigo, mesmo que em pensamento, torcendo pelo meu sucesso.

RESUMO

Este trabalho busca uma abordagem diferente para se trabalhar multiplicações e divisões em sala de aula, mostrando que por trás das tecnologias comumente utilizadas há uso da matemática. Para isto, apresenta-se um breve histórico da criptografia para então expor a proposta do método criptográfico trabalhado em sala de aula, a criptografia kid-RSA adaptada, e os resultados obtidos após a aplicação do mesmo método. Com as dificuldades que surgiram em sala durante a atividade com relação aos algoritmos de multiplicação e divisão, houve a necessidade de fazer reflexões a cerca de como se trabalham tais conteúdos e de fazer um resgate histórico em termos de definições e de algoritmos encontrados ao longo da história da matemática. Os métodos de multiplicação e divisão encontrados na história e citados neste trabalho podem servir como ideias para se apresentar alternativas aos algoritmos tradicionais de multiplicação e divisão, focando na necessidade de minimizar as dificuldades apresentadas por alguns alunos e que servem não só para o 6º ano, público alvo da atividade proposta nesta dissertação, como para ajudar qualquer aluno em qualquer série.

Palavras-chave: Criptografia. Multiplicação. Divisão. Ensino fundamental. Kid-RSA adaptada.

ABSTRACT

This work looks for a different approach to work multiplication and division at the classroom, showing that behind of the commonly technologies used has the use of mathematics. For this, a brief history of the cryptography is presented to expose the proposed cryptographic method worked in the classroom, the cryptography *kid-RSA adapted*, and the results obtained after the application of the same method. During classroom activity, some difficulties occurred in relation to multiplication and division algorithms, bringing the need to reflect on how to work such contents and to make a historical rescue in terms of definitions and algorithms found throughout the history of mathematics. The methods of multiplication and division found in the historical reports and cited in this work can serve as ideas to show alternatives to the traditional algorithms of multiplication and division, focusing on the need to minimize the difficulties presented by some students and that serve not only for the 6th grade, audience of the activity proposed in this dissertation, as to help any student in any grade.

Keywords: Cryptography. Multiplication. Division. Elementary School. Kid-RSA Adapted.

SUMÁRIO

INTRODUÇÃO

No pouco tempo que tenho como professora de matemática do 2º segmento do Ensino Fundamental, muitas foram as vezes em que, ao corrigir uma prova, por exemplo, me deparei com contas de divisão e multiplicação feitas de maneira errada, principalmente divisão, não só no sexto ano , como também nos anos seguintes.

Além disso, quase sempre me deparo com as seguintes perguntas: “Para que precisamos disto?” ou “Onde usaremos isto na nossa vida?”. Tais perguntas refletem um pouco dos questionamentos sobre como se ensina matemática. Podemos ver isto no seguinte trecho dos Parâmetros Curriculares Nacionais (PCN):

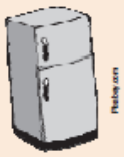
> Discussões no âmbito da Educação Matemática que acontecem no Brasil e em outros países apontam a necessidade de adequar o trabalho escolar a uma nova realidade, marcada pela crescente presença da Matemática em diversos campos da atividade humana. Tais discussões têm influenciado análises e revisões nos currículos de Matemática no ensino fundamental.
>
> (BRASIL, 1998, p.19)

Algumas páginas depois, podemos ler que muitas vezes o ensino da matemática só se preocupa com o que se acredita ser parte do dia-a-dia do aluno, na tentativa de dar significado ao conteúdo.

> Também a importância de levar em conta o conhecimento prévio dos alunos na construção de significados geralmente é desconsiderada. Na maioria das vezes, subestimam-se os conceitos desenvolvidos no decorrer das vivências práticas dos alunos, de suas interações sociais imediatas, e parte-se para um tratamento escolar, de forma esquemática, privando os alunos da riqueza de conteúdos proveniente da experiência pessoal.
> Outra distorção perceptível refere-se a uma interpretação equivocada da idéia de contexto, ao se trabalhar apenas com o que se supõe fazer parte do dia-a-dia do aluno. Embora as situações do cotidiano sejam fundamentais para conferir significados a muitos conteúdos a serem estudados, é importante considerar que esses significados podem ser explorados em outros contextos como as questões internas da própria Matemática e dos problemas históricos. Caso contrário, muitos conteúdos importantes serão descartados por serem julgados, sem uma análise adequada, que não são de interesse para os alunos porque não fazem parte de sua realidade ou não têm uma aplicação prática imediata.
>
> (BRASIL, 1998, p.23)

Podemos ver, nos materiais didáticos, exercícios como o ilustrado a seguir:

6 – Tereza comprou uma geladeira por R$ 4.200,00. Ela pagou em 8 parcelas iguais e sem juros. Quanto ela pagou em cada parcela?



(SME/RJ, 2017, p.18)

Tais tipos de exercícios não instigam o aluno a querer saber mais sobre algum assunto, além de se tornarem desinteressantes por serem repetitivos.

Levando em consideração estes aspectos e a visão dos alunos de que as quatro operações básicas (adição, subtração, multiplicação e divisão) só servem para coisas simples do cotidiano, tipo dividir uma conta de bar entre amigos, quis mostrar aos alunos que por trás das tecnologias modernas utiliza-se uma matemática que, para ser entendida, precisa-se compreender bem tais operações.

Para isto, trago nesta dissertação a proposta de se trabalhar com criptografia como uma atividade motivadora ao estudo das operações de multiplicação e divisão no conjunto dos números naturais. A escolha da criptografia para esta finalidade se deve ao fato da recente popularização de tal palavra, principalmente por conta do aplicativo de mensagens *Whatsapp*, muito usado pelos jovens.

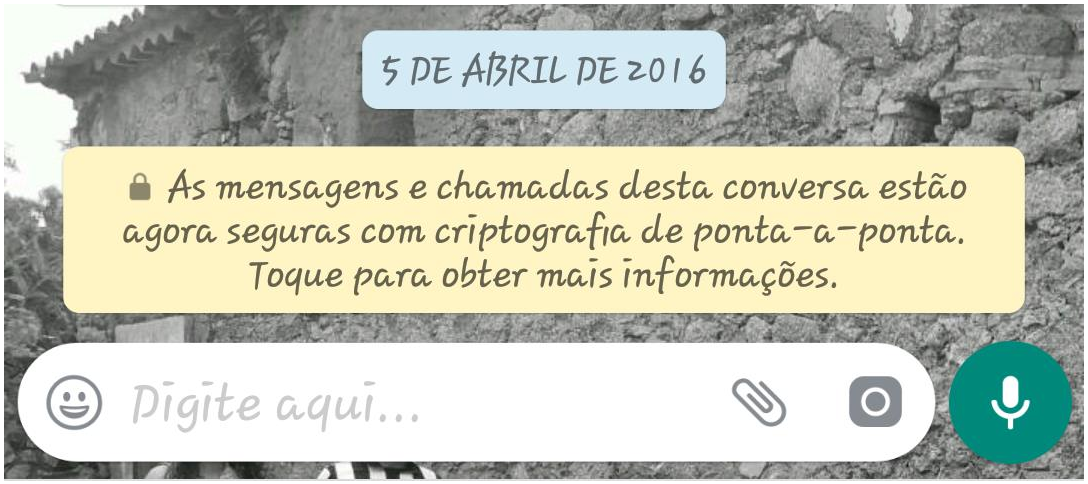


Imagem da mensagem que aparece no Whatsapp ao se iniciar uma conversa nova com algum contato

Junto a isto, motivada pelos resultados obtidos na atividade feita em sala, trago um breve resgate histórico de tais operações, como um incentivo a se buscar

alternativas para realizá-las de um modo diferente do tradicional, com o intuito de ajudar os alunos que têm dificuldades de dominar os métodos comumente usados em sala de aula.

Encontraremos, no Capítulo 1, uma breve história da criptografia, tendo em vista que ela será nosso pano de fundo. Já que utilizaremos a criptografia nas atividades, é interessante conhecer um pouco de sua história e evolução.

No Capítulo 2, apresentamos uma parte teórica necessária para compreender os sistemas criptográficos apresentados neste mesmo capítulo. Com relação a tais sistemas, abordamos o RSA que é muito conhecido e usado, que será o inspirador da nossa atividade. Além do RSA, falamos do kid-RSA, uma adaptação do RSA, feita pelo professor de matemática da Universidade de Washington Neal Koblitz, com o objetivo de se ensinar criptografia nas salas de aula do ensino básico. Por fim apresentamos uma adaptação do kid-RSA para a realidade da educação básica brasileira, chamada nesta dissertação de criptografia kid-RSA adaptada, que será a base da atividade apresentada no Capítulo 3.

No Capítulo 3, apresentamos o relato da atividade baseada na criptografia kid-RSA adaptada, aplicada em duas escolas situadas na cidade do Rio de Janeiro, uma pública e outra particular, e fazemos uma análise comparativa em relação aos erros cometidos pelos alunos.

O Capítulo 4 surgiu com a necessidade de se refletir sobre tais erros apresentados no capítulo anterior, analisando a realidade da sala de aula e resgatando a história da matemática no que diz respeito às operações de multiplicação e divisão. O resgate histórico é importante para que possamos encontrar alternativas para ajudar aqueles alunos com dificuldades nos algoritmos comumente ensinados em sala de aula.

Capítulo 1: HISTÓRIA DA CRIPTOGRAFIA

Como o objetivo deste trabalho é abordar as operações de multiplicação e divisão através da criptografia, é relevante vermos um breve histórico da arte de esconder mensagens. Mas antes, vejamos o que significa Criptografia. Em grego, *cryptos* significa secreto, oculto. Deste modo, criptografia é a arte da escrita secreta.

É interessante observar que se apenas escondermos a mensagem, de modo que qualquer busca mais simples faça com que a mensagem seja revelada, teremos a *esteganografia*. Tanto a esteganografia, quanto a criptografia, possuem seus primeiros relatos datados do século V antes de Cristo.

O primeiro relato da esteganografia é de Heródoto, século V antes de Cristo, que diz que Demarato, um grego exilado, conseguiu alertar aos espartanos os planos de Xerxes de atacar a Grécia. Segue o relato

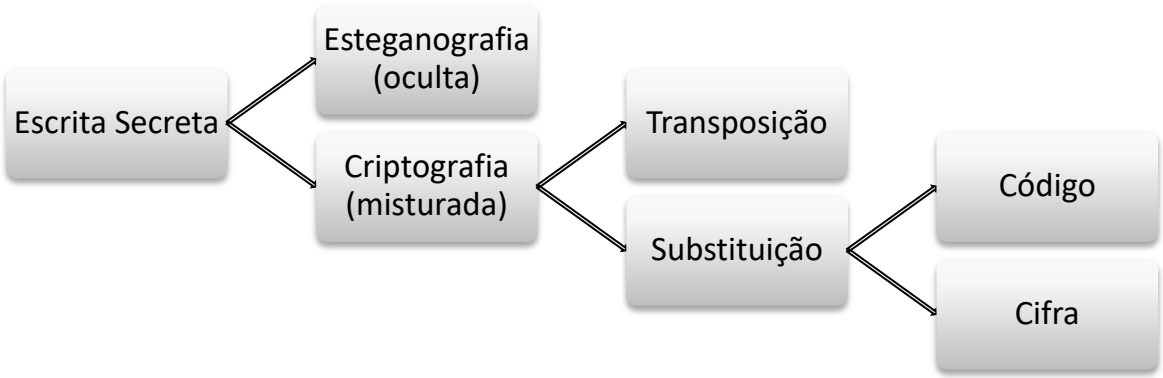
> O perigo de ser descoberto era grande; havia apenas um modo pelo qual a mensagem poderia passar: isso foi feito raspando a cera de um par de tabuletas de madeira, e escrevendo embaixo o que Xerxes pretendia fazer, depois a mensagem foi coberta novamente com cera. Deste modo, as tabuletas pareceriam estar em branco e não causariam problemas com os guardas ao longo da estrada. Quando a mensagem chegou ao seu destino, ninguém foi capaz de perceber o segredo, até que, pelo que entendi, a filha de Cleômenes, Gorgo, que era casada com Leônidas, adivinhou e contou aos outros que se eles raspassem a cera encontrariam alguma coisa escrita na madeira. Isto foi feito, revelando a mensagem, então transmitida para outros gregos.
>
> (SINGH, 2001, P. 20)

Repare que este modo de esconder a mensagem é frágil, qualquer guarda no caminho que desconfiasse e resolvesse raspar a tabuleta conseguiria ler a mensagem. Ao longo da história, existem outros relatos de uso da esteganografia, como por exemplo, os chineses que escreviam a mensagem em seda fina, amassavam até formar uma pequena bola, cobriam com cera e o mensageiro a engolia. No século XVI o cientista italiano Giovanni Porta descreveu como esconder uma mensagem dentro de um ovo cozido. No século XX, espiões utilizavam tintas invisíveis e até a própria urina para esconder mensagens. Note que mesmo sendo frágil, a esteganografia tem relatos por um longo período de tempo.

Tendo em vista a fragilidade da esteganografia, falemos então da criptografia, que é o foco deste capítulo. Na criptografia, a mensagem fica visível, mas incompreensível, indecifrável a quem não se destine a mensagem.

Na criptografia é necessário uma espécie de acordo prévio entre remetente e receptor, de modo que ambos consigam compreender a mensagem, mas, caso haja interferência de uma terceira pessoa, descobrir o conteúdo da mensagem será uma tarefa árdua, ou até mesmo impossível, dentro de um determinado espaço temporal.

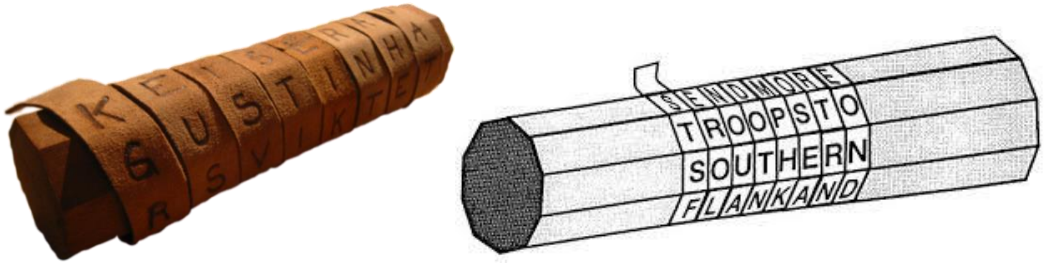
A criptografia pode ser dividida em dois ramos: transposição e substituição. A substituição, por sua vez, se ramifica em código (substituição de palavras) e cifra (substituição de letras)



Escrita secreta e suas ramificações

Transposição é quando as letras da mensagem são simplesmente reordenadas. Uma reordenação aleatória pode gerar um caos para retornar a mensagem inicial. Para termos uma transposição eficaz, é importante que haja uma regra de reordenação que seja de conhecimento de ambas as partes, remetente e receptor.

Um exemplo de criptografia utilizando o método de transposição é o *citale espartano*, que é o primeiro aparelho criptográfico militar e data do século V antes de Cristo.



Citale espartano

O *citale* funciona da seguinte forma: Enrola-se uma tira de couro sobre o bastão (*citale*) e escreve-se a mensagem. Ao desenrolar a tira de couro, passa-se a ter uma sequência de letras aleatórias, que só voltarão a fazer sentido se enrolarmos a tira de couro em outro *citale* de mesmo diâmetro.

> No ano de 404 a.C., Lisandro de Esparta recebeu um mensageiro ensanguentado e ferido, único sobrevivente de um grupo de cinco que partira da Pérsia numa árdua jornada. O mensageiro lhe entregou seu cinturão, que Lisandro enrolou em torno de seu citale para descobrir que o persa Farnabazo estava planejando atacá-lo. Graças ao citale, Lisandro estava preparado para o ataque, e o repeliu.
>
> (SINGH, 2001, P. 25)

Quando se trata de história e criptografia, a *cifra de César* é sempre lembrada. A cifra de César era umas das formas que Júlio César utilizava para se comunicar com suas tropas e consistia no deslocamento do alfabeto em três casas. Vejamos abaixo como funcionava:

Alfabeto original	a	b	c	d	e	f	g	h	i	j	k	l	m
Alfabeto cifrado	D	E	F	G	H	I	J	K	L	M	N	O	P

Alfabeto original	n	o	p	q	r	s	t	u	v	w	x	y	z
Alfabeto cifrado	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Por exemplo:

Texto original: Imperador César

Texto cifrado: Lpshudgru Fhvdu

Usar uma cifra como a de César, que basta deslocar o alfabeto, resulta em uma codificação fraca, pois basta verificar as 25 possibilidades de deslocamento para quebrar o código.

Se pensarmos em uma substituição aleatória de letras, dificultamos um pouco a quebra do código, pois passamos a ter 26! possibilidades, que nos dá algo da ordem de grandeza 10^{26}. Verificar essa enorme quantidade, sem ajuda de computação, seria uma tarefa bastante árdua e demorada.

Com relação a este tipo de cifra, existem inúmeras variantes, como, por exemplo, o quadrado de Vigenère (figura abaixo), que foi um aprimoramento da cifra de César e que permaneceu inquebrável por anos.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
01	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
02	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
03	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
04	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
05	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
06	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
07	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
08	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
09	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
10	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
11	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
12	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
13	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
14	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
15	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
16	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
17	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
18	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
19	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
20	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
21	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
22	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
23	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
24	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
25	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y
26	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z

Quadrado de Vigenère

A codificação via cifra de Vigenère consiste em ter uma palavra chave, que será utilizada para escolher qual linha será utilizada para cada letra do texto original, associada a uma letra da palavra chave. Exemplo, se na palavra chave temos uma letra I associada a uma letra P no texto original, em um dado momento da

codificação, teremos que procurar na linha iniciada por I a letra na coluna do p (p da linha não numerada), que é o X (que entrará no texto cifrado). Caso a palavra chave seja menor que a frase, repetimos a palavra chave. Vejamos um exemplo:

Palavra chave:	R I T O R I T O R I T
Texto original:	b r i l h o d o s o l
Texto cifrado:	S Z B Z Y W W C J W B

Como dito, usa-se a ideia da cifra de César, dando um incremento para que não fosse tão simples descobrir a mensagem através da contagem de frequência. Este método de cifragem foi quebrado no século XIX.

E com o uso da criptografia, vem a tentativa de quebrar, desvendar, mensagens criptografadas. A criptoanálise é a ciência que permite decifrar uma mensagem sem conhecer a chave. Quando se usa apenas substituição de uma letra por outra letra, como no caso da cifra de César, ou uma letra por um símbolo, podemos, em uma mensagem longa, quebrar o código utilizando apenas contagem de frequência.

Todo idioma possui uma letra que aparece com mais frequência. Na língua portuguesa, por exemplo, a letra A é a que aparece com maior frequência. Sendo assim, em uma mensagem longa escrita em português e criptografada através de substituição de letras, para quebrá-la basta comparar a frequência que as letras ou símbolos aparecem com a frequência das letras usadas na língua portuguesa.

Se em uma mensagem cifrada, por substituição de uma letra por outra, a letra F for mais frequente, há uma grande probabilidade que ela esteja substituindo a letra A. E através do estudo das frequências, acaba se tornando possível quebrar a mensagem. Vejamos um exemplo:

UQVPI BMZZI BMU XITUMQZIA,
WVLM KIVBI W AIJQI;
IA IDMA, YCM IYCQ OWZRMQIU,
VIW OWZRMQIU KWUW TI.
VWAAW KMC BMU UIQA MABZMTIA,
VWAAIA DIZHMIA BMU UIQA NTWZMA,
VWAAWA JWAYCMA BMU UIQA DQLI,

VWAAI DQLI UIQA IUWZMA

Texto codificado usando o site: http://www.numaboa.com.br/criptografia/124-substituicao-simples/165-codigo-de-cesar (acessado em 25/07/2018)

No texto codificado acima, temos a seguinte frequência de letras

Freqüencia de ocorrência de letras:

Rank	Letra	Ocorrências
1	i	27
2	a	25
3	m	18
4	w	16
5	u	14
6	q	12
7	z	9
8	v	8
9	b	7
10	d	4
11	t	4
12	c	4
13	l	3
14	k	3
15	y	3
16	o	2
17	r	2
18	j	2
19	n	1
20	p	1
21	x	1
22	h	1

Análise do texto criptografado via http://linguistica.insite.com.br/corpus.php (acessado em 25/07/2018)

Letra	Freqüência	Letra	Freqüência
A	14.63%	N	5.05%
B	1.04%	O	10.73%
C	3.88%	P	2.52%
D	4.99%	Q	1.20%
E	12.57%	R	6.53%
F	1.02%	S	7.81%
G	1.30%	T	4.34%
H	1.28%	U	4.63%
I	6.18%	V	1.67%
J	0.40%	W	0.01%
K	0.02%	X	0.21%

L	2.78%	Y	0.01%
M	4.74%	Z	0.47%

Tabela de frequência de letras no idioma português (fonte: https://www.gta.ufrj.br/grad/06_2/alexandre/criptoanalise.html - acessado em 25/07/2018)

Analisando as tabelas de frequência acima, podemos concluir que a letra A provavelmente foi substituída pela letra I. As letras E, O e S, são, nesta ordem, as mais frequentes após a letra A. E no texto cifrado, após a letra I, são A, M e W. Então

A = e, o ou s; M = e, o ou s; W = e, o ou s.

Como o A aparece seguidamente em uma palavra, S foi substituído pela letra A. Cabe notar que tem uma palavra onde o Z aparece seguidamente. Na nossa língua isso acontece com ss e rr. Como chegamos a conclusão que S foi substituído pelo A, então R foi substituído pelo Z.

M = e ou o; W = e ou o.

Considerando M = e, W = o e analisando as informações que já temos,

Alfabeto Original	A	B	C	D	E	F	G	H	I	J	K	L	M
Alfabeto Cifrado	I	**J?**	**K?**	**L?**	M	**N?**	**O?**	**P?**	**Q?**	**R?**	**S?**	**T?**	**U?**

Alfabeto Original	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Alfabeto Cifrado	**U?**	**V?**	W	**X?**	**Y?**	Z	A	**B?**	**C?**	**D?**	**E?**	**F?**	**G?**	**H?**

chegamos a conclusão que o alfabeto, provavelmente, foi deslocado 8 casas. Fazendo as substituições corretas, encontramos:

Substituição antes de deduzir o deslocamento do alfabeto	Substituição após deduzir o deslocamento do alfabeto
UQVP**a** B**erra** B**e**U X**a**TU**e**Q**ra**A,	“Minha terra tem palmeiras,
oVL**e** K**a**VB**a** **o** A**a**JQ**a**;	Onde canta o Sabiá;
as **a**D**es**, YC**e** **a**YCQ O**or**R**e**Q**a**U,	As aves, que aqui gorjeiam,
V**ao** O**or**R**e**Q**a**U K**o**U**o** T**a**.	Não gorjeiam como lá.
V**osso** K**e**C B**e**U U**a**Q**s** **es**B**re**T**as**,	Nosso céu tem mais estrelas,
V**ossas** D**ar**H**eas** B**e**U U**a**Q**s** NT**ores**,	Nossas várzeas têm mais flores,

V**ossos** J**os**YC**es** B**e**U U**a**Q**s** DQL**a**, Nossos bosques têm mais vida,
V**ossa** DQL**a** U**a**Q**s a**U**ores** Nossa vida mais amores”

Canção do Exílio, Gonçalves Dias

Isto é um exemplo de como uma análise de frequência em conjunto com o conhecimento da língua pode ajudar a quebrar uma mensagem codificada.

Os códigos apresentados, uma vez que a pessoa soubesse codificar, saberia também decodificar. E com o advento das telecomunicações, passou a ser cada vez mais importante que informações pudessem ser repassadas de forma segura, que quem soubesse codificar, não precisaria saber decodificar. Esse é o princípio dos códigos de chave pública, ideia introduzida em 1976 por W. Diffie e M.E. Hellman.

O código mais conhecido de chave pública é o RSA, inventado em 1978. Este método é seguro, pelo menos por enquanto, pois para quebrá-lo seria necessário fatorar o número ***n***, que faz parte da chave pública, e ***n*** é formado a partir da multiplicação de dois números primos grandes. Até este momento, não há um algoritmo suficientemente rápido que fatore tal número.

Da cifra de César ao famoso RSA, um longo caminho foi percorrido. Um trajeto possível graças aos estudos avançados dentro da área e ao surgimento de poderosas ferramentas tecnológicas. No próximo capítulo, aprofundaremos o estudo do RSA, vendo como ele funciona e adaptando para o uso em sala de aula.

Capítulo 2: CRIPTOGRAFIA RSA, Kid-RSA E Kid-RSA ADAPTADA

Antes de falarmos sobre criptografia RSA, kid-RSA e de sua adaptação que estamos propondo, precisamos retomar alguns conceitos teóricos necessários para a compreensão de cada algoritmo criptográfico a ser abordado. Para isto, serão utilizados os livros ARITMÉTICA, da coleção PROFMAT, e Números Inteiros e Criptografia RSA, do S.C. Coutinho.

2.1 Números inteiros e aritmética modular:

Seja $\mathbb{Z}$ o conjunto dos números inteiros.

2.1.1 Divisibilidade

Sejam $a,b \in \mathbb{Z}$. Dizemos que *a divide b* ou *a é divisor de b* quando existe $c \in \mathbb{Z}$ tal que $b = ac$.

Um número inteiro positivo *p* é dito *primo* se possui exatamente dois divisores positivos, a saber, 1 e *p*.

Dois números inteiros *a* e *b* são ditos *primos entre si* quando o máximo divisor comum entre eles é 1, ou seja, *mdc* (*a*, *b*) = 1. Se *p* é primo e *p* não é divisor de *a*, então *mdc* (*a*, *p*) = 1

Se *b* divide *ac* e *mdc* (*a*, *b*) = 1 então *b* divide *c*. Em particular, se *p* e *q* são números primos distintos tais que *ap* = *bq* então *p* divide *b* e *q* divide *a*.

2.1.2 Teorema da Divisão Euclidiana:

Sejam *a* e *b* dois números inteiros com b ≠ 0. Existem dois únicos números inteiros *q* e *r* tais que

$$a = bq + r, \text{ com } 0 \leq r \leq |b|$$

2.1.3 Congruência módulo n:

Seja $n > 1$ um número inteiro. Dizemos que dois números inteiros *a* e *b são congruentes módulo n* se os restos de suas divisões euclidianas por *n* são iguais. Neste caso, escrevemos $a \equiv b \bmod n$

Exemplos:

$5 \equiv 3 \mod 2$ (5 dividido por 2 deixa resto 1 e 3 dividido por 2 também deixa resto 1)

$17 \equiv 7 \mod 10$ (17 dividido por 10 deixa resto 7 e 7 dividido por 10 também deixa resto 7)

Se $a \equiv b \mod n$, existem únicos inteiros k_1, k_2 e r, com $0 \leq r < n$, tais que

$$a = nk_1 + r \quad \text{e} \quad b = nk_2 + r$$

Então

$$a - nk_1 = b - nk_2 \Rightarrow a = b + n(k_1 - k_2)$$

Ou seja, quando $a \equiv b \ mod \ n$ podemos escrever $a = nq + b$, com $q \in \mathbb{Z}$. Assim, dizer que a e b são congruentes módulo n é a mesma coisa que dizer que $a - b$ é múltiplo de n.

A congruência módulo n é uma relação de equivalência no conjunto dos números inteiros, ou seja, para todos $a, b, c \in \mathbb{Z}$ temos:

- $a \equiv a \mod n$
- $a \equiv b \mod n \Rightarrow b \equiv a \mod n$
- $a \equiv b \mod n$ e $b \equiv c \mod n \Rightarrow a \equiv c \mod n$

Sendo a congruência módulo n uma relação de equivalência, podemos trabalhar com classes de equivalência:

Seja $a \in \mathbb{Z}$. A classe de congruência módulo n de a é formada pelos inteiros b que satisfazem $a \equiv b \ mod \ n$, isto é, $b - a = kn$, para algum $k \in \mathbb{Z}$. Podemos assim descrever a classe de a na forma

$$\bar{a} = \{a + kn : k \in \mathbb{Z}\}$$

O conjunto $\mathbb{Z}_n = \{\bar{0}, \bar{1}, \dots, \overline{n-1}\}$, onde cada classe de equivalência é representada pelos possíveis restos em uma divisão por n, é chamado *conjunto dos inteiros módulo n*.

2.1.4 Aritmética modular

Sejam *a, b, c, d, n* $\in \mathbb{Z}$ e *n* > 1 tais que $a \equiv c \mod n$ e $b \equiv d \mod n$

Valem as seguintes propriedades:

- **Adição:** $a + b \equiv c + d \mod n$
- **Multiplicação:** $ab \equiv cd \mod n$
- **Potência:** Para todo número inteiro *e* > *1*, $a^e \equiv c^e \mod n$

Inverso módulo n

Sejam *a, b, n* inteiros e *n* > 1 tais que $ab \equiv 1 \mod n$

Dizemos que *b* é o inverso de *a* módulo *n*.

Teorema de inversão:

A classe $\bar{a}$ tem inverso em $\mathbb{Z}_n$ se, e somente se, *a* e *n* são primos entre si.

Exemplos:

$3.5 \equiv 1 \mod 7$, logo 5 é o inverso de 3 em $\mathbb{Z}_7$

$77.53 \equiv 1 \mod 60$, logo 53 é o inverso de 77 em $\mathbb{Z}_{60}$

Pequeno Teorema de Fermat:

Sejam $a \in \mathbb{Z}$ e *p* um número primo, então

$$a^p \equiv a \mod p$$

Além disso, se mdc(*a*,*p*) = 1, ou seja, *p* não divide *a*, então

$$a^{p-1} \equiv 1 \mod p$$

Função φ de Euler

φ é uma função que a cada inteiro *n* > 1 associa a quantidade de números inteiros entre 0 e *n* – 1 que são primos com *n*.

Se *n* é primo, temos $\varphi(n) = n - 1$.

Se *a* e *b* são primos entre si, ou seja, se mdc (*a*,*b*) =1, temos

$$\varphi(ab) = \varphi(a)\,\varphi(b)$$

Teorema de Euler

Sejam n, $a \in \mathbb{Z}$ com $n > 1$ e mdc(n,a) = 1. Então

$$a^{\varphi(n)} \equiv 1 \mod n$$

Com a base teórica vista acima, podemos analisar o funcionamento da criptografia RSA, kid-RSA e da adaptação de kid-RSA que estamos propondo.

2.2 Criptografia RSA

Este é um sistema criptográfico de chave pública. Como o nome já sugere, a chave pública é de conhecimento de todos. Além da chave pública, há também uma chave secreta, privada, que é de conhecimento apenas do receptor. A chave pública é utilizada para codificar a mensagem e a chave secreta para decodificar, por isto ela é de conhecimento apenas do receptor da mensagem. Tal sistema, assim como outros, transforma a mensagem em números antes de codifica-la.

De uma maneira bem simplista, podemos comparar sistemas criptográficos de chave pública da seguinte forma:

O baú aberto e o cadeado são as chaves públicas

O tesouro é a mensagem

Quem quiser enviar o tesouro ao dono da chave do cadeado deve colocar o tesouro no baú e fechá-lo com cadeado. Este é o processo de codificação, qualquer um podia colocar qualquer objeto no baú e fechá-lo. Nesta situação, a chave do cadeado do baú é a chave secreta. Apenas o receptor possui a chave do cadeado. Sendo assim, apenas ele consegue abrir o cadeado e pegar o tesouro.

O baú fechado representa a mensagem codificada

A chave do cadeado é a chave secreta

O baú aberto com o tesouro dentro representando a mensagem decodificada

Cabem aqui alguns esclarecimentos. As mensagens, já transformadas em números, são enviadas em blocos, cuja ordem é importante. Não se pode enviar o bloco 2 (w_2) antes do bloco 1 (w_1) pois traz problemas na hora de recuperar a mensagem. Os blocos são divididos respeitando as seguintes regras:

- Cada bloco deve ter valor menor que o valor de *n*. *n* faz parte da chave pública e veremos a frente como obter *n*.
- Os blocos não podem iniciar com zero, pois o zero se perderia ao longo do processo, trazendo problemas na hora de recuperar a mensagem.

Além dessas duas regras, algumas observações são válidas para a divisão dos blocos:

- É bom que não se faça a divisão dos blocos colocando cada letra em um bloco, pois cairíamos no caso da cifra de César, que é facilmente quebrável com contagem de frequência aliada à tecnologia atual.
- Colocar um algarismo em cada bloco também não é interessante, pois geraria muitas contas, tornando o processo de codificação e decodificação longo.
- O ideal é colocar a maior quantidade de algarismos possível em cada bloco, pois reduz o processo e evita que apareça uma letra correspondendo a um bloco.

Veremos alguns exemplos com relação a divisão de blocos mais à frente. Vamos verificar como acontece cada etapa:

2.2.1 Pré-codificação

Nesta etapa cada letra é transformada em um número, seguindo a tabela abaixo:

A	B	C	D	E	F	G	H	I	J	K	L	M
10	11	12	13	14	15	16	17	18	19	20	21	22

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
23	24	25	26	27	28	29	30	31	32	33	34	35

Não utilizaremos

A	B	C	D	E	F	G	H	I	J	K	L	M
1	2	3	4	5	6	7	8	9	10	11	12	13

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
14	15	16	17	18	19	20	21	22	23	24	25	26

pois haveria problemas do tipo:

12 é AB ou L?

Do modo proposto, sabemos que cada letra corresponde a um número de dois algarismos. Para indicar o espaço entre duas palavras, é utilizado o número 99. Esta ideia de conversão pode ser encontrada em Coutinho, 2005, que é uma abordagem didática. Nela, caracteres especiais, assim como algarismos e letras acentuadas não são contempladas. Computacionalmente, essa transformação é feita via tabela ASCII. Sendo assim, adotaremos a ideia mais simples, por ser melhor para se trabalhar com os alunos de Ensino Fundamental como um todo.

Por exemplo, transformando-se a frase **Amo a Bia** em números, de acordo com a tabela, tem-se:

102224991099111810

Para codificar com o método RSA, é necessário escolher dois números primos positivos distintos *p* e *q*. Escolhidos esses dois números, pode-se determinar *n* da seguinte forma.

$$n = pq$$

Além de *n*, serão necessários outros dois números inteiros positivos *e* e *d*, de modo que *e* seja inversível módulo $\varphi(n)$, ou seja, mdc (e,$\varphi(n)$) = 1. Como n = pq, vimos, em 2.1.10, que

$$\varphi(n) = \varphi(pq) = \varphi(p).\varphi(q) = (p-1).(q-1)$$

E *d* será o inverso de *e* em $\varphi(n)$. Ou seja,

$$ed \equiv 1 \mod \varphi(n)$$

Com isto temos nossa chave pública, que é o par (n,e), e a chave secreta que será o par (n,d).

2.2.2 Codificação

Seja *w* um bloco de mensagem a ser codificado (lembrando que *w* < *n* e não começa por zero).

C(w) será a mensagem codificada. Obtém-se C(w) da seguinte forma:

C(w) = resto da divisão de w^e por n

Se

$$w^e \equiv r_1 \mod n, \text{ com } r_1 < n$$

então $C(w) = r_1$.

Após fazer este processo com todos os blocos, envia-se a mensagem através dos blocos codificados, respeitando a ordem dos mesmos.

2.2.3 Decodificando

Seja *y* um bloco de mensagem codificado.

D(y) será a mensagem decodificada. Obtém-se D(y) da seguinte forma:

D(y) = resto da divisão de y^d por n

Se $y^d \equiv r_2 \mod n$, com $r_2 < n$, então $D(y) = r_2$.

2.2.4 Exemplo

Dados p = 11 e q = 13, temos:

n = 11.13 = 143 e $\varphi(143) = (11-1).(13-1) = 120$

Tomando e = 7, temos que mdc(7,120) = 1. Logo *e* é inversível módulo $\varphi(143)$.

Então, d = 103, pois $7.103 \equiv 721 \equiv 1 \mod \varphi(143)$.

Mensagem: Amo a Bia → 102224991099111810

A melhor divisão, seguindo as regras e as observações, é a seguinte:

$w_1 = 102$ $w_2 = 22$ $w_3 = 49$ $w_4 = 9$ $w_5 = 109$ $w_6 = 91$
$w_7 = 118$ $w_8 = 10$

Codificando cada bloco w_i, obtemos:

$102^7 \equiv 119 \mod 143$
$22^7 \equiv 22 \mod 143$
$49^7 \equiv 36 \mod 143$
$9^7 \equiv 48 \mod 143$
$109^7 \equiv 21 \mod 143$
$91^7 \equiv 130 \mod 143$
$118^7 \equiv 79 \mod 143$
$10^7 \equiv 10 \mod 143$

Assim, os blocos codificados são

$y_1 = 119$ $y_2 = 22$ $y_3 = 36$ $y_4 = 48$ $y_5 = 21$ $y_6 = 130$
$y_7 = 79$ $y_8 = 10$

Decodificando cada bloco y_i, obtemos:

$119^{103} \equiv 102 \mod 143$
$22^{103} \equiv 22 \mod 143$
$36^{103} \equiv 49 \mod 143$
$48^{103} \equiv 9 \mod 143$
$21^{103} \equiv 109 \mod 143$
$130^{103} \equiv 91 \mod 143$
$79^{103} \equiv 118 \mod 143$
$10^{103} \equiv 10 \mod 143$

Sendo assim, recuperamos a mensagem:

102224991099111810 → Amo a Bia.

2.2.5 Por que D(C(b)) = b funciona?

Por definição

$$D\big(C(b)\big) \equiv \big(C(b)\big)^d \equiv (b^e)^d \equiv b^{ed} \mod n \quad (*)$$

Lembrando que n = pq com *p*,*q* números inteiros positivos primos distintos. Como *d* é o inverso de *e* módulo $\varphi(n)$, temos:

$$ed \equiv 1 \mod \varphi(n)$$

$$ed = 1 + k\,\varphi(n),\ k \in \mathbb{Z}$$

$$ed = 1 + k\,(p-1)\,(q-1)$$

Sendo assim

$$b^{ed} \equiv b^{1+k\varphi(n)} \equiv b^{1+k(p-1)(q-1)} \equiv b.(b^{p-1})^{k(q-1)} \mod p$$

Se mdc(b,p) ≠ 1, então $b \equiv 0 \mod p$ e $b^{ed} \equiv 0^{ed} \equiv 0 \mod p$. Logo

$$b^{ed} \equiv b \mod p$$

Se mdc(b,p) = 1, então, pelo teorema de Fermat, temos

$$b^{ed} \equiv b.(b^{p-1})^{k(q-1)} \equiv b.1^{k(q-1)} \equiv b \mod p$$

Ou seja, se *b* for múltiplo de *p* ou não, teremos

$$b^{ed} \equiv b \mod p$$

De modo análogo, teremos

$$b^{ed} \equiv b \mod q$$

Mas queremos

$$b^{ed} \equiv b \mod n$$

Até agora temos que

$$b^{ed} \equiv b \mod p$$

$$b^{ed} \equiv b \mod q$$

Podemos reescrever as duas congruências acima como

$$b^{ed} = pk_1 + b\,,\quad k_1 \in \mathbb{Z} \quad (1)$$

$$b^{ed} = qk_2 + b\,,\quad k_2 \in \mathbb{Z} \quad (2)$$

Das duas equações, obtemos

$$pk_1 = qk_2 \Rightarrow \text{p divide q ou p divide } k_2$$

Como mdc(p,q)=1, p só pode dividir k_2. Logo,

$$k_2 = pk_3\,,\quad k_3 \in \mathbb{Z} \qquad (3)$$

Deste modo, substituindo (3) em (2), temos:

$$b^{ed} = qk_2 + b \Rightarrow b^{ed} = qpk_3 + b \Rightarrow b^{ed} \equiv b \mod n \qquad (4)$$

Sendo assim, voltando a (*) e usando (4), temos:

$$D\big(C(b)\big) \equiv b \mod n$$

2.3 Criptografia Kid-RSA

A criptografia kid-RSA é uma proposta encontrada em Koblitz,1997. O autor propõe métodos criptográficos que podem ser abordados em sala de aula, pois ele acredita no potencial da criptografia para enriquecer o ensino da matemática. Kid-RSA é uma proposta para ensino médio, cuja descrição encontrada neste artigo apresentamos abaixo:

> *As letras serão escritas em base 26, ou seja, A $\rightarrow$ 0, B $\rightarrow$ 1, C $\rightarrow$ 2, ..., Z $\rightarrow$ 25.*
> *Alice escolhe dois inteiros a e b, calcula M = ab – 1, escolhe mais dois inteiros a' e b' e finalmente calcula*
>
> $$e = a'M + a \qquad d = b'M + b$$
> $$n = \frac{ed - 1}{M} = a'b'M + ab' + a'b + 1$$
>
> *Sua chave pública é (n,e) e sua chave secreta é d. Para enviar à Alice um texto m, basta fazer c $\equiv$ em (mod n). Alice decodifica a mensagem recebida c, calculando*
>
> $$dc \mod n.$$
>
> *Ao se fazer isso, recuperamos a mensagem m pois*
>
> $$dc \equiv dem \equiv 1 \,.\, m \equiv m \mod n$$
>
> *(*Neal Koblitz, 1997, p.320, *tradução da autora)*

Cabe ressaltar que antes de codificar é necessário reescrever a mensagem, que está escrita em base 26, em base 10. Ou seja, m, no texto, já está em base 10. Repare que o texto não diz como identificar um espaço no meio de duas palavras, O texto também não fala da necessidade de que cada bloco seja menor que n. Além disso, teremos problemas caso a palavra comece com A. Veja abaixo o que acontece quando codificamos a palavra amor.

Palavra a ser enviada: AMOR

Calculando m:

$m = 0.26^3 + 12.26^2 + 14.26 + 17 = 8493$

Determinando chaves

Tomemos, por exemplo, a = 5, b = 2, a' = 4 e b' = 7. Então:

M = 5.2 – 1 = 9 e = 4.9 + 5 = 41 d = 7.9 + 2 = 65

$n = \frac{41.65-1}{9} = 296$

Portanto,

Chave pública: (n,e) = (296 , 41)

Chave secreta: d = 65

Formando os blocos:

$m_1 = 84$ $m_2 = 93$

Neste caso, como os algarismos não representam uma letra, a preocupação é exclusiva em ser menor que n e não começar por zero. O artigo não menciona isto, mas se a mensagem for enviada sem considerar tais regras, não conseguiremos recuperar a mensagem

Codificando

$c_1 \equiv 41.84 \pmod{296}$

$c_1 \equiv 188 \pmod{296}$

$c_2 \equiv 41.93 \pmod{296}$

$c_2 \equiv 261 \pmod{296}$

Serão enviados os blocos: 188 e 261

Decodificando

$65.188 \equiv 12220 \equiv \mathbf{84} \pmod{296}$

$65.261 \equiv 16965 \equiv \mathbf{93} \pmod{296}$

Deste modo, recuperamos a mensagem: m = **8493**

Agora só é necessário transformar a mensagem m, que está em base 10, para base 26.

8493 ÷ 26 = 326, resto 17

326 ÷ 26 = 12, resto 14

$m = (12\ 14\ 17)_{26}$ = MOR

A letra *A* da palavra amor se perdeu na hora de transformarmos de base 26 para base 10, pois *A* é representado por zero e, no caso do exemplo, $0.26^3 = 0$ perdendo-se assim a letra *A*.

2.4 Criptografia Kid-RSA Adaptada

Nesta seção apresentamos nossa proposta de adaptação da criptografia Kid-RSA para ser utilizada como uma atividade motivadora ao estudo das operações de multiplicação e divisão de naturais no segundo segmento do Ensino Fundamental.

Nesta adaptação utilizaremos a ideia de como codificar e decodificar a mensagem vista na seção 2.3 e a ideia de transcrição da palavra/frase vista na seção 2.2. Com relação à conversão das palavras para números, não utilizaremos a ideia vista na seção 2.3, pois, além de trazer o problema com palavras iniciadas com a letra *A*, teríamos que lidar com conversão de bases, que não faz parte do currículo obrigatório do 2º segmento do Ensino Fundamental, tal conteúdo não consta nos Parâmetros Curriculares Nacionais (PCN).

Com relação à codificação e à decodificação, na seção 2.3 precisamos do conhecimento de congruências, que também é um conteúdo que não consta no PCN como obrigatório para o 2º segmento do Ensino Fundamental.

Então, ao invés de usarmos a relação A $\rightarrow$ 0, B $\rightarrow$ 1, C $\rightarrow$ 2, ..., Z $\rightarrow$ 25, ou seja, escrever a mensagem em base 26, usaremos a relação vista anteriormente para RSA na seção 2.2:

A	B	C	D	E	F	G	H	I	J	K	L	M
10	11	12	13	14	15	16	17	18	19	20	21	22

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
23	24	25	26	27	28	29	30	31	32	33	34	35

Cabe ressaltar que para representar o espaço entre duas palavras, utilizaremos o número 99.

Para contornar o problema com relação a congruências, utilizaremos o Teorema da Divisão Euclidiana.

Sendo assim, reescrevemos kid-RSA da seguinte forma adaptada:

Alice escolhe dois inteiros positivos *a* e *b*, calcula *M = ab – 1*; escolhe mais dois inteiros positivos *a'* e *b'* e finalmente calcula

e = a'M + a ***d = b'M + b*** $n = \frac{ed-1}{M} = a'b'M + ab' + a'b + 1$ ***(1)***

Sua chave pública é *(n,e)* e sua chave secreta é *d.*

Para enviar à Alice um texto *m*, basta fazer

em = nq + r* , sendo *q* e *r*, respectivamente, o quociente e o resto da divisão do produto entre *e* e *m* por *n.

c = r será a mensagem codificada enviada a Alice.

Alice decodifica a mensagem recebida *c*, calculando

dc = nk + l.

onde *k* e *l* serão, respectivamente, o quociente e o resto da divisão do produto entre *d* e *c* por *n*. Além disso, *l* será a mensagem *m* original.

Cabe fazer algumas observações sobre o envio da mensagem codificada. A mensagem deverá ser enviada em blocos, utilizando a mesma ideia trabalhada e discutida na seção 2.2, de modo que cada bloco seja um número menor que *n* e que não comece por zero. Cada bloco de mensagem será codificado separadamente e em ordem e será enviado separadamente e na mesma ordem.

Vamos verificar a última afirmação (l = m).

$M = ab - 1 \Rightarrow ab = M + 1$ (2)

$de = (b'M + b).(a'M + a) \Rightarrow$

$de = a'b'M^2 + ab'M + a'bM + ab$

Por (2) temos

$de = a'b'M^2 + ab'M + a'bM + M + 1$

$de = M(a'b'M + ab' + a'b + 1) + 1$

Por (1) temos $n = \frac{ed-1}{M} = a'b'M + ab' + a'b + 1$ e, portanto,

$de = Mn + 1$ (3)

Analisando o processo de codificação:

$em = nq + r \Rightarrow r = em - nq$

$c = r \Rightarrow c = em - nq$

Analisando o processo de decodificação:

$dc = d(em - nq) \Longrightarrow$

$dc = dem - dnq \Rightarrow$

Por (3) temos $de = Mn + 1$ e, portanto,

$dc = (Mn + 1)m - dnq \Rightarrow$

$dc = Mnm + m - dnq \Rightarrow$

$dc = (Mm - dq)n + m \Rightarrow$

Mas temos que *dc* = *nk* + *l*, logo

$nk + l = (Mm - dq)n + m$

Como *l* é o resto da divisão de *dc* por *n* e *m* é menor que *n*, pois, como visto anteriormente, a mensagem é enviada em blocos com valores menores que *n*, podemos concluir que

l = *m*

2.4.1 Exemplos

Consideremos a = 5, b = 2, a' = 4 e b' = 7. Então:

M = 5.2 – 1 = 9 e = 4.9 + 5 = 41 d = 7.9 + 2 = 65

$n = \frac{41.65-1}{9} = 296$

Portanto:

Chave pública (296,41)

Chave secreta 65

a) <u>Mensagem</u>: PAZ $\rightarrow$ 251035

$m_1 = 25$ $m_2 = 103$ $m_3 = 5$

Lembrando que para codificar precisamos fazer em = nq + r, c = r

$m_1 = 25$

41.25 = 1025

1025 = 296.3 + 137

$c_1 = 137$

$m_2 = 103$

41.103 = 4223

4223 = 296.14 + 79

$c_2 = 79$

$m_3 = 5$

41.5 = 205

205 = 296.0 + 205

$c_3 = 205$

Alice receberá os blocos codificados: $c_1 = 137$, $c_2 = 79$ e $c_3 = 205$

Alice decodifica fazendo $dc_i = nk + l_i$, $m_i = l_i$, com i = 1, 2,3:

$c_1 = 137$

65.137 = 8905

8905 = 296.30 + 25

$m_1 = 25$

$c_2 = 79$

65.79 = 5135

5135 = 296.17 + 103

$m_2 = 103$

$c_3 = 205$

65.205 = 13325

13325 = 296.45 + 5

$m_3 = 5$

Desta forma, Alice consegue decodificar a mensagem e recuperar a mensagem original. Para recuperar a mensagem original, basta juntar m_1, m_2 e m_3, obtendo 251035. Que significa PAZ.

b) Mensagem: Amo a Bia $\rightarrow$ 102224991099111810

A melhor divisão, seguindo as regras e as observações, é a seguinte:

$w_1 = 102$ $w_2 = 22$ $w_3 = 49$ $w_4 = 9$ $w_5 = 109$ $w_6 = 91$

$w_7 = 118$ $w_8 = 10$

Codificando

102 . 41 = 296 . 14 + 38

4182 = 296 . 14 + 38

$c_1 = 38$

22 . 41 = 296 . 3 + 14

902 = 296 . 3 + 14

$c_2 = 14$

49 . 41 = 296 . 6 + 233

2009 = 296 . 6 + 233

$c_3 = 233$

9 . 41 = 296 . 1 + 73

369 = 296 . 1 + 73

$c_4 = 73$

109 . 41 = 296 . 15 + 29

4469 = 296 . 15 + 29

$c_5 = 29$

91 . 41 = 296 . 12 + 179

3731 = 296 . 12 + 179

$c_6 = 179$

118 . 41 = 296 . 16 + 102

4838 = 296 . 16 + 102

$c_7 = 102$

10 . 41 = 296 . 1 + 114

410 = 296 . 1 + 114

$c_8 = 114$

Serão enviados os blocos: $c_1 = 38$, $c_2 = 14$, $c_3 = 233$, $c_4 = 73$, $c_5 = 29$, $c_6 = 179$, $c_7 = 102$ e $c_8 = 114$

Decodificando

$38 . 65 = 296 . 8 + 102$

$2470 = 296 . 8 + 102$

$w_1 = 102$

$14 . 65 = 296 . 3 + 22$

$910 = 296 . 3 + 22$

$w_2 = 22$

$233 . 65 = 296 . 51 + 49$

$15145 = 296 . 51 + 49$

$w_3 = 49$

$73 . 65 = 296 . 16 + 9$

$4745 = 296 . 16 + 9$

$w_4 = 9$

$29 . 65 = 296 . 6 + 109$

$1885 = 296 . 6 + 109$

$w_5 = 109$

$179 . 65 = 296 . 39 + 91$

$11635 = 296 . 39 + 91$

$w_6 = 91$

$102 . 65 = 296 . 22 + 118$

$6630 = 296 . 22 + 118$

$w_7 = 118$

$114 . 65 = 296 . 25 + 10$

$7410 = 296 . 25 + 10$

$w_8 = 10$

Sendo assim, recuperamos a mensagem:

$$102224991099111810 \rightarrow \text{Amo a Bia.}$$

Capítulo 3: CRIPTOGRAFIA KID-RSA ADAPTADA: RELATO DE EXPERIÊNCIA EM SALA DE AULA

Neste capítulo apresentamos os resultados da experiência na aplicação de atividade baseada na nossa adaptação da criptografia Kid-RSA descrita no capítulo anterior. Iniciamos com uma breve descrição das escolas onde a atividade foi aplicada, fazendo um comparativo pedagógico entre elas. Em seguida, fazemos um relato de como a atividade foi aplicada em cada escola e um comparativo de erros e acertos com relação às escolas cuja atividade foi aplicada.

A atividade proposta foi aplicada em duas escolas na cidade do Rio de Janeiro, uma da rede municipal e outra particular. A faixa etária dos alunos que participaram desta atividade, em ambas as escolas, está em torno dos 10, 11 anos de idade.

3.1 Uma breve visão da escola municipal

A atividade foi realizada em uma escola da rede municipal localizada no bairro da Tijuca. Seus alunos são, em sua maioria, oriundos das comunidades que a cercam: Borel, Casa Branca, Formiga. No ano de 2018, todas as séries escolares possuem apenas uma turma em cada turno. Como a escola possui turmas desde a Educação infantil até o nono ano, poucos são os alunos de 6º ano oriundos de outras escolas.

O alunato, em sua maioria, é de classe D ou E. Muitos responsáveis são analfabetos ou semi-analfabetos ou ainda analfabetos funcionais, o que dificulta na hora de acompanhar a vida escolar de seus filhos. Muitos falam que não conseguem ajudar seus filhos a estudar por não lembrarem a matéria, por nunca terem visto tal matéria ou por eles próprios já terem demonstrado dificuldades em sua época de estudante. Poucos são os alunos cujos pais conseguem se fazer mais presentes em sua vida acadêmica e lhes dar um suporte.

O material didático disponibilizado são apostilas confeccionadas pela própria Secretaria Municipal de Educação do Rio de Janeiro, além dos livros fornecidos através do PNLD.

Desde 2017, esta escola participa do projeto OBMEP na Escola. Procuramos, através deste projeto, ampliar os conhecimentos matemáticos dos alunos que

apresentam bons resultados em sala de aula. Em 2018, o projeto contempla alunos de sétimo ao nono ano escolar.

3.2 Uma breve visão da escola particular

A atividade foi realizada em uma unidade de uma rede de ensino que possui 20 unidade no estado do Rio de Janeiro e 5 unidades fora do estado do Rio de Janeiro. Os alunos que chegam ao sexto ano costumam vir de outras escolas particulares, uma vez que esta rede de ensino ainda não possui primeiro segmento do Ensino Fundamental em todas as unidades e a unidade onde a atividade foi apresentada passará a ter o primeiro segmento do ensino Fundamental apenas no ano de 2019.

A atividade foi aplicada em 2018 na única turma de sexto ano desta unidade, que tem 45 alunos. Estes são provenientes, em sua maioria, dos bairros de: Madureira, Vaz Lobo, Irajá, Cascadura, Oswaldo Cruz e Vicente de Carvalho. Esta rede de ensino, como um todo, atende a alunos de classe média.

Tal instituição possui turmas de 6º ao 8º ano do Ensino Fundamental e 1º e 2º ano do Ensino Médio. No 9º ano do Ensino Fundamental e no 3º ano do Ensino Médio, os alunos são encaminhados para outras unidades, também localizadas no bairro de Madureira, de acordo com o tipo de turma que vão querer cursar. As últimas séries de cada ciclo escolar tem um caráter preparatório, podendo ter foco em concursos militares ou em concursos não militares.

A escola oferece, no contraturno, monitoria de algumas disciplinas, inclusive matemática. Os alunos podem utilizar as monitorias para tirar dúvidas tanto de conteúdo, quanto de exercício. Os discentes têm também acesso a um portal que contém várias vídeoaulas com breves resumos dos conteúdos e monitoria online. O material didático utilizado são apostilas produzidas pelo grupo de ensino no qual esta instituição faz parte.

3.3 Comparativos Pedagógicos

Pedagogicamente, existe uma grande diferença entre ambas as redes. Enquanto na escola municipal do Rio de Janeiro os alunos de 6º ano tem apenas 4 tempos de aula de matemática, cada um com 50 minutos, na escola particular onde a atividade foi aplicada os alunos de 6º ano tem 8 tempos de matemática, cada um com a mesma duração das escolas municipais. Ou seja, os alunos desta escola

particular têm o dobro de tempos de aula de matemática em comparação aos alunos da rede municipal de ensino do Rio de Janeiro.

Com relação aos planejamentos, tem-se basicamente o mesmo conteúdo a ser trabalhado, tanto em uma escola, quanto na outra. Contudo, como sinalizado, nesta rede particular há o dobro de tempo para se trabalhar tais conteúdos.

Essa diferença gigantesca reflete em como os conteúdos são apresentados. Por haver uma maior carga horária, nesta escola particular o conteúdo é trabalhado com maior aprofundamento, pois há mais tempo para fazer mais exercícios e diversificar no nível dos mesmos. Já nas escolas da rede municipal do Rio de Janeiro, enfrentamos uma corrida contra o tempo, tentando abordar a maior quantidade possível de conteúdo sem perder qualidade.

3.4 O Processo de Construção da Atividade

A proposta de trabalhar com criptografia em sala de aula de maneira infantil, surge para ajudar a dar significado à matemática. Utilizei o ano de 2017 para aprimorar a ideia e chegar à versão aplicada em 2018. Durante o processo de construção da atividade, três versões foram criadas.

As duas primeiras foram utilizadas em 2017 e a última em 2018. Conforme apliquei as duas primeiras versões em 2017, pude analisar o que precisava ser melhorado, gerando a versão 3, que foi a utilizada em sala no ano de 2018.

Na terceira versão, tomei cuidado na hora de escolher os valores de *a, a', b e b'* para não gerar valores de *e, d e n* altos demais e também fui cautelosa na escolha das palavras que seriam utilizadas. Tive esta precaução para não tornar a atividade demasiadamente desafiadora para os alunos, de modo que as operações de multiplicação e divisão não ficassem muito complicadas para eles resolverem dentro do tempo proposto.

Após os testes feitos em 2017, cheguei à conclusão que seria melhor colocar os alunos para trabalharem em duplas e/ou trios, com o objetivo de que um aluno pudesse ajudar o(s) outro(s). Cada dupla/trio recebeu ou a palavra BOA ou a palavra ECO.

Veja a seguir cada uma das versões.

Aluno (a): _____ Data: _____/_____/_____

AULA SOBRE CRIPTOGRAFIA E TEOREMA DA DIVISÃO EUCLIDIANA

Como vimos nos slides, para criptografar (codificar) um texto, precisamos usar uma tabela de conversão. Para auxiliar nossas atividades, segue abaixo a tabela de conversão:

Tabela de Conversão

A	B	C	D	E	F	G	H	I	J	K	L	M
10	11	12	13	14	15	16	17	18	19	20	21	22

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
23	24	25	26	27	28	29	30	31	32	33	34	35

Lembrando que, para simbolizar o espaço entre duas palavras, colocaremos 99.

Atividade 1

Sendo a chave pública

n = 167

e = 22

Vamos criptografar a palavra CEREJA.

Palavra: CEREJA

1º) Vamos converter a palavra em números

Palavra convertida em números: _____

2º) Vamos separar nos blocos (lembrando que cada bloco tem que ser menor que n e não pode começar por zero)

Blocos de mensagem:

3º) Vamos criptografar (codificar):

Aluno (a): Alice

Data: _____/_____/_____

AULA SOBRE CRIPTOGRAFIA E TEOREMA DA DIVISÃO EUCLIDIANA

Como vimos nos slides, para criptografar (codificar) um texto, precisamos usar uma tabela de conversão. Para auxiliar nossas atividades, segue abaixo a tabela de conversão:

Tabela de Conversão

A	B	C	D	E	F	G	H	I	J	K	L	M
10	11	12	13	14	15	16	17	18	19	20	21	22

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
23	24	25	26	27	28	29	30	31	32	33	34	35

Lembrando que, para simbolizar o espaço entre duas palavras, colocaremos 99.

Atividade 2

Sendo a chave pública

n = 167

e = 22

Vamos criptografar a palavra Bola.

Palavra: Bola

1º) Vamos converter a palavra em números

Palavra convertida em números: _____

2º) Vamos separar nos blocos (lembrando que cada bloco tem que ser menor que 167 e **NÃO** pode começar por zero)

Blocos de mensagem:

3º) Vamos criptografar (codificar):

Mensagem de: Alice

Para: _____

Mensagem codificada: _____

4°) Vamos decodificar:

Mensagem original: _____

Alunos (as): _____ Data: _____/_____/_____

REVISÃO DE MULTIPLICAÇÃO E DIVISÃO

Você sabia que é possível escrever uma mensagem de uma forma que só você possa entendê-la depois?

Vamos brincar de codificar a palavra!
Para isto, precisaremos transformar cada letra da palavra em número usando a tabela abaixo.

Tabela de Conversão

A	B	C	D	E	F	G	H	I	J	K	L	M
10	11	12	13	14	15	16	17	18	19	20	21	22

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
23	24	25	26	27	28	29	30	31	32	33	34	35

Curiosidade: Se quisermos escrever uma frase, utilizamos 99 para simbolizar o espaço entre duas palavras.

Atividade

Os números abaixo serão importantes

n = 123 & e = 22

Utilizaremos a palavra BOA.

1º) Vamos converter a palavra em números

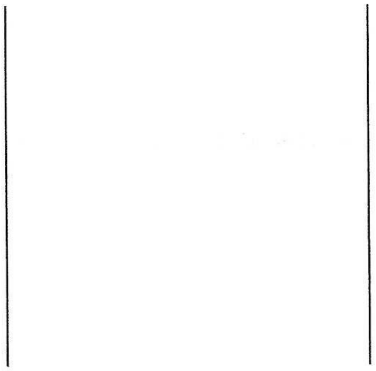
Palavra convertida em números: _____

2º) Vamos separar nos blocos (lembrando que cada bloco tem que ser menor que n e não pode começar por zero)
Blocos de mensagem:

As próximas etapas servem para embaralhar a mensagem, de modo que seja difícil ler a mensagem sem saber desembaralhá-la

3º) Vamos multiplicar cada bloco pelo valor do e

4º) Vamos dividir cada valor encontrado na 3ª etapa pelo valor do n



De: _____

Para: _____

'Mensagem': _____|_____|_____

Repare que, se vocês tentarem pegar a mensagem que receberam direto em palavra (usando a tabela de conversão) não aparecerá nada que faça sentido. Precisamos desembaralhar as mensagens. Faremos isto nas próximas etapas.

1°) Vamos multiplicar cada bloco por 28

2º) Vamos dividir cada valor encontrado na 1ª etapa pelo valor do n

3°) Escreva os restos em ordem: _____

4°) Olhe a tabela e recupere a mensagem: _____

Tabela de Conversão

A	B	C	D	E	F	G	H	I	J	K	L	M
10	11	12	13	14	15	16	17	18	19	20	21	22

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
23	24	25	26	27	28	29	30	31	32	33	34	35

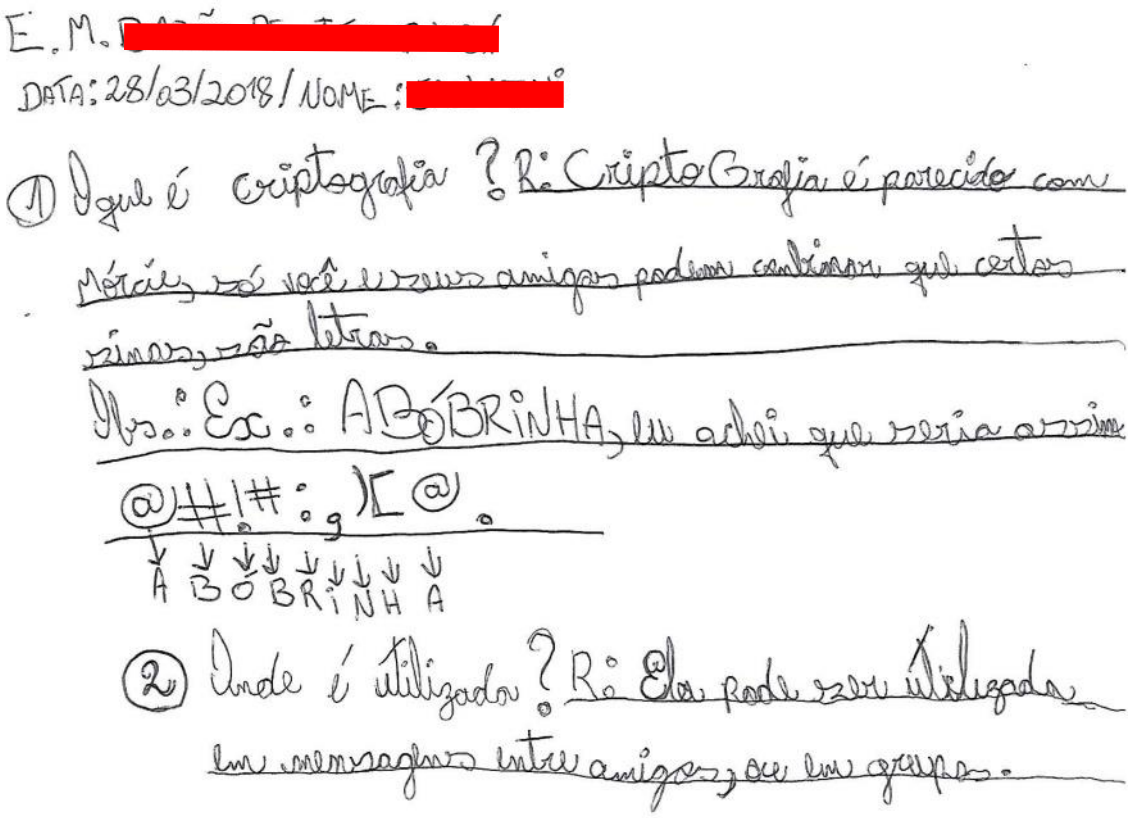
3.5 Relato da Atividade na Escola Municipal

Fiz um breve resumo do que se tratava a atividade, dizendo que tinha a ver com criptografia. Falei que a criptografia é utilizada no nosso cotidiano, como, por exemplo, no aplicativo *Whatsapp* que sinaliza, ao iniciar uma nova conversa, que as mensagens serão protegidas por criptografia de ponta-a-ponta. Expliquei que criptografia é como se colocássemos uma mensagem dentro de um baú com cadeado (CODIFICAÇÃO) e só quem possuísse a chave do cadeado poderia ler (DECODIFICAR) a mensagem.

A atividade foi realizada em uma das duas turmas de sexto ano que leciono nesta escola no ano de 2018, sendo feita logo após trabalhar com eles os conteúdos de multiplicação e divisão. Deste modo, a atividade foi apresentada como uma revisão de tais conteúdos. Para realizá-la, como dito anteriormente, formei duplas e trios, de modo que os alunos pudessem se ajudar, com uma parte da turma recebendo a palavra BOA e a outra recebendo a palavra ECO. Mesmo em duplas e trios, a atividade não ocorreu de maneira rápida. Planejei para iniciar e finalizar a atividade em 2 tempos de aula (cada tempo tem 50min), mas foi necessário mais tempo para que a maioria conseguisse finalizar. Havia 28 alunos no dia que iniciei a atividade.

Somente 2 duplas conseguiram finalizar no tempo proposto, inclusive um dos meninos de uma dessas duas duplas identificou que a mensagem codificada que eles receberam tinha problemas, pois eles não haviam conseguido encontrar a palavra (eles receberam o 1º bloco de mensagem errado).

Como a maioria dos alunos não finalizou em 2 tempos, utilizei mais um tempo e meio, aproximadamente, para que os outros alunos finalizassem. Além disso, pedi para que pesquisassem, utilizando seus celulares e a internet fornecida pelo meu celular, o que é criptografia, uma vez que falei muito rapidamente com eles sobre o que é criptografia no início da atividade, onde é utilizada, já que só dei um exemplo do uso da criptografia, e o que acharam da atividade. No geral, a maioria das duplas/trios relatou ter achado a atividade legal, divertida. Somente uma dupla disse não ter gostado da atividade. Uns 3 alunos haviam faltado no dia que comecei a atividade, para esse alunos, pedi somente que pesquisassem o que é criptografia e onde ela é usada. Para minha surpresa, um desses alunos, não fez a pesquisa, pois ele já tinha uma noção do que é criptografia (como mostra a figura a seguir).


E. M. [redacted]

DATA: 28/03/2018 / NOME: [redacted]

① O que é criptografia? R: CriptoGrafia é parecido com Mórcis só você e seus amigos podem combinar que certos sinais, são letras.

Ex.: ABÓBRINHA, eu achei que seria assim @#!#:g)Σ@.

A B Ó BR I NH A

② Onde é utilizado? R: Ela pode ser utilizada em mensagens entre amigos, ou em grupos.

Respostas dadas pelo aluno que não pesquisou na internet

Nas imagens a seguir, vemos um caso de sucesso.

Alunos (as) [redacted]

Data: 26/03/18

REVISÃO DE MULTIPLICAÇÃO E DIVISÃO

Você sabia que é possível escrever uma mensagem de uma forma que só você possa entendê-la depois?

Vamos brincar de codificar a palavra!
Para isto, precisaremos transformar cada letra da palavra em número usando a tabela abaixo.

Tabela de Conversão

A	B	C	D	E	F	G	H	I	J	K	L	M
10	11	12	13	14	15	16	17	18	19	20	21	22

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
23	24	25	26	27	28	29	30	31	32	33	34	35

Curiosidade: Se quisermos escrever uma frase, utilizamos 99 para simbolizar o espaço entre duas palavras.

Atividade

Os números abaixo serão importantes

n = 123 & e = 22

Utilizaremos a palavra ECO.

1º) Vamos converter a palavra em números

Palavra convertida em números: 14 12 24

2º) Vamos separar nos blocos (lembrando que cada bloco tem que ser menor que n e não pode começar por zero)

Blocos de mensagem:

14 | 122 | 4

As próximas etapas servem para embaralhar a mensagem, de modo que seja difícil ler a mensagem sem saber desembaralhá-la

3º) Vamos multiplicar cada bloco pelo valor do e

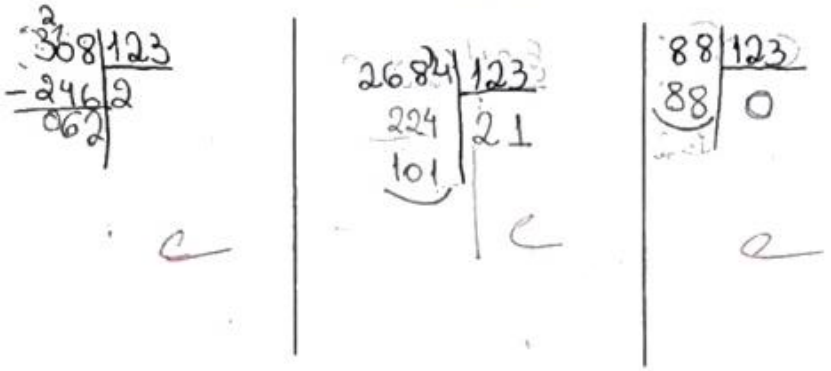
a)
$$\begin{array}{r} 14 \\ \times\ 22 \\ \hline 28 \\ +\ 28\boxtimes \\ \hline 308 \end{array}$$
c

b)
$$\begin{array}{r} 122 \\ \times\ 22 \\ \hline 244 \\ +\ 244\boxtimes \\ \hline 2684 \end{array}$$
c

c)
$$\begin{array}{r} 22 \\ \times\ 4 \\ \hline 88 \end{array}$$
c

Folha 1 – frente – do trio A

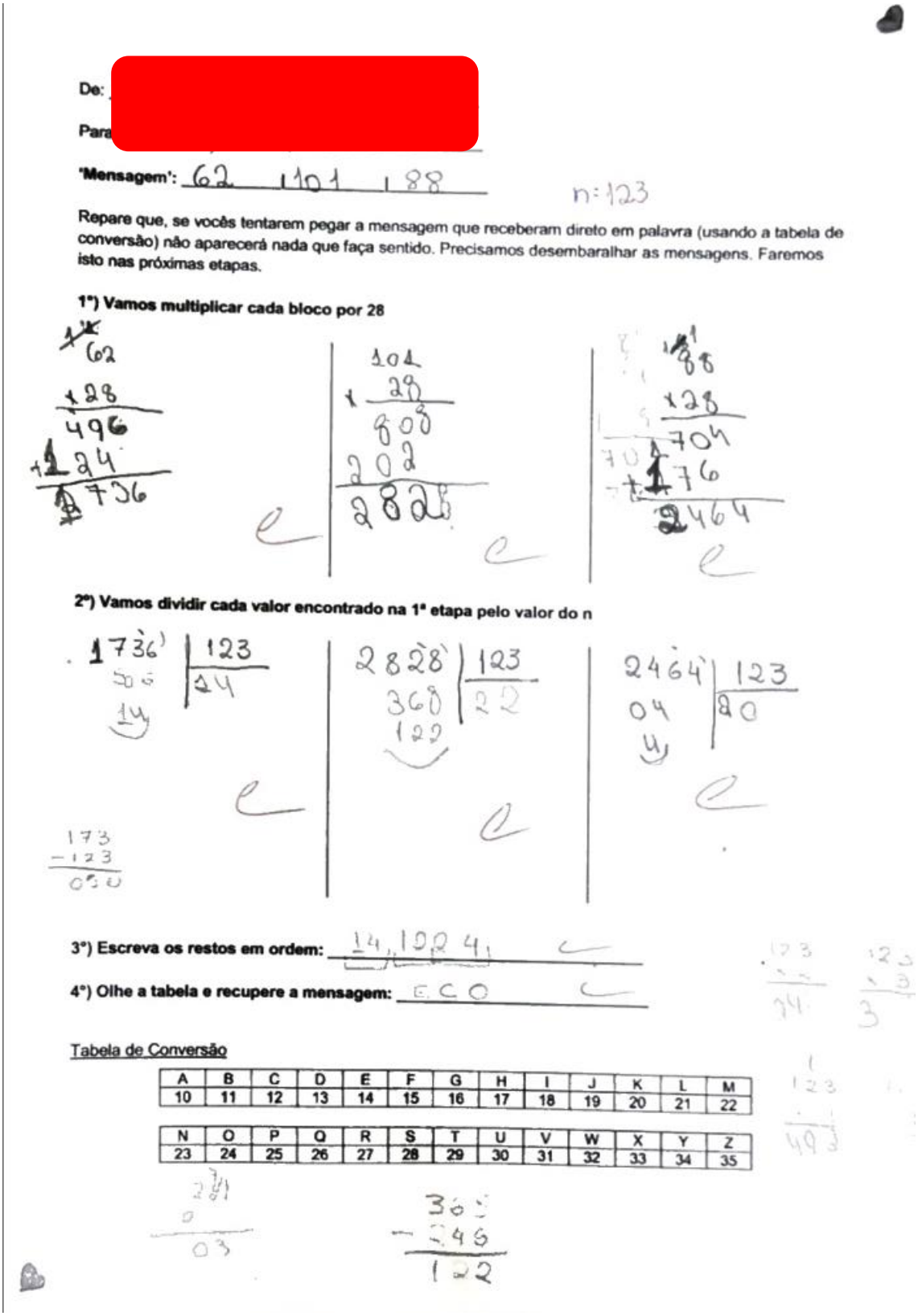
4ª) Vamos dividir cada valor encontrado na 3ª etapa pelo valor do n



123 × 2 = 246

268 − 246 = 022

224 − 123 = 101



De: [redacted]

Para [redacted]

'Mensagem': 62 101 88

n: 123

Repare que, se vocês tentarem pegar a mensagem que receberam direto em palavra (usando a tabela de conversão) não aparecerá nada que faça sentido. Precisamos desembaralhar as mensagens. Faremos isto nas próximas etapas.

1°) Vamos multiplicar cada bloco por 28

62 × 28 = 1736

101 × 28 = 2828

88 × 28 = 2464

2°) Vamos dividir cada valor encontrado na 1ª etapa pelo valor do n

1736 | 123 → 14

2828 | 123 → 22

2464 | 123 → 20

173 − 123 = 050

3°) Escreva os restos em ordem: 14, 122, 41

4°) Olhe a tabela e recupere a mensagem: E C O

Tabela de Conversão

A	B	C	D	E	F	G	H	I	J	K	L	M
10	11	12	13	14	15	16	17	18	19	20	21	22

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
23	24	25	26	27	28	29	30	31	32	33	34	35

Folha 2 – do trio A para o trio B

Nas outras duplas, erros bobos, ou de quem enviava a mensagem ou de quem recebia a mensagem, fizeram com que não chegassem a palavra correta.

3.6 Relato da Atividade na Escola Particular

A atividade foi aplicada ao final do 3º ciclo, no ano de 2018, momento que os alunos já haviam visto em sala tanto o algoritmo da multiplicação, quanto o da divisão. Havia 43 alunos na turma no dia da aplicação.

Foi feito um breve resumo do que se tratava a atividade. Foi dito que tinha a ver com criptografia, foi perguntado aos alunos se algum deles sabia o que significava criptografia. Uns três alunos deram respostas coerentes do tipo “É uma forma de escrever em códigos”. Após isto, foi explicado que criptografia é como se colocássemos uma mensagem dentro de um baú com cadeado (CODIFICAÇÃO) e só quem possuísse a chave do cadeado poderia ler (DECODIFICAR) a mensagem.

Após esta breve explicação foi dito que os alunos iriam codificar uma palavra e receber outra palavra para decodificar.

Eles se mostraram empolgados com a proposta. No decorrer da atividade, os alunos que estavam na 2ª folha (DECODIFICAÇÃO) e não conseguiam achar a palavra ficavam chateados e me chamavam para ver se havia algum erro em contas. Em alguns casos, sinalizei qual conta estava com problema, em outros, o problema havia sido na mensagem recebida, que estava errada, não havendo muita coisa a ser feita.

Da mesma forma que foi feito na escola municipal, a atividade foi realizada em duplas/trios com metade deles recebendo uma palavra, BOA, e a outra metade recebendo outra palavra, ECO. Grande parte da turma conseguiu concluir a atividade no tempo proposto, dois tempos de aula.

3.7 Comparando Resultados

Após a aplicação da atividade nas duas redes, fiz uma análise da atividade, identificando os erros que apareceram. Classifiquei os erros em 8 tipos:

- ERRO TIPO 1 → Algoritmo da multiplicação
- ERRO TIPO 2 → Algoritmo da multiplicação (tabuada)
- ERRO TIPO 3 → Algoritmo da multiplicação (soma)
- ERRO TIPO 4 → Algoritmo da divisão
- ERRO TIPO 5 → Algoritmo da divisão (subtração)
- ERRO TIPO 6 → Não identificável
- ERRO TIPO 7 → Falta de atenção

- ERRO TIPO 8 → Algoritmo da divisão (tabuada)

Na escola do município, houve um total de 12 duplas/trios. Na escola particular, houve um total de 15 duplas/trios.

No município, das 12 duplas/trios, 2 não conseguiram ir para a etapa da DECODIFICAÇÃO. Desses 2, uma dupla/trio teve dificuldade no algoritmo da multiplicação, não conseguindo nem concluir a folha de CODIFICAÇÃO, e a outra concluiu a folha de CODIFICAÇÃO, mas não teve tempo de ir para a folha de decodificação.

Já na escola particular, apenas uma dupla/trio não conseguiu ir para a etapa de DECODIFICAÇÃO.

Abaixo, veremos uma tabela comparativa de erros e acertos em ambas escolas, separados por folha (1ª folha é a da CODIFICAÇÃO e a 2ª folha é a da DECODIFICAÇÃO)

Escola	Municipal		Particular	
	1ª folha	2ª folha	1ª folha	2ª folha
Erro tipo 1	1	0	1	0
Erro tipo 2	1	1	2	1
Erro tipo 3	0	1	0	1
Erro tipo 4	1	0	2	0
Erro tipo 5	0	1	3	0
Erro tipo 6	1	3	3	1
Erro tipo 7	0	1	2	2
Erro tipo 8	0	1	0	1
Acertaram tudo	6	-	5	-
Encontraram o resto correto ao final de todos os passos, mas o quociente está errado	2	-	0	-
Acertaram tudo e acharam a palavra (caso 1)	-	2	-	3
Acertaram tudo, mas não achou a palavra pois recebeu a mensagem com erro (caso 2)	-	1	-	5
Acertaram tudo, mas não acharam a palavra pois em algum trecho pegaram o quociente no lugar do resto (caso 3)	-	2	-	0
Não conseguiram finalizar, mas o que fizeram estava certo	-	0	-	1

Tabela indicativa de erros encontrados por folha

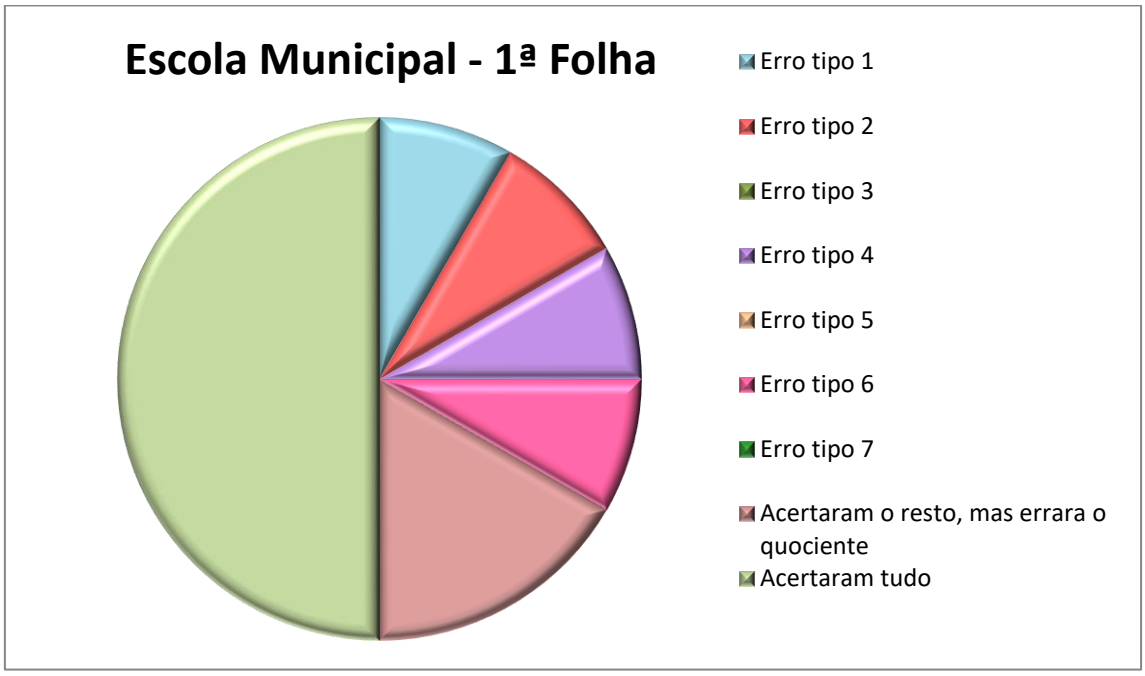
Na 1ª folha, os alunos do município não acumularam erros, ou seja, cada dupla/trio quando cometeu algum erro, cometeu apenas um tipo de erro na folha. Já na 2ª folha, alguns alunos acumularam erros, ou seja, cometeram dois tipos diferentes de erros.

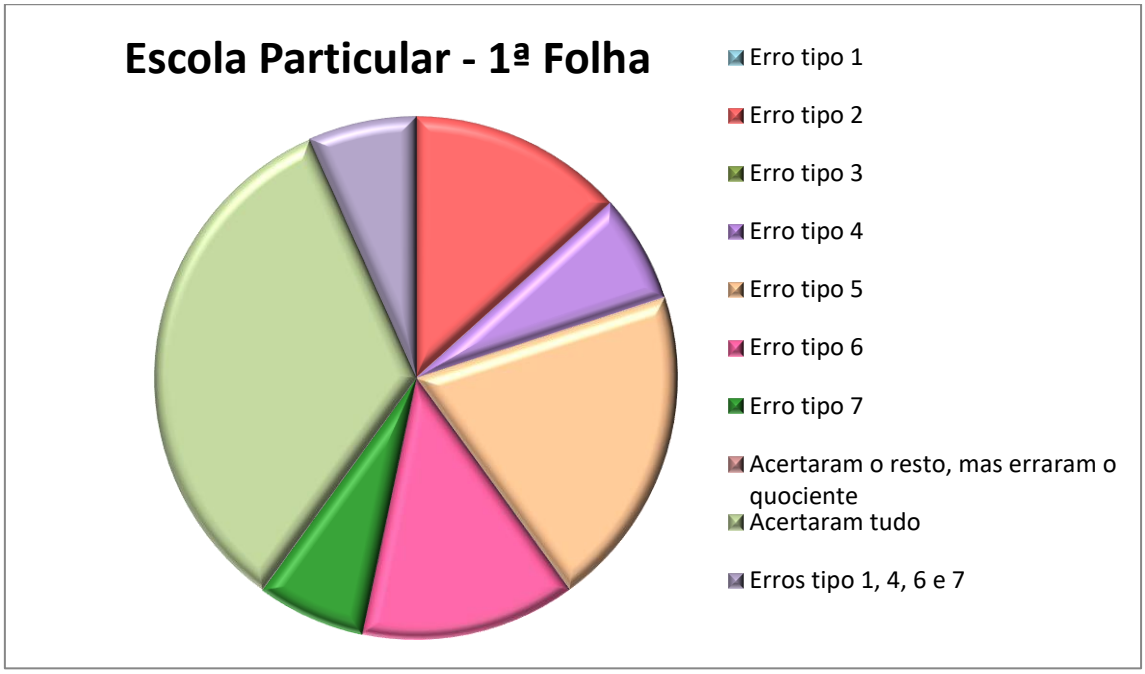
É interessante observar também que tais erros aconteceram apenas em um trecho, ou seja, das três multiplicações ou divisões que precisavam ser feitas, apenas uma delas continha algum problema. Isto pode ser pelo fato de que, como a atividade era feita em duplas/trios, os alunos podem ter dividido as tarefas entre si, cada um ficando responsável por fazer uma ou duas multiplicações/divisões.

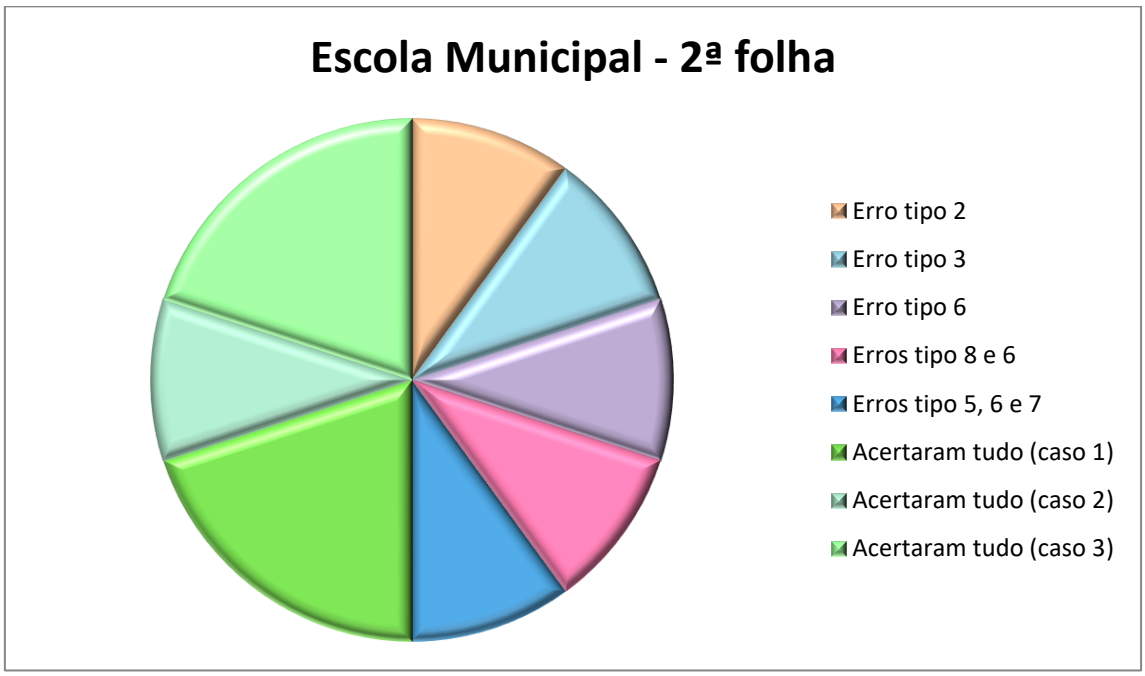
Observando agora os resultados obtidos na escola particular, na folha de CODIFICAÇÃO uma dupla/trio cometeu mais de um tipo de erro e na folha de DECODIFICAÇÃO outra dupla/trio cometeu mais de um tipo de erro. Da mesma maneira que aconteceu na escola pública, os erro não ocorreram em todos os blocos, o que demonstra que provavelmente os alunos dividiram as tarefas entre si, ficando cada um responsável por uma multiplicação e uma divisão.

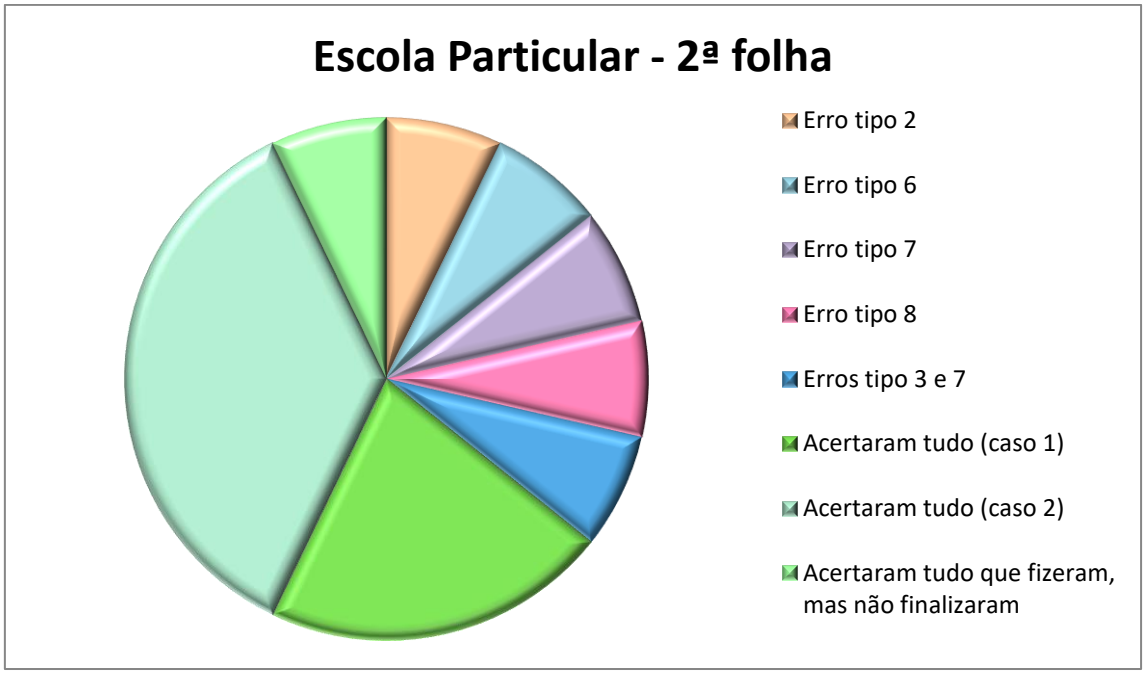
Como na escola particular grande parte dos que terminaram primeiro a primeira etapa (CODIFICAÇÃO) estavam com a mesma palavra, não tendo como trocar mensagens entre si, eu codifiquei a palavra que eles deveriam receber, para que não ficassem muito tempo ociosos.

Nos gráficos abaixo, podemos fazer um comparativo dos resultados com relação às duplas/trios que participaram das atividades em ambas as escolas.




Escola Particular - 1ª Folha
Erro tipo 1
Erro tipo 2
Erro tipo 3
Erro tipo 4
Erro tipo 5
Erro tipo 6
Erro tipo 7
Acertaram o resto, mas erraram o quociente
Acertaram tudo
Erros tipo 1, 4, 6 e 7

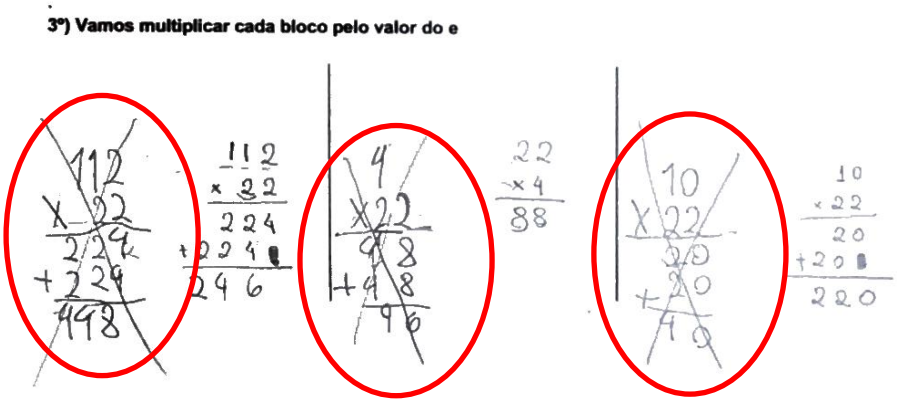

Escola Municipal - 2ª folha
Erro tipo 2
Erro tipo 3
Erro tipo 6
Erros tipo 8 e 6
Erros tipo 5, 6 e 7
Acertaram tudo (caso 1)
Acertaram tudo (caso 2)
Acertaram tudo (caso 3)



Podemos observar que, em média, a quantidade de erros e acertos foi muito próxima tanto em uma escola, quanto na outra. Todavia, os alunos da escola municipal precisaram de um tempo maior, quase 4 tempos de aula, para finalizar a atividade, além de terem mostrado uma dependência muito grande durante a execução da atividade. Mesmo com as frases explicativas, eles me chamavam para explicar o que deveria ser feito. Os alunos da escola particular foram bastante independentes durante a atividade, fazendo com que fosse necessário apenas 2 tempos de aula. Muitos nem esperaram eu dar todas as instruções iniciais para prosseguir. Um fato comum aos discentes de ambas as instituições foi a estranheza ao se deparar com divisão onde o dividendo era menor que o divisor. Eles não sabiam como lidar com tal situação, que precisou ser explicada aos alunos, tanto da escola municipal, quanto da escola particular.

Para exemplificar os tipos de erro, mostro, abaixo, fotos de trechos da atividade feita pelos alunos.

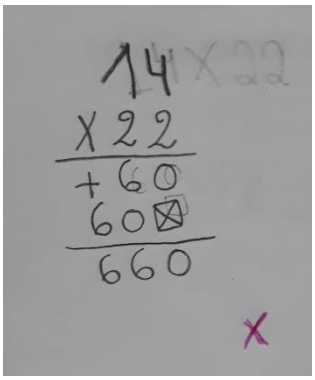
- Erro tipo 1 (O que está circulado foi o que a dupla/trio havia feito, o que não está circulado fui eu que fiz para explicar a dupla/trio)



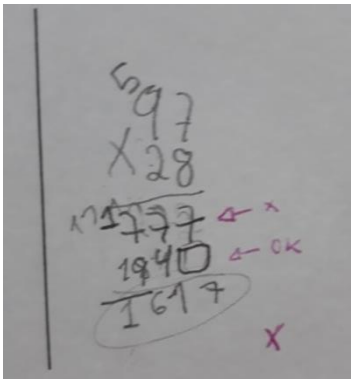
Erro encontrado na 1ª folha

A dupla/trio ainda tem dificuldades com relação a parte posicional do algoritmo da multiplicação.

- Erro tipo 2



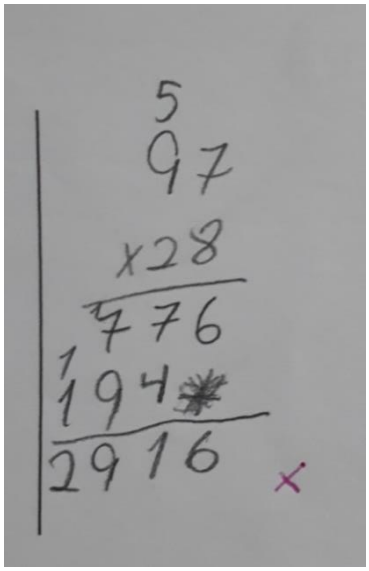
Erro encontrado na 1ª folha



Erro encontrado na 2ª folha

No primeiro exemplo, a dupla/trio errou todas as multiplicações. Já no segundo exemplos, vemos que o erro foi apenas na hora de multiplicar 8x7, que a dupla/trio fez 8x7=57 ao invés de 8x7=56.

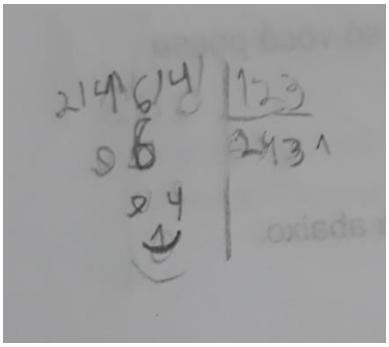
- Erro tipo 3



Erro encontrado na 2ª folha

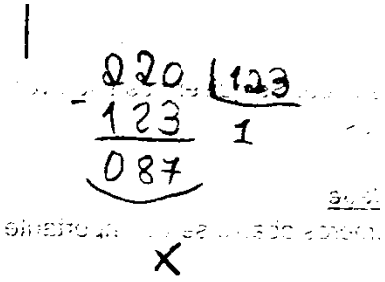
A dupla/trio fez 1+7+9=19 ao invés de 1+7+9=17.

- Erro tipo 4



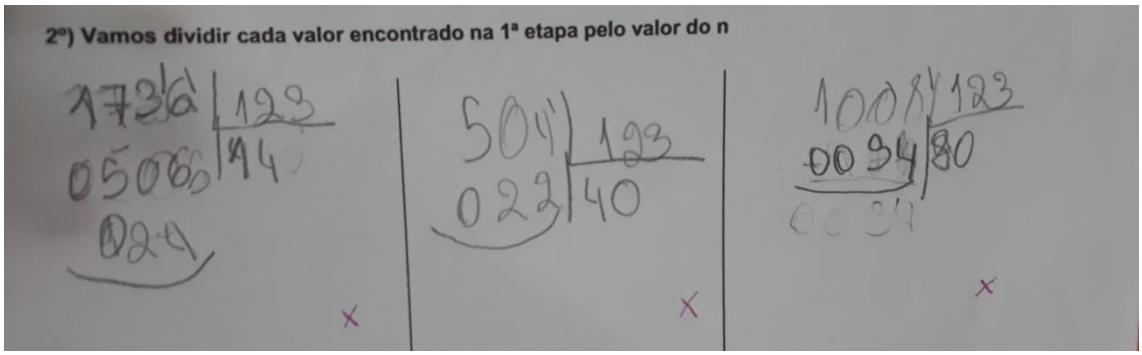
Aparentemente esta dupla/trio fez a divisão algarismo a algarismo, fazendo uma relação do primeiro algarismo do dividendo, com o primeiro algarismo do divisor (fazendo assim 2÷1=2). Após segundo algarismo do dividendo, com o primeiro algarismo do divisor (fazendo assim 4÷1=4). Na sequência, terceiro algarismo do dividendo com o segundo algarismo do divisor (fazendo assim 6÷2=3). Por fim, quarto algarismo do dividendo com o terceiro algarismo do divisor (fazendo 4÷3=1 com resto 1). Claramente o algoritmo da divisão ainda não foi dominado por eles.

- Erro tipo 5



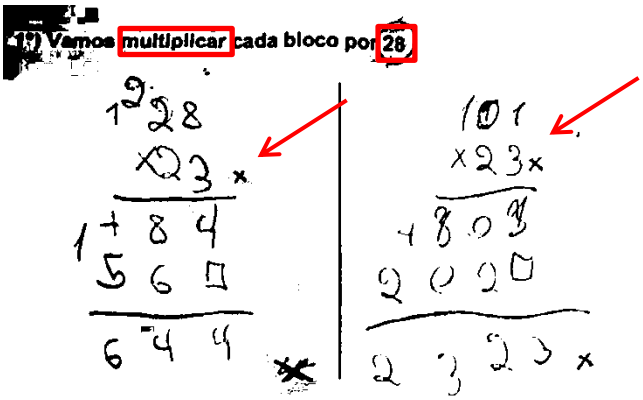
A dupla/trio cometeu um erro ao fazer 220-123=87 ao invés de 220-123=97.

- Erro tipo 6



No primeiro bloco, como o aluno não deixou a conta de multiplicação (4 x 123), nem a conta de subtração (506 – 492) não há como saber em qual etapa ele errou. Já no segundo e terceiro bloco, a mesma situação se repete além do aluno adicionar um zero ao lado esquerdo do 4 e 8, respectivamente, sem motivos.

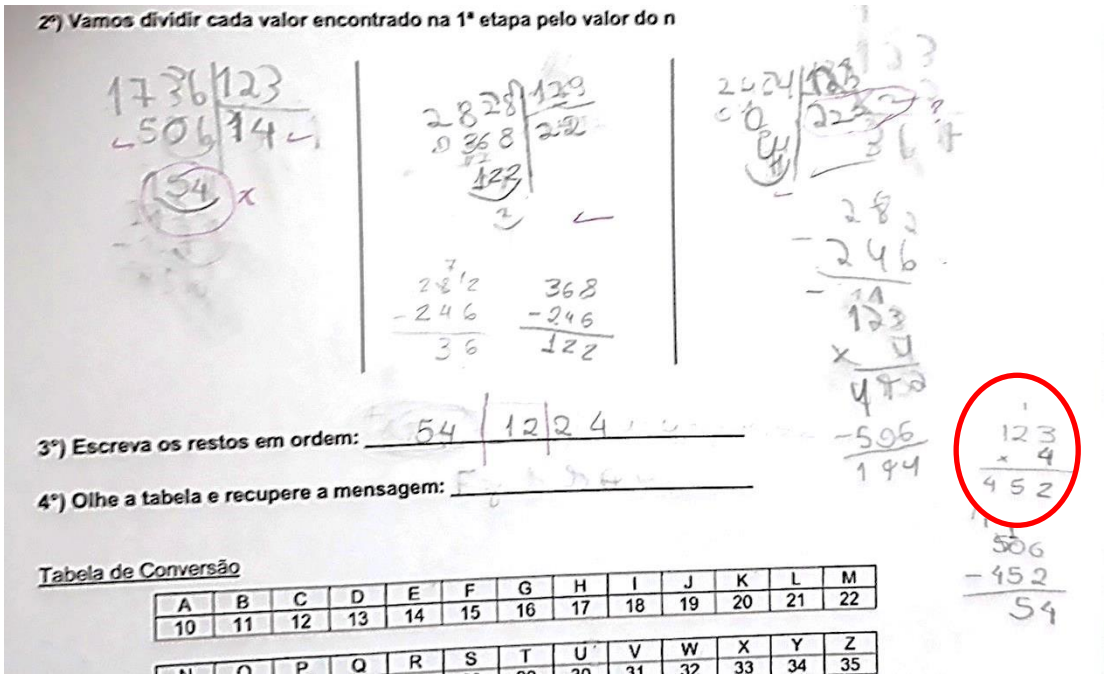
- Erro tipo 7



Erro encontrado na 2ª folha

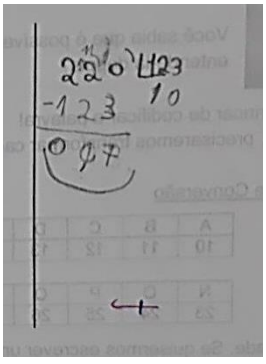
A dupla/trio multiplicou por 23, provavelmente confundido com o valor utilizado com divisor 123 (esquecendo do 1 da ordem das centenas), ao invés de usar o valor indicado na 2ª folha, que era 28.

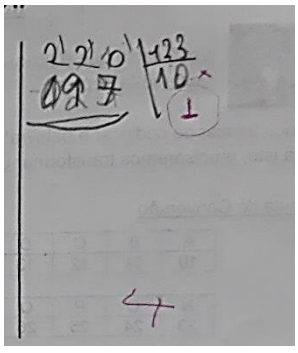
- Erro tipo 8



A dupla/trio errou na multiplicação de 123x4, eles encontraram como resultado 452 ao invés de 492.

- Acertaram o resto, mas erraram o quociente





Quis destacar este caso, pois mostra a dificuldade que os alunos têm com relação a quando se deve colocar o zero no quociente. (220 = 123 x 1 + 97)

3.8 Considerações

Podemos concluir que, em geral, mesmo com todas as dificuldades, alunos da escola municipal e da escola particular conseguem chegar com um mesmo nível de compreensão dos algoritmos no 6º ano do Ensino Fundamental. O que os diferencia é a autonomia e a agilidade. Por terem mais recursos e mais tempo para fazer exercícios em sala de aula, os alunos da escola particular ganham uma independência maior na execução das atividades enquanto que os alunos da rede municipal ainda são muito dependentes, precisando de uma explicação verbal do que já está explicado de forma escrita. A agilidade dos alunos da escola particular em resolver o que foi proposto acaba sendo uma consequência da maior autonomia deles.

Com relação à situação de um quantitativo pequeno encontrar a palavra final, tem-se o fato de que não pode haver nenhum erro em nenhuma conta, em nenhuma etapa, o que é bem complicado de se exigir de uma criança/adolescente, tendo em vista que sempre acontece uma falta de atenção que gera algum dos erros expostos.

Aproveito para deixar algumas sugestões. As três versões apresentadas podem ser utilizadas, cabe ao professor fazer uma análise do nível de dificuldade de cada uma para saber se está adequado ao nível de sua turma, uma vez que esta é uma atividade que pode ser feita em qualquer ano escolar. Essa atividade também pode ser feita com palavras maiores e até com frases, contudo, mais uma vez, fica a critério do professor verificar o que é melhor para sua(s) turma(s). Uma última sugestão, é que, ao invés de fazer os alunos codificarem uma palavra e decodificarem outra palavra, que eles apenas recebam palavras para decodificar e que se use o tempo que seria gasto na codificação com uma explicação um pouco mais detalhada sobre o que é criptografia, podendo usar uma apresentação de slides e citando a Cifra de César.

Capítulo 4: VISÕES PEDAGÓGICAS E HISTÓRICAS SOBRE MULTIPLICAÇÃO E DIVISÃO

Neste capítulo, abordaremos reflexões sobre as dificuldades encontradas pelos alunos com as operações de multiplicação e divisão. Além disto, mostraremos alguns algoritmos que surgem durante a história da matemática, comentando um possível uso dos mesmos nas salas de aula.

Essas discussões/reflexões são de extrema importância, tendo em vista que alguns alunos chegam ao sexto ano ainda tendo dificuldade com estas operações, fazendo-se necessário que tentemos outras abordagens, diferentes das usuais.

4.1 No contexto da sala de aula

Tradicionalmente, a matemática traz uma carga negativa de ser a matéria mais difícil, sendo a mais odiada. Isto muitas das vezes surge enquanto as crianças ainda estão nos anos iniciais, seja por influência das professoras, seja por influencia dos pais ou ambos. Às vezes esse sentimento vem no segundo segmento do ensino fundamental, quando há uma transformação, a matemática deixando o lado lúdico e sendo totalmente teórica, baseando-se em conceitos, algoritmos e exercícios, sem que haja uma transição suave entre esses dois mundos.

> Mesmo sabendo que o sujeito, como ressalta Brasil (1997, p. 55) 'À medida que se deparar com situações-problema - envolvendo adição, subtração, multiplicação, divisão, potenciação e radiciação -, ele irá ampliando seu conceito de número', muitas vezes este se depara com o ensino de uma prática repetitiva, que se tratando das operações matemáticas não refletem e nem absorvem seus significados, dificultando sua compreensão, desde cedo, das propostas de cálculos que envolvem essas situações.
>
> (PIRES; ABRANTES; BORBA, 2013)

Esse sentimento de repulsa acaba por bloquear o aprendizado dos alunos, que passam a nem se esforçar para tentar compreender o mínimo. Além disso, há uma orientação curricular que exige que transmitamos uma quantidade enorme de conteúdo em um espaço de tempo, muitas vezes, curto, fazendo com que acabemos por escolher entre cumprir o cronograma proposto ou fazer com que todos os alunos cheguem aos objetivos propostos, tendo em vista que cada aluno tem seu próprio tempo de aprendizagem.

> A aprendizagem da Matemática, assim como de outros conceitos, envolve processos que, apesar de inerentes ao funcionamento da inteligência, desenvolvem-se conforme as solicitações ambientais, o que faz com que existam diferenças individuais na compreensão de novos conceitos, tornando necessário, portanto, levar em consideração os esquemas disponíveis, assim como o ritmo de aprendizagem de cada um.
>
> (TEIXEIRA, 2004 APUD ZATTI; AGRANIONIH; ENRICONE, 2010)

E por muitas vezes professores acabam por escolher o cronograma, pelos mais diversos motivos, e diversos alunos vão ficando cada vez mais para trás.

Analisando o conteúdo específico a ser tratado neste capítulo, segundo Swetz (1987), divisão era considerada a operação mais difícil de ser ensinada e a mais difícil de ser compreendida pelos estudantes, por pelo menos 500 anos e cita Pacioli:

> “if a man can divide well, everything else is easy, for all the rest is involved therein.””
>
> (*Suma de arithmetica, geometria, proportioni et proportionalita*, Lucas Pacioli apud Swetz 1987, p.212)

Nesse trecho, Pacioli basicamente diz que se um homem sabe dividir, qualquer outra coisa será fácil. Ou seja, os problemas dos estudantes, principalmente com relação à divisão, remontam de longa data, não são problemas exclusivos da atualidade.

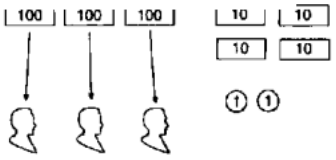
No contexto da multiplicação e da divisão, tem-se dois algoritmos “mágicos” e nada intuitivos, num primeiro momento, a uma criança na faixa etária dos 7 anos, quando tais algarismos são introduzidos. O que é sugerido na literatura é que se trabalhe com essas crianças o lúdico. Pode-se até traçar um paralelo com elas entre o lúdico e o algoritmo, de modo que o aprendizado dos algoritmos não seja tão mecânico e sem sentido como pode ser visto a seguir em uma sugestão para divisão.

EXAMINANDO UMA CONTA DE DIVIDIR

Considere a conta **3 4 2 ÷ 3.**

Todos nós sabemos efetuá-la, mas, nem sempre sabemos o porquê de cada passagem da conta. Para facilitar o entendimento desse algoritmo, vamos imaginar que o número 342 corresponde a 342 reais em 3 notas de cem reais, 4 notas de dez reais e 2 moedas de um real. Veremos, então, que dividir 342 por 3 é bastante parecido com a ação de repartir a quantia de 342 reais entre 3 pessoas. Acompanhe.

Para repartir o dinheiro, começamos dividindo as 3 notas de cem.

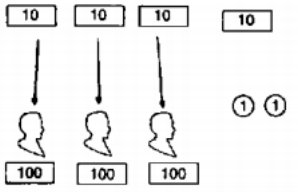


Na conta, dividimos 3 centenas por 3, resultando 1 centena, sem deixar resto.

3 4 2 | 3
0 1

11

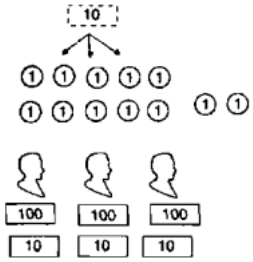
Depois, repartimos as 4 notas de dez. Agora, sobrará uma nota.



Na conta, dividimos as 4 dezenas por 3. Restará 1 dezena.

3 4 2 | 3
0 1 1 1

Para dividir a nota de dez que restou, devemos trocá-la por 10 moedas de um real. Teremos 12 reais, no total.



Na conta, descemos o algarismo 2. Isso corresponde a juntar aquela dezena que restou com as duas unidades, resultando 12 unidades.

3 4 2 | 3
0 1 2 1 1

Agora pode-se completar a repartição do dinheiro. Dividindo as 12 moedas, cada pessoa recebe 4. No final, cada uma ficou com 114 reais.

Encerramos a conta dividindo 12 unidades por 3, o que dá 4. O resultado final é 114.

(IMENES, 1996, P.11 e P.12)

Podem-se encontrar também sugestões para que os alunos sejam motivados a criar suas próprias estratégias para resolução antes que se ensine o algoritmo em si.

> No caso do algoritmo, acreditamos que os alunos devem ter oportunidade de expor suas ideias de representação e criar quem sabe suas próprias formas de resolução. Quando, por exemplo, a professora propõe que as crianças resolvam a seu modo a multiplicação 14 x 12 e que em seguida demonstrem para o restante da turma as diferentes formas a que conseguiram chegar, pode obter soluções interessantes que poderiam ter sido suprimidas se não tivesse dado a oportunidade para que as crianças exercitassem seu pensamento autônomo. Do mesmo modo, esse tipo de atividade mostra-se fundamental para o processo de construção do

> algoritmo habitual que começa a ser utilizado pelas crianças naturalmente, sem imposições.
>
> (SOUZA, 2010)

Ainda sobre a vivência individual do aluno de criar suas próprias estratégias, o PCN também destaca a importância de tal atitude.

> Assim como outros procedimentos de cálculo, as técnicas operatórias usualmente ensinadas na escola também apóiam-se nas regras do sistema de numeração decimal e na existência de propriedades e regularidades presentes nas operações. Porém, muitos dos erros cometidos pelos alunos são provenientes da não-disponibilidade desses conhecimentos ou do não-reconhecimento de sua presença no cálculo. Isso acontece, provavelmente, porque não se exploram os registros pessoais dos alunos, que são formas intermediárias para se chegar ao registro das técnicas usuais.
>
> (BRASIL,1998, p.78)

Quando os alunos chegam ao 6º ano do ensino fundamental, espera-se que os mesmos já tenham dominado tais algoritmos e que só seja necessário recordar e cobrar um nível de dificuldade um pouco maior em uma questão ou outra. Mas a complexidade dos algoritmos é tão grande para alguns alunos, que multiplicações e divisões mais básicas podem ainda ser difíceis para eles. Tal angústia se apresenta em séries anteriores também.

Batista (1995), em sua pesquisa em turmas de 2ª série a 4ª série (equivalentes ao 3º ano até 5º ano), observou um grande percentual de erros quando a multiplicação é feita por números com duas ordens e na divisão o percentual de erros é alto independente da divisão ser feita por número de uma ordem ou de duas ordens.

Porcentagem de acertos e erros dos alunos de 2ª, 3ª e 4ª séries em operações aritméticas.

OPERAÇÕES ARITMÉTICAS	2ª série AC	ER	NF	TOT	3ª série AC	ER	NF	TOT	4ª série AC	ER	NF	TOT
SOMA												
s/ "vai um"	86,4%	9,1%	4,5%	**22**	*	*	*		-	-	-	
c/ "vai um	40,7%	52,2%	7,1%	**113**	62,9%	29,5%	7,6%	**105**	86,7%	13,3%	0,0%	**90**
SUBTRAÇÃO												
s/ "emprestar"	64,1%	28,1%	7,8%	**64**	*	*	*		-	-	-	
c/ "empréstimo"	21,7%	65,2%	13,1%	**46**	37,9%	57,9%	2,2%	**45**	72,2%	25,0%	2,8%	**36**
MULTIPLICAÇÃO												
p/ unidade	53,6%	36,4%	10,0%	**110**	70,8%	26,8%	2,4%	**41**	68,4%	31,6%	0,0%	**19**
p/ dezena	*	*	*		9,2%	55,3%	35,5%	**76**	44,9%	49,4%	5,7%	**87**
DIVISÃO												
p/ unidade	*	*	*		48,0%	42,0%	10,0%	**50**	-	-	-	
p/ dezena	-	-	-		-	-	-		37,5%	50,0%	12,5%	**16**

* Totais muito baixos para cálculo de porcentagem.
- Não foi aplicada nessa turma.
AC-acertos **ER**-erros **NF**-não fez **TOT**-total

(Batista, 1995, p.63)

Sobre tal pesquisa, Batista diz ainda:

> Conforme se observa na Tabela I, os acertos em cada tipo de operação aritmética tendem a aumentar à medida que o aluno avança na escolaridade. Entretanto, o total de erros por série é bastante alto em relação às expectativas de desempenho previstas nas propostas curriculares (CENP, 1988). Assim é que foram constatados os seguintes percentuais de erros; [...] Verifica-se, assim que os erros se concentram em operações mais complexas, tais como: [...] multiplicação e divisão por números com dois algarismos. Parece, portanto que o problema não reside na compreensão da operação em si, mas na realização do cálculo em situações de maior complexidade.
>
> (Batista, 1995, p.63)

O que se discute, em diversos trabalhos e pesquisas, é que essa grande dificuldade com os algoritmos se dá pelo fato de serem algoritmos que levam em consideração o valor posicional dos números. Para o aluno que está aprendendo, o “vai um” que aparece em somas e multiplicações, nesta última podendo ser um “vai dois”, “vai três” etc, é só mais um mecanismo ensinado pelo(a) professor(a) e este, por muitas vezes, por ser formado em pedagogia e não ter um estudo aprofundado em matemática, não compreende o que está por trás do “vai um”. Analisemos a conta a seguir:

$$\begin{array}{r} {\scriptstyle 1} \\ 23 \\ \times\ \ 5 \\ \hline 115 \end{array}$$

O “vai um” que aparece é uma dezena que não foi ainda usada na conta decorrente da decomposição do resultado 5x3 = 15 = 10 + 5, onde o 5 permanece na posição das unidades e a dezena fica “esperando” poder ser usada.

Já na divisão, temos que repartir grupos maiores e o que resta transformar em grupos menores (como sugerido em Conversa de professor – matemática), que também passa pela questão do valor posicional do número, vejamos:

$$\begin{array}{r|l} 22'7 & 3 \\ \cline{2-2} 17 & 75 \\ \quad 2 & \end{array}$$

Começamos dividindo 22 dezenas por 3 que resulta em 7 dezenas e sobra 1 dezena, transformamos essa uma dezena em 10 unidades e unimos com as 7 unidades que tínhamos, passando a ter 17 unidades. Dividimos essas 17 unidades por 3 que resulta em 5 unidades e sobram 2 unidades.

Ou seja, os problemas com os algoritmos comumente apresentados aos alunos passam pela ausência de explicação do significado dos mesmos, que é totalmente baseado no sistema de numeração posicional decimal.

> Outra questão a considerar é que a compreensão dos algoritmos tradicionais das quatro operações exige o domínio das propriedades do sistema de numeração decimal, compreensão considerada tardia pela literatura (KAMII, 1996). Infere-se, portanto, que muitos erros cometidos pelos alunos podem ser devidos ao descompasso entre o tempo em que esses algoritmos são ensinados na escola e o tempo próprio de cada criança para a compreensão dos mesmos.
>
> (ZATTI; AGRANIONIH; ENRICONE, 2010)

Neste ponto, cabem aqui alguns questionamentos: ‘*Será que não poderíamos ensinar outros algoritmos aos alunos, cabendo aos mesmo decidir qual é o melhor para si?’, ‘Para os alunos com maior dificuldade, o uso da calculadora não seria interessante?’, ‘Deixar a tabuada afixada em algum lugar visível a todos os alunos pode ajudar no processo?’*

A calculadora, em certo momento, poderia ser útil para dar segurança aos alunos, sendo esta usada para mera conferência. A tabuada afixada entra como

auxiliar da mesma forma que a calculadora, sendo que o uso desta pode ser feito a qualquer momento, evitando os erros devido ao fato de não terem a tabuada decorada (alguns alunos compreendem o algoritmo, mas ainda não tem a tabuada decorada, nem conseguem construir a mesma, e se enrolam nas contas por conta disto). Podemos até nos questionar da necessidade de ter a tabuada decorada desde cedo, mas deixaremos este questionamento para o leitor refletir. Na próxima seção, traremos a discussão sobre os algoritmos.

4.2 No contexto histórico

Antes de analisarmos algoritmos diversos, cabe recuperar as definições mais primitivas das operações de multiplicação e divisão, uma vez que muitos dos algoritmos que veremos fazem parte da história de matemática.

4.2.1 Multiplicação

Historicamente, a multiplicação era definida mais ou menos com a mesma ideia utilizada com as crianças, que é uma definição que vale para inteiros positivos. O que se mostra para as crianças é:

$$m.n = n + n + ... + n, \text{ com } m \text{ parcelas iguais a } n \text{ e } m, n \in \mathbb{N}$$

As definições mais antigas, como a encontrada no The Crafte of Nombrynge (ano de 1300 aproximadamente), citada por alguns autores como Swetz e Smith, são um pouco mais complicadas pois geram um ciclo onde a definição de multiplicação está embasada na definição de divisão e vice-versa, mas também traz na sua essência o que é passado para as crianças nas séries iniciais e que foi escrito acima.

> “multiplicacion is a bryngynge to-geder of 2 thynges in on nombor, the quych on nombor contynes so mony tymes on, howe mony tymes bem vyntees in the nowmbre of that 2”
>
> (The Crafte of Nombrynge apud SWETZ, 1989)

Swetz diz que a ideia por traz deste trecho é a seguinte:

“Para entender multiplicação é necessário saber que multiplicar um número por si mesmo ou por outro é encontrar, dados dois números, um terceiro que contenha um desses números tantas vezes quanto a unidade cabe no outro”

(SWETZ, 1989, tradução da autora)

Por exemplo, 3x10 = 30, uma vez que o 10 cabe 3 vezes dentro do 30, da mesma forma que o 1 cabe 3 vezes no 3. Fica um pouco mais claro, com o exemplo, o fato da definição de multiplicação ter embutida a definição de divisão, como comenta Swetz:

“This definition is slightly circular, in that in its explanation it refers to the process of division; however, its essence lies in the realization that multiplication, *motiplicare*, may be viewed as repeated addition.”

(SWETZ, 1989)

Traduzindo o que Swetz diz temos:

Esta definição é ligeiramente circular, uma vez que na sua explicação há referência ao processo de divisão; entretanto, sua essência se encerra na realização de que multiplicação pode ser vista como repetidas adições.

Alguns autores fazem críticas ou ainda fazem um alerta com relação a se definir a multiplicação como adição de parcelas iguais, como pode ser visto em Souza, 2010:

“Há uma prática comum nas salas de aula que apresenta a multiplicação somente do ponto de vista de ‘adição de parcelas iguais’, [...], ela não pode ser difundida como única”

(Souza, 2010)

Mas não é um absurdo querer usar tal definição para multiplicação ao se introduzir tal conteúdo, pelo menos dentro do conjunto dos números naturais, tendo em vista que, historicamente, esta foi uma das primeiras definições.

Vejamos agora alguns dos algoritmos de multiplicação encontrados ao longo da história.

4.2.1.1 Método Egípcio (Bunt; Jones; Bedient, 1988, p.11)

Os egípcios utilizavam um método de dobrar os números para depois somar os que fossem úteis. Vejamos o funcionamento do método egípcio através de um exemplo:

41 x 54

\	1	54
	2	108
	4	216
\	8	432
	16	864
\	32	1728

Repare que colocamos o 1 ao lado do 54 e depois fomos só dobrando os valores. Paramos no 32 pois 41 = 32 + 8 + 1. Por isso as linhas que contém o número 1, 8 e 32 estão marcadas. Para obter o resultado da multiplicação desejada, basta somar os valores que aparecem ao lado dos valores 1, 8 e 32. Logo

$$41 \times 54 = 54 + 432 + 1728 = 2214$$

Observe que o que fizemos com o 41 foi escrevê-lo como uma soma de potências de 2. Ou seja, este método, traz por trás dele, saber escrever um dos dois fatores como sendo uma soma de potências de dois, isto é, conhecer sua representação binária.

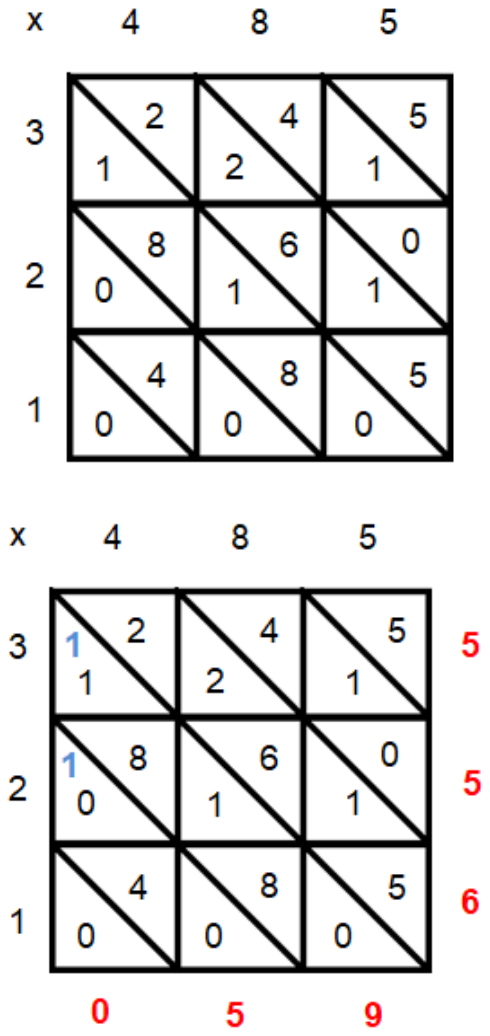
É um algoritmo interessante, mas não acredito ser útil como uma alternativa ao algoritmo que já conhecemos.

4.2.1.2 Gelosia (multiplicação árabe) (Boyer; Merzbach, 1989, p.242)

Neste método, coloca-se um fator na parte de cima do quadro e na lateral esquerda coloca-se o outro fator, escrevendo o número de baixo para cima. O número de cima determinará quantas colunas o quadro terá e o número da lateral determinará quantas linhas terá o quadro. Cada quadrado formado será dividido por uma diagonal, começando no canto superior esquerdo e terminando no canto inferior direito. Faz-se a multiplicação de cada número da linha por um número da coluna colocando seu resultado no quadrado correspondente à linha e à coluna trabalhada, sendo que a dezena ficará abaixo da diagonal e a unidade na parte de cima da diagonal do quadrado. Depois, somam-se os valores de cada diagonal e caso o

valor seja maior ou igual a 10, o algarismo da dezena é somado no resultado da próxima diagonal. O resultado final será lido da esquerda para direita e depois de baixo para cima.

Vejamos como funciona tal algoritmo através do seguinte exemplo: 123 x 485



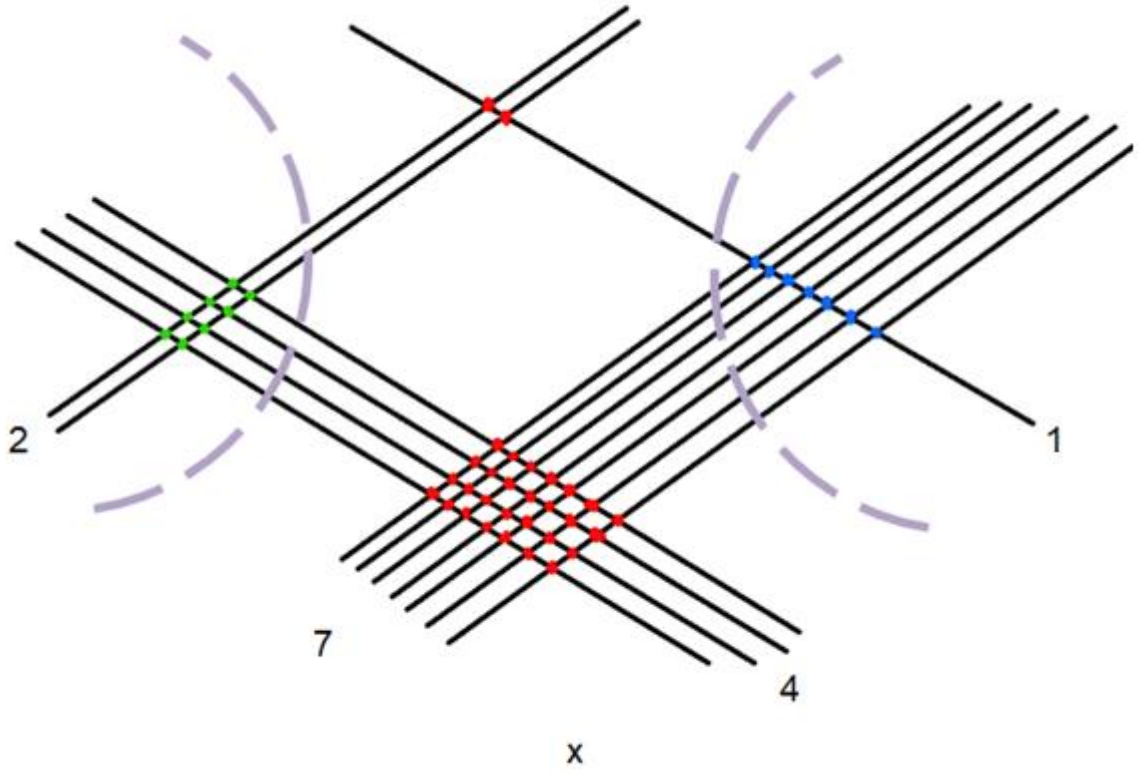
Por este algoritmo, chegamos ao resultado 123 x 485 = 59655. Existem variações com relação ao local em que se colocam o multiplicando e o multiplicador, o que influencia em como aparecerá o resultado.

Ele é simples, pois só é necessário por o resultado da multiplicação de dois algarismos nas respectivas casas e depois fazer somas em diagonal, começando pela diagonal superior do lado direito. Caso uma soma seja maior ou igual a dez, precisamos fazer o “vai um”, “vai dois”, etc.

Ele é parecido com o nosso, mas estruturado de uma forma diferente. É um método simples, que poderia ser ensinado sem problema algum para as crianças. Pode ser usado como uma opção para crianças que tenham dificuldade com o algoritmo comumente ensinado.

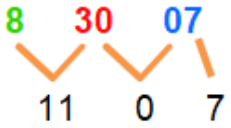
4.2.1.3 Multiplicação Chinesa (SOLDATELLI, 2016)

Os chineses utilizavam palitos de bambu para fazer as multiplicações. Para fazer 27 x 41, por exemplo, “arma-se” essa expressão no formato de um **V**, com os algarismos de cada número bem separados. Ao lado de cada algarismo, coloca-se a quantidade de bambus que representa aquele algarismo. Como na figura a seguir:



O sinal da multiplicação foi colocado na figura para ajudar na compreensão

Para encontrar o resultado, contamos as interseções dos bambus, de acordo com as cores.



Logo, 27 x 41 = 1107

Também é um método bem tranquilo para se apresentar às crianças, podendo ser uma alternativa para aquelas que encontram dificuldades com o método comumente ensinado.

4.2.2 Divisão

Divisão é a operação que encontra, dados dois números, um terceiro número que está contido no maior tantas vezes quanto a unidade está contida no menor. Por exemplo, 70 divididos por 35 dá 2, pois 35 está contido 2 vezes no 70, da mesma forma que o 1 está contido no 2 duas vezes. Esta é definição encontrada em *Treviso Arithmetic* (1478), como pode ser visto no capítulo 2 do livro Capitalism and Arithmetic de Frank J. Swetz. Cabe observar, que tal definição só é válida para os números naturais.

Da mesma forma que a multiplicação, as primeiras definições históricas não consideram outros conjuntos numéricos. A definição de divisão vai sendo atualizada, historicamente, conforme a necessidade, da mesma forma que se faz na escola.

Com relação aos algoritmos, a divisão não possui uma grande diversidade como a multiplicação. E estes são muito parecidos com o que se usualmente se apresenta aos alunos, mudando a forma de arrumar o passo a passo.

4.2.2.1 Método Egípcio (Bunt; Jones; Bedient; 1988, p.11 / Abe; Marcatto; 2007)

É bem parecido com o método da multiplicação. Utilizaremos multiplicações por 2 e divisões por 2. Vamos fazer 15 ÷ 4

\	1	4
\	2	8
	4	16
\	$\bar{2}$	2
\	$\bar{4}$	1

A notação $\bar{n}$ é usada para indicar $\frac{1}{n}$.

Repare que colocamos o 1 ao lado do 4 e depois fomos dobrando os valores até ultrapassar 15. Depois passamos a fazer divisões por 2, começando da primeira linha.

Paramos no $\overline{4}$ pois 15 = 4 + 8 + 2 + 1. Por isso as linhas que contém os números 4, 8, 2 e 1 estão marcadas. Para obter o resultado da divisão desejada, basta somar os valores que aparecem ao lado dos valores 4, 8, 2 e 1. Logo

1 x 4 + 2 x 4 + $\overline{2}$ x 4 + $\overline{4}$ x 4 = 15

(1 + 2 + $\overline{2}$ + $\overline{4}$) x 4 = 15

15 ÷ 4 = 1 + 2 + $\overline{2}$ + $\overline{4}$

Os egípcios também usavam multiplicar por 2 e dividir por 3.

Cabe reparar que no exemplo dado, a divisão não gera uma dízima periódica. Vejamos, como exemplo, 25÷7:

\	1	7
\	2	14
	4	28

Neste caso, não conseguiremos achar soma 25. O mais próximo que conseguimos chegar é 21 = 7 + 14. Logo, esta divisão terá resto 4 = 25-21. Quociente inteiro 3 = 1 + 2. Caso queira-se continuar, multiplica-se o resto por dez e divide-se por 7 (40 ÷ 7).

\	1	7
	2	14
\	4	28
	8	56

Neste caso, não conseguimos achar soma 40. O mais próximo que conseguimos chegar é 35 = 7 + 28. Quociente: 5 = 1 + 4 (5 décimos). Logo, tem-se resto 5. Para prosseguir, faz-se o resto vezes dez e divide-se por 7 (50 ÷ 7)

\	1	7
\	2	14

\ 4 28

8 56

Mais uma vez não será possível encontrar a soma desejada. O mais próximo que conseguimos será 49 = 7 + 14 + 28 e o resto será 1. Quociente: 7 = 1 + 2 + 4 (7 centésimos). Se pararmos por aqui, teremos:

25÷7 = 3, 57...

Como no caso da multiplicação feita pelos egípcios, é um algoritmo interessante, mas não acredito ser útil como uma alternativa ao algoritmo que já conhecemos.

4.2.2.2 Método Galley (Smith, 1958, p.136 a 138)

Este método recebe este nome por se assemelhar a um barco ao final de todo o processo.

"Galley: (in the past) a long, low ship with sails that was usually rowed by prisoners or slaves."

(Definição retirada de https://dictionary.cambridge.org/pt/dicionario/ingles/galley acessado em 5/8/2018)

Em uma livre tradução, temos que galley era um navio longo e baixo com velas que geralmente era remado por prisioneiro ou escravos.

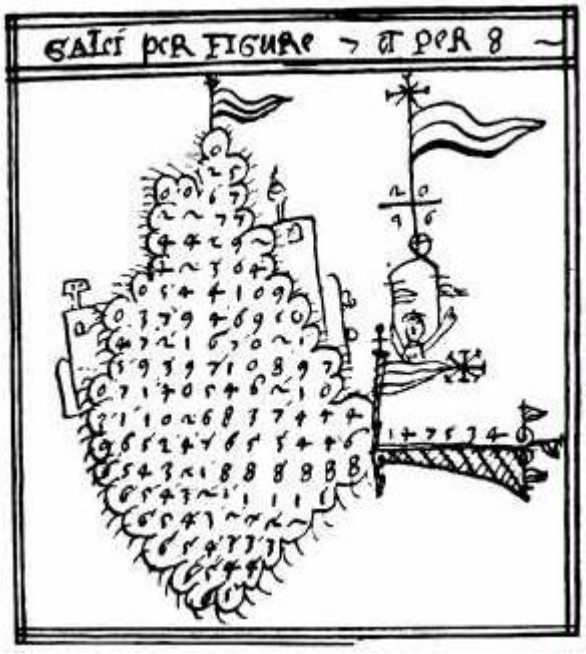


Ilustração de uma conta feita através do método Galley

É um método um pouco confuso, por isso, o demonstrarei passo a passo. Faremos, como exemplo, 4324 ÷ 31. Escrevemos o 4324, uma barra ao lado direito do número e, do lado direito da barra, construiremos o quociente. Começamos colocando o 31 embaixo do 43 e 1 do lado direito da barra, pois 1 x 31 = 31 é o valor que mais se aproxima de 43 sem ultrapassá-lo.

```
4324 | 1
31
```

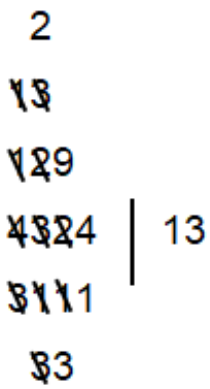
Agora faremos 4 – 3 x 1 = 1, colocaremos o resultado acima do 4 e cortaremos o 4 e o 3.

```
 1
4324 | 1
31
```

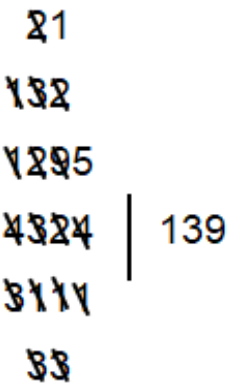
Consideraremos o número 13 (obtido com o 1 acima do 4 e com o 3 do lado do 4). Faremos 13 – 1 x 1 = 12, colocaremos o resultado acima do 13 e cortaremos o 13 e o 1. Colocaremos o 31 novamente abaixo dos números, deslocado em uma casa.

```
 1
12
4324 | 1
31
```

Repetiremos este processo até não termos mais o que dividir. Agora colocaremos o 3 ao lado do 1 que está no quociente. Faremos 12 – 3 x 3 = 3, colocaremos o resultado acima da unidade do 12 e cortaremos o 12 e o 3. Faremos 32 – 1 x 3 = 29, colocaremos o resultado acima do 32 e cortaremos o 32 e o 1. Colocaremos o 31 novamente abaixo dos números, deslocado em uma casa.



Agora colocaremos o 9 ao lado do 3 que está no quociente. Faremos 29 – 3 x 9 = 2, colocaremos o resultado acima das unidades do 29 e cortaremos o 29 e o 3. Faremos 24 – 1 x 9 = 15, colocaremos o resultado acima do 24 e cortaremos o 24 e o 1.



Sendo assim, 139 será o quociente da divisão e 15 o resto.

Definitivamente, este método não é interessante para mostrar aos alunos. Causaria ainda mais dúvidas.

4.2.2.3 Divisão por estimativa

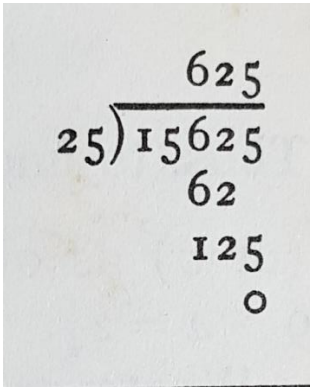
(http://portaldoprofessor.mec.gov.br/fichaTecnicaAula.html?aula=10553)

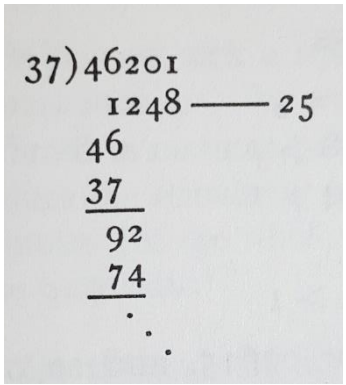
Neste método, pega-se um valor qualquer, desde que este não ultrapasse o dividendo na hora de multiplicar pelo divisor. Subtrai-se o valor da multiplicação pelo dividendo. Repete-se o processo com o que sobra da subtração quantas vezes forem necessárias. O quociente será a soma das estimativas. Vejamos o exemplo abaixo, da divisão de 479 por 31.

479	31
-310	10
169	+5
-155	15
14	

Temos então que na divisão de 479 por 31 o quociente é 15 e o resto é 14. Este método é interessante para aqueles com dificuldades no método comumente ensinado em sala de aula.

Ao longo da história, outros métodos apareceram, mas estes usavam exatamente a mesma ideia do método que utilizamos em nossas salas de aula, somente a forma de organizar cada membro da divisão que é diferente, como nos casos abaixo:





Imagens retiradas do livro History of Mathematics, DE.Smith

Em ambas as imagens, o divisor fica ao lado esquerdo do dividendo.

Na primeira, constrói-se o quociente acima do dividendo e coloca-se o resto de cada etapa da divisão (156 ÷ 25, 62 ÷ 25; 125 ÷ 25) abaixo do dividendo.

Na segunda, constrói-se o quociente abaixo do dividendo e o resto é colocado à direita do quociente. Logo abaixo do quociente, coloca-se os cálculos de cada etapa da divisão (46-37x1 = 9; 92 – 37x2 = 18; ...)

Após estas análises, vemos que, com relação à multiplicação, temos alguns algoritmos para dar suporte aos alunos com dificuldade. Todavia, com relação à

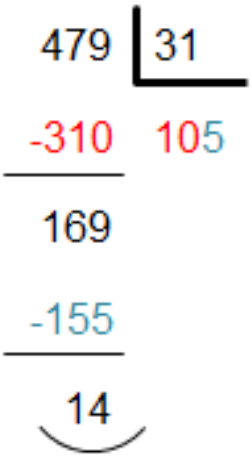
divisão, apesar de haver outros algoritmos, apenas um é um pouco mais simples do que o algoritmo comumente usado nas salas de aula, a divisão por estimativas.

CONCLUSÃO

O ensino das operações de multiplicação e divisão de números naturais é sempre apresentado em um mesmo formato, com os mesmos tipos de exercícios, que, ao longo do tempo, se tornam desinteressantes para as crianças pois todo ano elas veem mais do mesmo, tendo em vista que tais conteúdos são introduzidos no 3º ano e revisitados até o 6º ano. Contudo, para aqueles(as) alunos(as) que têm dificuldades, tais exercícios só causam mais frustração.

A atividade proposta neste trabalho traz algo novo, um desafio novo, podendo até ser apresentado como um jogo para os alunos. Tira os alunos da zona de conforto de fazer mais um exercício parecido com outros que já fizeram no 3º, 4º e 5º ano, e os instiga a retomar seus papéis questionadores. Na escola municipal, por exemplo, graças a esta atividade, fui capaz de identificar alunos com dificuldades sérias que, com os exercícios do caderno pedagógico fornecido pela Secretaria Municipal de Educação do município do Rio de Janeiro feitos antes de aplicar tal atividade, não consegui identificar.

Ao longo do estudo que fiz para este trabalho, pude compreender que a deficiência no aprendizado com relação ao algoritmo da divisão, que é o mais crítico para os alunos, é de longa data. Os diferentes métodos para se resolver multiplicação e divisão encontrado na história da matemática e aqui apresentados no capítulo 4, nos mostram algumas alternativas a se trabalhar em sala, principalmente com aqueles alunos com maior dificuldade. Dos alunos que já passaram por mim, muitos acabavam tentando resolver divisões, de modo intuitivo para eles, pelo método da estimativa. Contudo, por falta de uma formalização do método em sala de aula, eles misturam a intuição com o método que aprenderam, obtendo um resultado errado. O exemplo da seção 4.2.2.3, seria resolvido da seguinte forma por tais alunos:



Chego a conclusão de que trazer uma nova proposta, como a criptografia kid-RSA adaptada trabalhada em sala de aula, pode nos ajudar a enxergar com outros olhos as dificuldades de alguns alunos, possibilitando repensar nossas práticas didáticas e nos fazendo buscar alternativas para o melhor aprendizado de todos.

REFERÊNCIAS BIBLIOGRÁFICAS

Batista, C. G. **Fracasso Escolar: Análise de erros em operações matemáticas**. Zetetiké, Campinas (SP), v.3, n.4, p.61-72, 1995. < https://periodicos.sbu.unicamp.br/ojs/index.php/zetetike/article/view/8646881/13783> . Acesso em: 24 jun. 2018

BRASIL. **Parâmetros Curriculares Nacionais (PCNs).** Matemática. Ensino Fundamental. Terceiro e quarto ciclos. Brasília: MEC/SEF, 1998.

BOYER, C. B; MERZBACH, U.C. **A History of Mathematics.** Estados Unidos da América: John Wiley & Sons, INC., 1989.

BUNT, L.N.H; JONES, P. S.; BEDIENT, J. D. **The Historical Roots of Elementary Mathematics**. New York: Dover Publications, INC, 1988

COUTINHO, S. C. **Números Inteiros e Criptografia RSA.** Rio de Janeiro: IMPA, 2005.

HEFEZ, A. **Aritmética.** Rio de Janeiro: SBM, 2014.

IMENES, LUIS MÁRCIO. **Conversa de professor – matemática.** Brasília: Ministério da Educação e do Desporto, Secretaria de Educação ã Distância, 1996. Disponível em: < http://www.dominiopublico.gov.br/download/texto/me002427.pdf >. Acesso em: 5 ago. 2018.

KOBLITZ, Neal. **CRYPTOGRAPHY AS A TEACHING TOOL.** Cryptologia, 21:4, 317-326, 1997

PIRES, Maria José da Silva; ABRANTES, Nyedia Nara Furtado; BORBA, Valéria Maria de Lima Borba. Matemática e multiplicação: dificuldades e novos olhares em torno deste ensino. Revista Principia, IFPB, João Pessoa, n. 23, p. 87-94, dez 2013. <http://periodicos.ifpb.edu.br/index.php/principia/article/viewFile/118/93>. Acesso em: 14 jun. 2018

SANTOS, M.L.B dos. **Ficha de aula: Divisão – divisor com dois algarismos – Processo por estimativa "fácil e lógico".** Rio de Janeiro: 2010. Disponível em < http://portaldoprofessor.mec.gov.br/fichaTecnicaAula.html?aula=10553 >. Acesso em: 26 jul.2018

SINGH, S. **O Livro dos Códigos: a ciência do sigilo – do antigo Egito à criptografia quântica.** Rio de Janeiro: Editora Record, 2001

SME/RJ. Caderno Pedagógico de Matemática do 6º ano - 1º Bimestre. 2017

SMITH, D. E. **History of Mathematics** – Volume II. New York: Dover Publications, INC., 1958.

SOLDATELLI, A. **Etnomatemática: a Multiplicação ao Redor do Mundo.** SCIENTIA CUM INDUSTRIA. Universidade de Caxias do Sul. V.4, N.4, p.219-222, 2016

SOUZA, Katia do Nascimento Venerando de. **AS OPERAÇÕES DE MULTIPLICAÇÃO E DIVISÃO NAS SÉRIES INICIAIS DO ENSINO FUNDAMENTAL**. Revista de Iniciação Científica da FFC, UNESP, Marília, v.10, n. 1. 2010. <http://www2.marilia.unesp.br/revistas/index.php/ric/article/view/273/259 >. Acesso em: 14 jun.2018

SWETZ, F. J. **Capitalism and Arithmetic**. Illinois: Open Court, 1989

ZATTI, Fernanda; AGRANIONIH, Neila Tonin; ENRICONE, Jacqueline Raquel Bianchi. **Aprendizagem matemática: desvendando dificuldades de cálculo dos alunos.** Perspectiva, Florianópolis, v. 34, n. 128, p. 115-132, dez. 2010.
< http://www.uricer.edu.br/site/pdfs/perspectiva/128_142.pdf>. Acesso em: 14 jun. 2018