ARITMÉTICA MODULAR E SUAS POSSIBILIDADES NA FORMAÇÃO CONTINUADA DE PROFESSORES DE MATEMÁTICA

Sérgio Ricardo Pereira de **Mattos**
Mestrado em Ensino das Ciências na Educação Básica, UNIGRANRIO
Brasil
patmatematica@gmail.com

Cleonice **Puggian**
Mestrado em Ensino das Ciências na Educação Básica, UNIGRANRIO
Brasil
cleo.puggian@gmail.com

Abel Rodolfo Garcia **Lozano**
Mestrado em Ensino das Ciências na Educação Básica, UNIGRANRIO
Brasil
cliciavp@terra.com.br

Resumo

Nosso trabalho consiste em um estudo qualitativo baseado na metodologia pesquisa-ensino. Explora a promoção do pensamento aritmético e algébrico através de atividades didáticas que envolvem os conceitos da aritmética modular. O estudo foi realizado através da observação participativa de um experimento de ensino realizado com 20 professores de matemática que atuam na educação básica do município de Duque de Caxias e de entrevistas semi-estruturadas com cinco desses professores. Os resultados preliminares desta investigação indicam que, mediante a escolha adequada dos conteúdos e da metodologia de ensino, o estudo de assuntos inerentes à teoria dos números favorece o desenvolvimento de idéias fundamentais da matemática, tais como: conjecturas, argumentações e demonstrações, além de ajudar os estudantes no entendimento conceitual da aritmética e da álgebra.

Palavras-chave: Teoria dos Números, Aritmética Modular, Educação Matemática, Formação Continuada de Professores

Abstract

This research is a qualitative study based on an approach called “research- teaching”. It explores the promotion of arithmetic and algebraic thinking through activities that involve the concepts of modular arithmetic. The study was based on a teaching experiment conducted with 20 math teachers who work in basic education in the city of Duque de Caxias. Data was collected through participant observation and semi-structured interviews with five of these teachers. Preliminary results of this investigation indicate that, through the appropriate choice of content and teaching methodology, the study of issues related to number theory favors the development of fundamental ideas in mathematics, such as assumptions, arguments and demonstrations. We conclude that this type of initiative supports teachers and students in the conceptual understanding of arithmetic and algebra.

Keywords: Numbers Theory, Modular Arithmetic, Mathematics Education, Teachers Training

1. INTRODUÇÃO

A teoria dos números é a área da matemática que desenvolve estudos sobre as propriedades dos números inteiros.

> "[...] Numa carta dirigida a Bernhard Frénicle de Bessy, Fermat anuncia um resultado surpreendente: se *p* é um primo e *a* um inteiro que não é divisível por *p*, então *p*, divide $a^{p-1}-1$. Na mesma carta comenta: "Eu lhe enviaria a demonstração se não temesse que ela é demasiado comprida". (MILIES e COELHO, 2006, p. 98).

A primeira demonstração desse resultado, conhecido como "pequeno Teorema de Fermat", foi publicada em 1736, quase um século depois, por Euler. Posteriormente Euler deu outras demonstrações do mesmo resultado. Numa delas, ele utiliza freqüentemente os "restos de divisões por *p*", que deram origem à Teoria das Congruências. Esse método de trabalho também foi usado por Lagrange e Legendre, mas só se tornou explícito nas *Disquisitiones* de Gauss, na qual aparecem a definição precisa e o simbolismo que se usa até hoje.

Embora o estudo da aritmética esteja presente nos currículos do ensino obrigatório em todos os países, há muito tempo, conforme afirma Lins e Gimenes (2006), o mesmo não acontece com a aritmética desenvolvida por Gauss, também conhecida como aritmética modular. No entanto, apesar da aritmética modular não ser uma parte da matemática "contemplada" nas salas de aulas em todos os níveis, usamos os restos das divisões para resolver diversos problemas no nosso dia a dia. Portanto, embora este conceito seja pouco trabalhado na educação básica, acreditamos que tenha um potencial motivador para a aprendizagem, pois é de fácil contextualização, possibilita a elaboração de atividades didáticas capazes de desafiar os alunos, consolida o aprendizado do conceito de divisibilidade, possibilita um contexto diferente do conhecido pelos alunos para a realização das operações aritmética e promove o desenvolvimento do pensamento conceitual, por outro lado permite que o aluno veja a importância das propriedades (comutativa, associativa, etc...), pois estas não são satisfeitas sempre, na aritmética modular.

A questão que orienta a investigação apresentada neste texto é: como é possível promover o desenvolvimento do pensamento aritmético e algébrico, através de atividades didáticas que envolvem os conceitos da aritmética modular? Decidimos realizar este estudo junto a professores do ensino básico explorando o conceito, as propriedades e aplicações da aritmética modular.

Esta investigação se justifica por vários motivos, são eles: a) contribuir para a formação continuada dos professores que atuam na educação básica; b) explorar as possibilidades da aritmética modular para o desenvolvimento do raciocínio lógico e pensamento conceitual entre alunos do ensino fundamental e médio; c) consolidar as pesquisas sobre o ensino e aprendizagem desse tema, que são relativamente esparsas e desconectadas; e, ainda d) desenvolver novos encaminhamentos para iniciativas de formação inicial de professores em matemática, tanto no ensino médio quanto no ensino superior, as quais ainda reproduzem modelos tradicionais.

2. REFERENCIAL TEÓRICO

Este trabalho buscou nos estudos de D'Ambrosio (1996), D'Amore (2007), Lins e Gimenez (2006), Portanova (2005), Santaló (2008) e Vasconcelos (2000) suporte para realizar reflexões sobre os encaminhamentos da pesquisa em educação matemática. No que se refere a

utilização de conteúdos da teoria dos números no ensino básico recorremos aos trabalhos de Resende (2007), Costa (2007) e Groenwald (2009).

O mundo em que vivemos está em constante transformação. Os avanços tecnológicos e o processo de globalização colocam o homem do século XXI diante de novos desafios. Por conta disso, tanto a escola, quanto os professores devem estar preparados para adaptar o ensino, seja em conteúdo, seja em metodologia, a estas mudanças. Segundo Santaló (2008)

> A missão dos educadores é preparar as novas gerações para o mundo em que terão de viver. Isto quer dizer proporcionar-lhes o ensino necessário para que adquiram as destrezas e habilidades que vão necessitar para seu desempenho, com comodidade e eficiência, no seio da sociedade que enfrentaram ao concluir sua escolaridade (p.11).

Nesse contexto, a formação de um aluno crítico, ativo e autônomo na construção do seu conhecimento passa a ser o objetivo do processo de ensino e aprendizagem. Assim compreendemos que

> a capacidade de raciocínio de um aluno desenvolve-se ao longo de um período de tempo e está intimamente ligada à vivência de uma gama de experiências variadas e potencialmente ricas, relacionadas aos diferentes tipos de pensamentos que estão inter-relacionados aos diferentes ramos da matemática: a lógica, a aritmética, a álgebra, a geometria, a probabilidade e a estatística, e que devem ser, especialmente no ensino fundamental, apresentados como um todo integrado, num currículo em espiral, organizado num grau crescente de complexidade. (PORTANOVA, 2005, p.19).

Sendo assim, para que os alunos possam desenvolver o pensamento matemático, é preciso fazer com que eles vivenciem experiências didáticas que explorem as diferentes áreas do conhecimento matemático. Ainda segundo Portenova (2005), o desenvolvimento do pensamento aritmético se dá inicialmente a partir da construção do conceito de número e do sistema de numeração decimal, posteriormente, amplia-se com a compreensão do significado das operações matemáticas, permitindo seu uso adequado na resolução de problemas.

Atualmente, no âmbito da pesquisa em educação matemática está-se explorando a concepção de sentido numérico. Lins e Gimenez (2006), definem sentido numérico como o conjunto de características capazes de estabelecer uma relação entre os números e as operações matemáticas, com o objetivo de resolver problemas. Dentre estas características destacam a capacidade de descobrir significados para os números e as operações, reconhecer o valor relativo dos números, identificar padrões, estabelecer relações entre diferentes quantidades e desenvolver estratégias de raciocínio para resolução de problemas.

Nesse sentido pode-se dizer que os procedimentos aritméticos constituem um sistema de organização que servem à resolução de problemas. Quando identificamos a possibilidade de generalização no trabalho aritmético podemos levar os alunos a estabelecerem uma relação com a álgebra, tornando-a significativa. Segundo Portanova (2005), "[,,,] os trabalhos com a aritmética devem se desenvolver juntamente com a álgebra, um implicado com o desenvolvimento do outro" (p.24).

No que diz respeito à concepção de pensamento algébrico vamos considerar a definição dada por Portanova (2005):

> O pensamento algébrico é desenvolvido a partir de estudos básicos empreendidos na área da aritmética, uma vez que o aluno já perceba a existência de diferentes conjuntos numéricos e das operações possíveis de se realizar entre os seus elementos. (PORTANOVA, 2005, p.24).

A autora destaca ainda que o desenvolvimento do pensamento algébrico pode levar os alunos a realizar abstrações e generalizações que não eram possíveis no nível do pensamento aritmético. De acordo com Lins e Gimenez (2006):

> A educação algébrica se dá na medida em que a produção de conhecimento algébrico serve ao propósito de iluminar ou organizar uma situação, como uma ferramenta e não como objeto primário do estudo. (LINS E GIMENEZ, 2006, p.109).

Para esses autores pensar algebricamente é pensar em produzir significado para os números e as operações aritméticas, trabalhar com as propriedades das operações sem relacioná-las a objetos físicos e operar sobre os números com a idéia de variável.

Com base nos argumentos expostos, entendemos que é na análise e na compreensão das estruturas matemáticas, na relação com o conceito de variável e na produção de significado para os números e as operações aritméticas que a álgebra assume um papel de destaque no estudo da matemática.

A educação para a cidadania, que é um dos grandes objetivos da educação de hoje, exige uma "apreciação" do conhecimento moderno, impregnado de ciência e tecnologia. Assim, o papel do professor de matemática é particularmente importante para ajudar o aluno nessa apreciação, assim como para destacar alguns dos importantes princípios éticos a ela associados. (D'AMBROSIO, 1996, p. 87). O professor assume um papel decisivo na formação do cidadão, pois suas concepções educacionais e conhecimentos profissionais contribuirão para a formação do pensamento de seus alunos. Concordamos com D'Ambrósio (1996) que

> "o grande desafio para a educação é pôr em prática hoje o que vai servir para amanhã. Pôr em prática significa levar pressupostos teóricos, isto é, um saber/fazer acumulado ao longo de tempos passados, ao presente. Os efeitos da prática de hoje vão se manifestar no futuro. Se essa prática foi correta ou equivocada só será notado após o processo e servirá como subsídio para uma reflexão sobre os pressupostos teóricos que ajudarão a rever, reformular, aprimorar o saber/fazer que orienta a nossa prática. (D'AMBROSIO, 1996, p. 80).

3. METODOLOGIA DE PESQUISA

Para a realização desse estudo optamos por uma abordagem qualitativa do tipo pesquisa-ensino. Segundo Penteado (2010), pesquisa ensino é aquela realizada pelo professor durante a sua prática docente. Nossa investigação está sendo desenvolvida em duas etapas. A primeira constituiu-se em um levantamento bibliográfico e a segunda, por sua vez, na implementação de um experimento de ensino, que de acordo com Groenwald, Sauer e Frank (2005), busca criar um espaço de discussão, onde os alunos possam refletir e buscar soluções para os problemas propostos, e o professor, através da observação e da analise das conjecturas levantadas pelos alunos, possa promover o desenvolvimento da atividade.

O estudo aqui apresentado foi realizado como piloto de nossa pesquisa e consiste em um curso de extensão para professores de matemática do ensino básico, com o tema "Introdução da aritmética modular na educação básica". Contou com a participação de cinco professores de matemática da rede municipal de Duque de Caxias e teve como carga horária 12horas/aula. O curso foi realizado em três encontros de 4h/a cada, no período da manhã (08:00 às 1200). O primeiro encontro ocorreu em uma das salas do curso de Mestrado em Ensino das Ciências da UNIGRANRIO, os dois seguintes, em uma sala de reunião da Secretaria de Educação da Prefeitura de Duque de Caxias. O registro dos eventos foi feito por meio da observação participativa com o auxílio da gravação de áudio e vídeo.

4. DESCRIÇÃO DA EXPERIÊNCIA

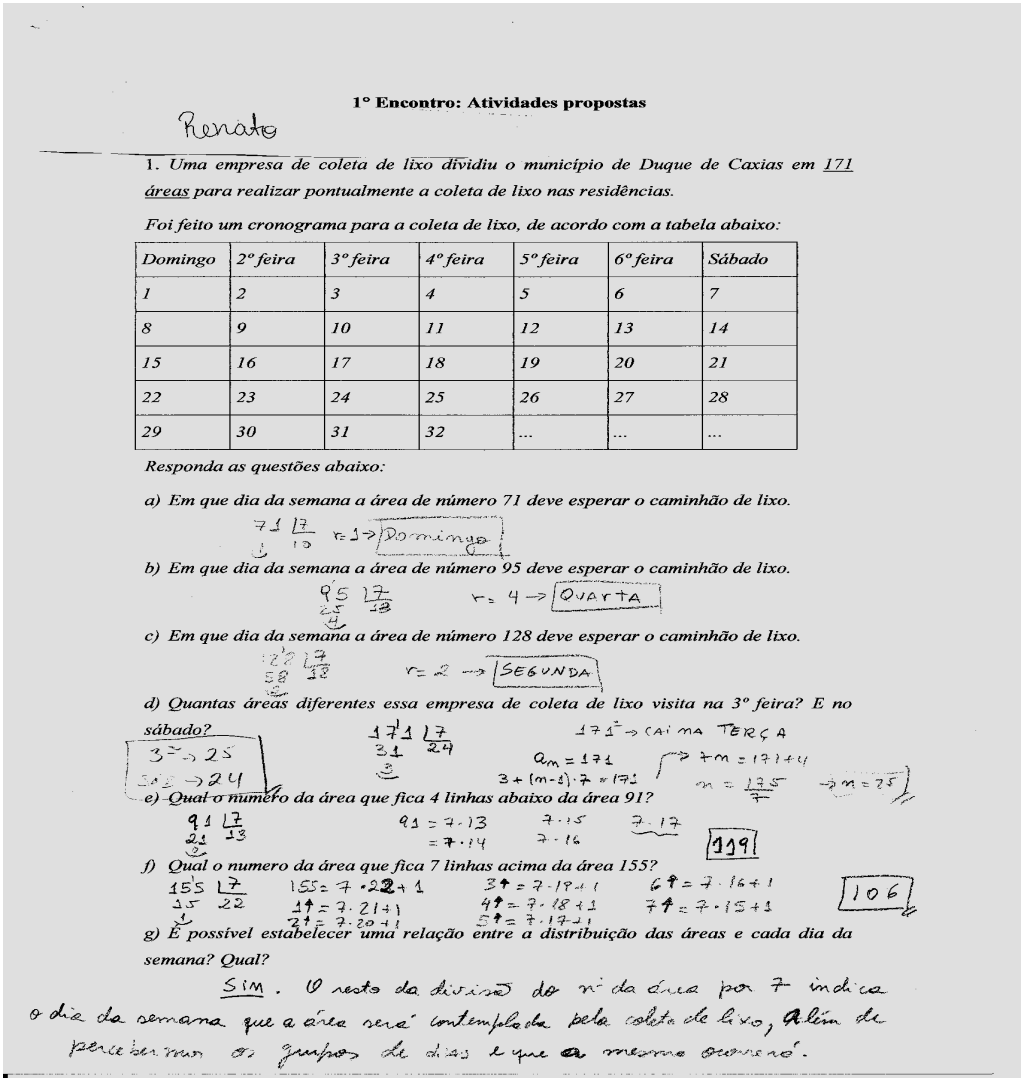
Iniciamos o primeiro encontro com a apresentação de cada professor e, na seqüência, fizemos um esclarecimento sobre a natureza científica do curso, informando que esse experimento de ensino faria parte de um trabalho de pesquisa para o Mestrado em Ensino das Ciências na Educação Básica da UNIGRANRIO. Foi então solicitada a permissão dos participantes para a realização da pesquisa, através do termo de consentimento livre e esclarecido (TCLE). Em seguida distribuímos um questionário socioeconômico que continha perguntas sobre família, situação econômica, moradia, formação e trajetória acadêmica, experiência profissional, quantidade de empregos, outra atividade profissional e carga de trabalho semanal. Este questionário foi prontamente respondido por todos os participantes. Levamos aproximadamente 30 minutos nesta etapa.

A metodologia de ensino adotada durante as aulas foi a resolução de problemas. Esta proposta metodológica defende a apresentação do problema antes dos conceitos e das técnicas de como resolvê-lo, permitindo que os alunos assumam uma postura de investigação frente a qualquer situação ou fato que possa ser questionado. De acordo com Smole (2007) a metodologia resolução de problemas corresponde a um modo de organizar o ensino, indo além dos aspectos puramente metodológicos. Implica tomada de consciência frente ao que é ensinar e, consequentemente, do que significa aprender.

As atividades didáticas elaboradas para todas as aulas foram planejadas de forma a promover a reflexão sobre os conceitos envolvidos, oferecer um contexto de formulação e validação de conjecturas, possibilitar a identificação de padrões de comportamento e estimular a capacidade de generalizar com o objetivo de resolver problemas. Apresentamos, a seguir, duas atividades desenvolvidas individualmente pelos professores durante o curso "Introdução da Aritmética Modular na Educação Básica". A primeira atividade foi desenvolvia pelo professor Renato, como apresentada na Figura 1.

Entendemos que a resolução passo a passo de cada etapa desse problema induz ao conceito de congruência modulo m, portanto, durante o comentário das estratégias utilizadas pelos professores fizemos intervenções e apresentamos formalmente os conceitos envolvidos. De uma forma geral os participantes do experimento não apresentaram dificuldade para resolver as atividades. Nos três primeiros problemas (letras a, b, c), todos os professores adotaram a divisão como procedimento de resolução, determinando a resposta de acordo com o resto encontrado nessa divisão. Acreditamos que o padrão nas respostas dos participantes deu-se em virtude da socialização das estratégias utilizadas na atividade anterior e nas discussões geradas. O mesmo não aconteceu nos problemas seguintes (letras d, e, f), onde os métodos de resolução diferem uns

dos outros, mas preservam a idéia de trabalhar com o resto da divisão por sete. No problema da letra "g", onde pedimos para os participantes estabelecessem a relação existente entre a distribuição das áreas e os dias da semana, todos os professores responderam que as áreas estavam distribuídas de acordo com o resto encontrado na divisão por sete, no entanto, em nenhuma das respostas dadas encontramos referência ao algoritmo da divisão, isto é, 7q + r, como um algoritmo adequado para resolução dos problemas.



1° Encontro: Atividades propostas

Renato

1. *Uma empresa de coleta de lixo dividiu o município de Duque de Caxias em 171 áreas para realizar pontualmente a coleta de lixo nas residências.*

Foi feito um cronograma para a coleta de lixo, de acordo com a tabela abaixo:

Domingo	*2° feira*	*3° feira*	*4° feira*	*5° feira*	*6° feira*	*Sábado*
1	*2*	*3*	*4*	*5*	*6*	*7*
8	*9*	*10*	*11*	*12*	*13*	*14*
15	*16*	*17*	*18*	*19*	*20*	*21*
22	*23*	*24*	*25*	*26*	*27*	*28*
29	*30*	*31*	*32*	...	...	...

Responda as questões abaixo:

a) Em que dia da semana a área de número 71 deve esperar o caminhão de lixo.

71 | 7 → 10 | 1 → Domingo

b) Em que dia da semana a área de número 95 deve esperar o caminhão de lixo.

95 | 7 → 13 | 4 → QUARTA

c) Em que dia da semana a área de número 128 deve esperar o caminhão de lixo.

128 | 7 → 18 | 2 → SEGUNDA

d) Quantas áreas diferentes essa empresa de coleta de lixo visita na 3° feira? E no sábado?

3ª → 25

Sáb → 24

17 | 7 → 24 | 3

171 → CAI NA TERÇA

$a_m = 171$

$3 + (m-1)\cdot 7 = 171$

$7m = 171 + 4$

$m = \frac{175}{7}$

$m = 25$

e) Qual o número da área que fica 4 linhas abaixo da área 91?

91 | 7 → 21 | 2

$91 = 7 \cdot 13$

$= 7 \cdot 14$

$7 \cdot 15$

$7 \cdot 16$

$7 \cdot 17$

119

f) Qual o numero da área que fica 7 linhas acima da área 155?

155 | 7 → 15 | 22 | 1

$155 = 7 \cdot 22 + 1$

$1\uparrow = 7 \cdot 21 + 1$

$2\uparrow = 7 \cdot 20 + 1$

$3\uparrow = 7 \cdot 19 + 1$

$4\uparrow = 7 \cdot 18 + 1$

$5\uparrow = 7 \cdot 17 + 1$

$6\uparrow = 7 \cdot 16 + 1$

$7\uparrow = 7 \cdot 15 + 1$

106

g) É possível estabelecer uma relação entre a distribuição das áreas e cada dia da semana? Qual?

Sim. O resto da divisão do nº da área por 7 indica o dia da semana que a área será contemplada pela coleta de lixo, Além de percebermos os grupos de dias e que a mesma ocorrerá.

Figura 1. Problema introdutório ao conceito de congruência modulo m

Durante os comentários um dos professores comentou que devido às várias operações matemáticas envolvidas na resolução desse problema, era possível utilizar essas atividades para abordar expressões numéricas no oitavo ano, por exemplo. Luiz complementa dizendo que, como estávamos trabalhando com os números naturais, era possível propor essas atividades para turmas do sexto ano. Nesse contexto, onde os participantes tentavam estabelecer o público e o conceito a ser trabalhado com as atividades desenvolvidas, o professor Fred faz o seguinte comentário:

Fred: [...] cada um pode pegar um problema desse e utilizar uma de suas idéias, que estão muito legais, para usar em sala de aula. Eu já vou pensar em varias coisas, como eu vou usar e em que série eu vou usar aquilo [...] aí eu já poso pensar em expressão algébrica no oitavo ano. Naquela outra questão que nós estávamos fazendo, por exemplo, eu estava pensando, eu falei, não, eu montei uma mini expressão numérica 91 + 4.7. Eu já penso varias paradas ali, se eu trabalhar isso no quinto e no sexto ano, eu já penso até em trabalhar ordem de prioridade das operações em expressões numéricas, [...] cada pessoa que pegar isso ai, vai pensar em quinhentas coisas diferentes. Você ta jogando a idéia e eu[...]

Luiz: [...] a letra **d** é formidável, questão formidável, porque a sequência começa, ela não começa por um múltiplo de sete e ai dá essa distorção, a tendência do aluno na lógica, possa marcar o sábado e a terça-feira com a mesma quantidade [...].

O professor Renato explica que ao resolver o problema da segunda lista, pensou:

Renato: [...] como é que um aluno que tenha entendido a dinâmica da coisa resolveria isso? Qual o numero da área que fica 4 (quatro) linhas abaixo da área 91 ? Bem, 91÷7 deixa resto zero, são treze grupos completos, 91 = 7. 13. Então um linha abaixo é 7. 14, duas linhas abaixo é 7. 15 [...]. Esse foi o raciocínio que eu pensei. Como é que o aluno ia pensar isso? Eu acho que ele ia pensar assim.

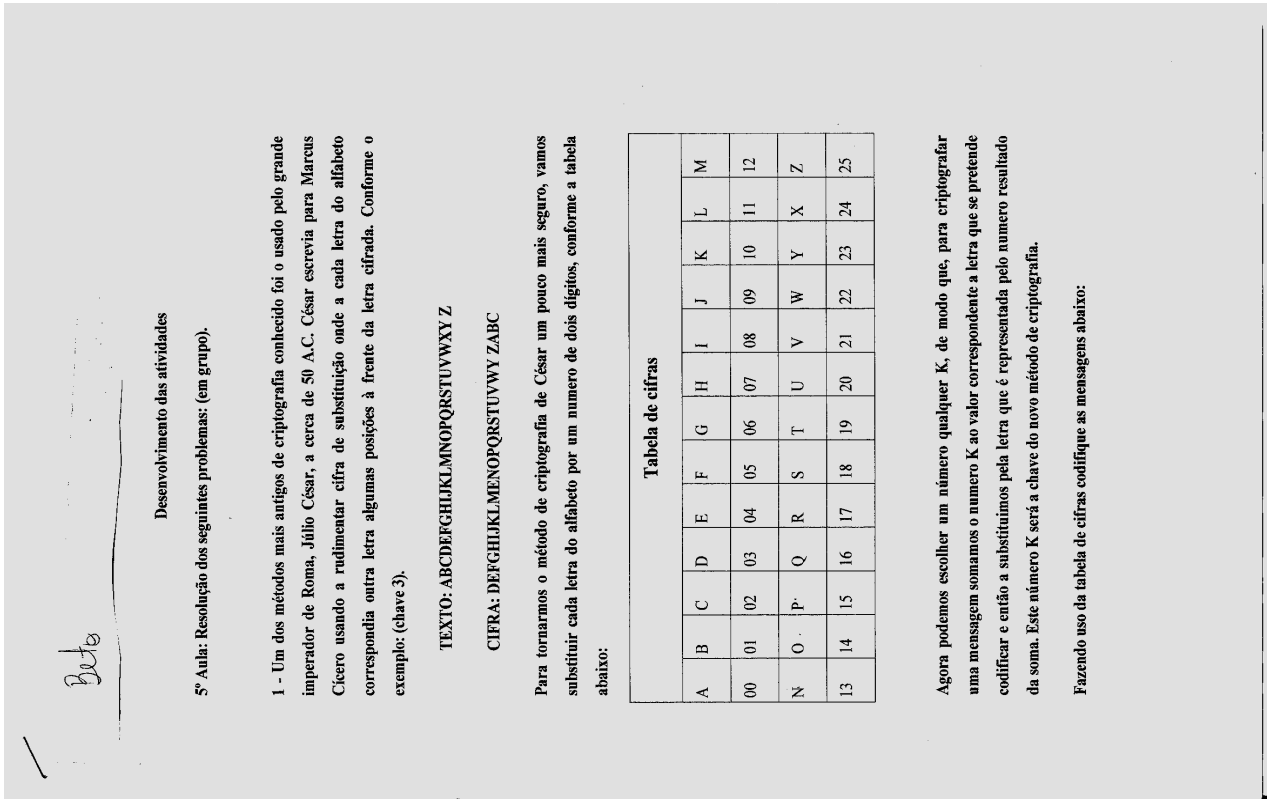
Aproveitamos para comentar que resoluções como as citadas acima podem auxiliar na compreensão do conceito do algoritmo da divisão. Podemos mostrar o papel que cada parcela (divisor, dividendo, quociente e resto) desempenha na operação divisão. Durante o curso, a partir dos resultados desses problemas, definimos congruência modulo m, introduzimos a idéia de operação de classes de resto e exploramos o conceito de classes de equivalência.

A atividade que apresentamos na Figura 2 teve como objetivo identificar e explorar a utilização da aritmética modular em atividades didáticas que envolvem a criptografia.

O problema 1 (letra a, b, c) consiste em propor aos participantes que codifiquem mensagens utilizando o método de criptografia descrito no problema. Solicitamos aos participantes que encolhessem mensagens diferentes para codificar e trocassem as mensagens para que pudessem decodificar. No inicio houve pequenas dúvidas, como por exemplo: Basta trocar a letra pelo número correspondente na tabela e somar o valor da chave K? Quando o resultado dessa soma não pertencer a tabela, o que faço? Após os esclarecimentos necessários demos prosseguimento à atividade. Tirando pequenos erros de substituição de letras, todos entenderam a idéia da atividade e fizeram corretamente. No problema 2, pedimos que os professores, baseados no método descrito no problema, elaborassem um algoritmo capaz de codificar e outro capaz de decodificar as mensagens. Apesar dos professores mostrarem que haviam compreendido o funcionamento do método de criptografia, reconhecendo inclusive que se tratava de uma congruência modulo 26, eles não conseguiram resolver o problema. Decidimos então fazer com eles passo a passo, apresentando a seguinte resposta para o problema:

> *O método descrito acima consiste em somar o número equivalente a letra da mensagem e a chave K, substituindo o resultado dessa soma. Observe essa soma não pode ser superior a 25, pois de acordo com a tabela, não existe letra no alfabeto que corresponda a um número maior que 25. Seja P o digito equivalente a uma letra do texto original, C o digito equivalente a letra do texto cifrado e K a chave, então:* $C \equiv (P + K) \bmod 26$. *A decodificação pode ser feita pela:* $(C - K) \equiv P \bmod 26$.

Figura 2. Enunciado do problema de criptografia



Beto

Desenvolvimento das atividades

5ª Aula: Resolução dos seguintes problemas: (em grupo).

1 - Um dos métodos mais antigos de criptografia conhecido foi o usado pelo grande imperador de Roma, Júlio César, a cerca de 50 A.C. César escrevia para Marcus Cícero usando a rudimentar cifra de substituição onde a cada letra do alfabeto correspondia outra letra algumas posições à frente da letra cifrada. Conforme o exemplo: (chave 3).

TEXTO: ABCDEFGHIJKLMNOPQRSTUVWXYZ

CIFRA: DEFGHIJKLMENOPQRSTUVWY ZABC

Para tornarmos o método de criptografia de César um pouco mais seguro, vamos substituir cada letra do alfabeto por um numero de dois dígitos, conforme a tabela abaixo:

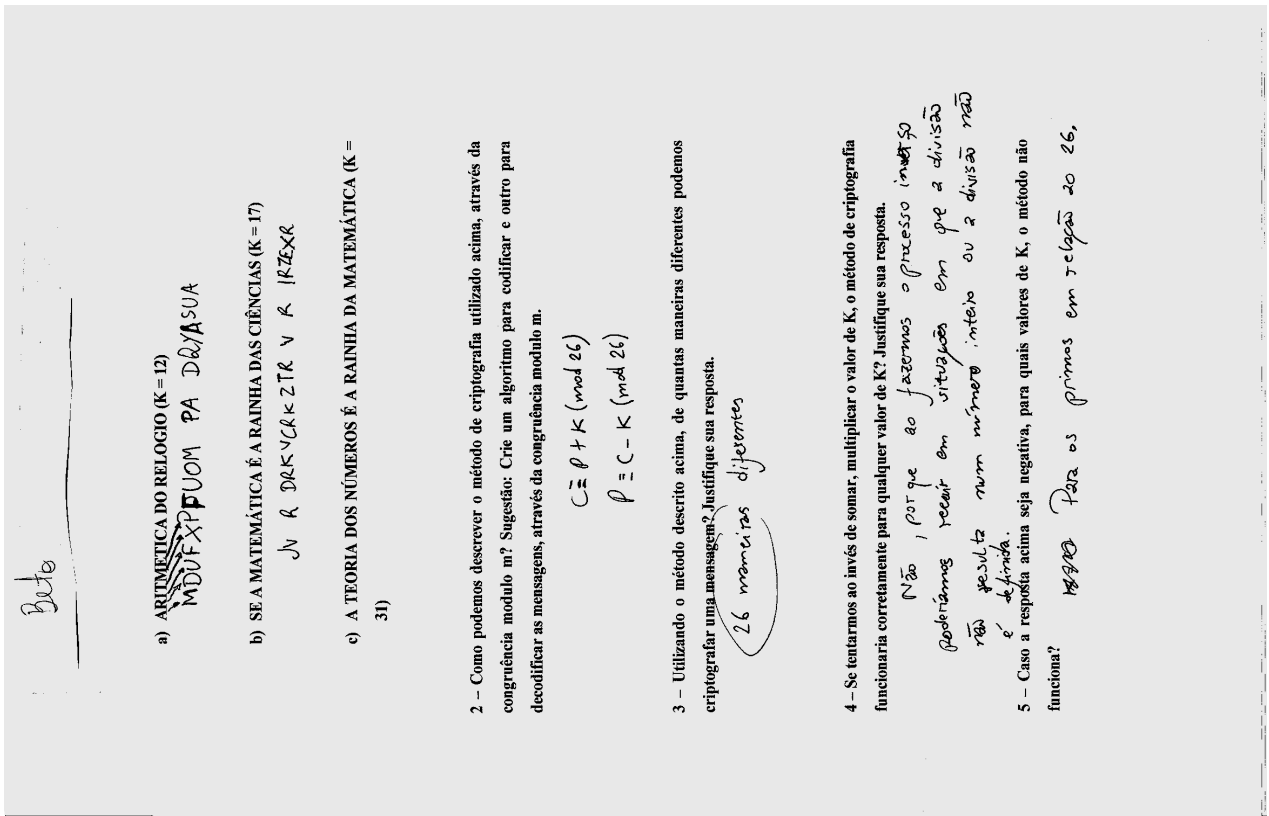
Tabela de cifras

A	B	C	D	E	F	G	H	I	J	K	L	M
00	01	02	03	04	05	06	07	08	09	10	11	12
N	O	P	Q	R	S	T	U	V	W	Y	X	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

Agora podemos escolher um número qualquer K, de modo que, para criptografar uma mensagem somamos o numero K ao valor correspondente a letra que se pretende codificar e então a substituimos pela letra que é representada pelo numero resultado da soma. Este número K será a chave do novo método de criptografia.

Fazendo uso da tabela de cifras codifique as mensagens abaixo:

Figura 3. Questões referentes ao problema de criptografia



Beto

a) ARITMETICA DO RELOGIO (K = 12)

MDUFXPPUOM PA DRYASUA

b) SE A MATEMÁTICA É A RAINHA DAS CIÊNCIAS (K = 17)

JV R DRKVCRKZTR V R IRZEXR

c) A TEORIA DOS NÚMEROS É A RAINHA DA MATEMÁTICA (K = 31)

2 – Como podemos descrever o método de criptografia utilizado acima, através da congruência modulo m? Sugestão: Crie um algoritmo para codificar e outro para decodificar as mensagens, através da congruência modulo m.

$C \equiv P + K \pmod{26}$

$P \equiv C - K \pmod{26}$

3 – Utilizando o método descrito acima, de quantas maneiras diferentes podemos criptografar uma mensagem? Justifique sua resposta.

26 maneiras diferentes

4 – Se tentarmos ao invés de somar, multiplicar o valor de K, o método de criptografia funcionaria corretamente para qualquer valor de K? Justifique sua resposta.

Não, porque ao fazermos o processo inverso podemos recair em situações em que a divisão não resulta num número inteiro ou a divisão não é definida.

5 – Caso a resposta acima seja negativa, para quais valores de K, o método não funciona?

Para os primos em relação ao 26.

O Professor Beto e os demais participantes do curso foram acompanhando a explicação e resolvendo os problemas propostos. Ao final da resolução, perceberam que não se tratava de uma atividade muito complicada, confirmando que eles podiam ter resolvido.

Sobre esse problema o professor Renato faz o seguinte comentário:

> Renato: Bem melhor do que eu pensei, pensei num troço mais difícil. Pensei assim, seja N um número qualquer, (N+K) ≡ 0 mod 26, mas não vai adiantar nada porque não é o objetivo, eu não vou achar a letra cifrada eu só percebo se vai ser côngruo a zero modulo 26[...].

Os participantes do curso não apresentaram dificuldade no problema 3 (três). Logo perceberam que independente de K poder assumir qualquer valor inteiro, as possibilidades estavam restritas aos possíveis restos deixados na divisão por 26.

No problema quatro somente dois professores responderam corretamente e justificaram sua resposta, se referindo a restrição do conjunto dos números inteiros, em relação à operação divisão. Segue o comentário do professor Renato sobre sua resposta:

> Renato: Não, porque quando você está multiplicando, para você tentar decodificar, você pode cair em número que não divida o outro, porque se você multiplica [...]. Primeiro problema é multiplicar, você consegue achar a cifra e quando você vai decodificar você vai dividir na divisão, você pode encontrar um número que não é divisível pelo outro, ai você foge do campo dos inteiros.

Durante os comentários surge um questionamento do professor Fred, sobre a existência da criptografia através de matrizes:

> Fred: Mas assim, existe a criptografia feita por matrizes, daí o ideal seria matriz inversa...

Luiz complementa:

> Luiz: Desde que a matriz seja quadrada, né...
>
> Renato: Quadrada e inversível...

Aproveitamos esse momento e falamos sobre utilizar a criptografia na escola como forma de abordar assuntos como matrizes, funções, expressões dentre outros temas da matemática.

No problema cinco pedimos que os professores, ao perceberem que na multiplicação o método de criptografia não era eficaz para qualquer valor de K, identificassem para quais valores o método funcionava. Para facilitar a visualização dos professores apresentamos uma tabela de multiplicação módulo 26, em slide. A seguir apresentamos parte dessa tabela:

Tabela multiplicação modulo 26

X	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
2	0	2	4	6	8	10	12	14	16	18	20	22	24	0	2	4	6	8	10	12	14	16	18	20	22	24
3	0	3	6	9	12	15	18	21	24	1	4	7	10	13	16	19	22	25	2	5	8	11	14	17	20	23
4	0	4	8	12	16	20	24	2	6	10	14	18	22	0	4	8	12	16	20	24	2	6	10	14	18	22
5	0	5	10	15	20	25	4	9	14	19	24	3	8	13	18	23	2	7	12	17	22	1	6	11	16	21
6	0	6	12	18	24	4	10	16	22	2	8	14	20	0	6	12	18	24	4	10	16	22	2	8	14	20
7	0	7	14	21	2	9	16	23	4	11	18	25	6	13	20	1	8	15	22	3	10	17	24	5	12	19

Nosso objetivo com esse problema era levar os professores a perceberem uma propriedade importante da aritmética modular, conhecida como teorema da inversão: *A classe α têm inverso em Zn se, e somente se, α e n são primos entre si.* É fácil visualizar na tabela acima que somente as classes representadas por números primos com o 26 possuem inverso. Em um problema anterior já havíamos explorado superficialmente essa propriedade, através da construção de tabelas.

Assim como na atividade anterior, eles não conseguiram identificar tal comportamento e assim generalizar. No entanto, os professores realizaram outras conjecturas interessantes através da observação da tabela. Perceberam, por exemplo, que somente os números primos com o 26 possuíam como resultado da multiplicação de classes todos os possíveis restos da divisão por 26, ou seja, os números que possuíam divisores em comum com o 26 depois de certo momento, os resultados da multiplicação de classes começam a se repetir. Tentaram também verificar porque a classe 13 só tinha como resultado 0 (zero) ou 13 (treze). Seguem alguns comentários realizados pelos professores ao observarem a tabela:

Renato: Não funciona para K = 0.

Luiz: Eu vou ter letras repetidas representando letras diferentes, eu posso pegar uma mensagem codificada com 5 (cinco) a, mas o primeiro a representa um r, o segundo representa um s, eu não tenho como fazer isso.

Após os esclarecimentos e a apresentação formal do teorema da inversão, com o auxilio da tabela, os professores comentaram:

Luiz: Putz, pode crê, formidável.

Fred: Show de bola.

Renato: É essa última eu não ia pensar mesmo.

Fred: Era difícil de pensar.

Luiz: A criptografia não é uma coisa simples. É chato para trabalhar. É maneiro assim, uma questão viável, mas a gente trabalha com o fator tempo, se você coloca isso em uma prova, nego vai ficar 2 (duas) horas fazendo [...]. Dá para fazer uma questão de criptografia, eu acho que sim [...].

Ao final dessa discussão agradecemos aos participantes pela participação e pelas excelentes contribuições que deram no decorrer do curso.

CONCLUSÕES PRELIMINARES

Um dos nossos objetivos durante o planejamento do curso era elaborar atividades baseadas no conceito da aritmética modular que levassem os professores de matemática a ampliar sua compreensão e promover o desenvolvimento do pensamento aritmético e algébrico. Dentre as conclusões preliminares, podemos destacar que os professores que participaram do estudo demonstraram não estarem familiarizados com o conceito de congruência modulo m.

Durante o curso, notamos que os professores demonstraram dificuldades e um pouco de resistência ao trabalharem os problemas que exigiam uma argumentação formal dos conceitos envolvidos ou exploravam uma parte conceitual do assunto. Além disso, foi possível perceber que os participantes não estavam acostumados a desenvolver, em sala de aula, atividades como as trabalhadas nos encontros.

Considerando que a formação inicial desses docentes ocorreu há, em média, 10 anos, suspeitamos que esses conceitos não foram trabalhados de modo adequado, um fato já indicado pela pesquisa de Resende (2007), que estudou o significado da disciplina Teoria dos Números na licenciatura. Esta autora destaca que as disciplinas que abordam tópicos da teoria dos números nos cursos de licenciatura em matemática oferecidos pelas universidades brasileiras tratam os conteúdos de maneira tradicional, carecendo de uma abordagem que privilegie a formação do professor de matemática da escola básica e de um tratamento pedagógico do conteúdo adequado.

Outra constatação refere-se à apropriação do conhecimento teórico sobre aritmética modular pelos participantes do estudo. Percebemos através da análise das atividades desenvolvidas durante o curso que os professores, após conhecerem a proposta didática fundamentada no conceito de congruência modulo m, passaram a utilizar esses conceitos como ferramenta para resolução dos problemas seguintes.

Consideramos, a motivação dos professores, um ponto positivo do estudo, eles se mostraram bastantes entusiasmados com os problemas propostos e as idéias levantadas, procurando sempre que possível relacionar as atividades que estávamos desenvolvendo com a realidade da sala de aula. Dentre os assuntos, apontados pelos professores, que poderiam ser trabalhados a partir das atividades propostas, destacamos: expressões numéricas, expressões algébricas, sequências, progressão e algoritmo da divisão. No entanto, ao longo das aulas eles perceberam que o leque de possibilidades era ainda maior, por exemplo, podíamos explorar o conceito de classes de equivalência, as propriedades das operações matemáticas em um contexto diferente do usual, um sentido para a divisão de números inteiros não construído com o uso da operação em situação de repartição, além de promover um contexto de formulação e validação de conjecturas.

Essa experiência também indicou a necessidade de atrelarmos os conhecimentos específicos aos metodológicos, isto é, de promover a compreensão dos conceitos matemáticos através da prática pedagógica. Portanto, acreditamos que iniciativas como a proposta nesta pesquisa, podem constituir oportunidades de formação continuada, durante as quais os professores do ensino básico podem revisitar os conceitos matemáticos com propósitos didáticos. Sobre essa questão, destacamos o trabalho de Moreira e David (2005), que estudaram o conhecimento matemático do professor, sua formação e prática docente na escola básica. Estes autores destacam que a formação matemática na licenciatura ainda desenvolve-se baseada nos valores conceituais e estéticos da matemática cientifica, e estes são insuficientes para matemática escolar e às vezes até mesmo inadequado. Este estudo sugere que a concepção sobre formação de professores deve levar em conta a especificidade do trabalho docente e tomar a matemática escolar como referência.

Para Lins e Gimenez (2006) a aritmética do século XX oferece respostas a problemas teóricos muito recentes, como a matemática discreta, a criptografia, a exploração máxima na economia, os problemas de minimização, a análise numérica, os problemas de interação, dentre outros. Para os autores a aritmética não pode ser reduzida a regras escolares ou a aritmética dos números naturais, ela deve ser desenvolvida nas escolas com o objetivo de resolver problemas.

Os resultados preliminares desta investigação indicam que, mediante a escolha adequada dos conteúdos e da metodologia de ensino, o estudo de assuntos inerentes à teoria dos números favorece o desenvolvimento de idéias fundamentais da matemática, tais como: conjecturas, argumentações e demonstrações, além de ajudar os estudantes no entendimento conceitual da

aritmética e da álgebra. Cursos como o descrito neste trabalho oferecem uma oportunidade ímpar para o desenvolvimento do pensamento conceitual entre os professores da escola básica, criando novas possibilidades para a melhoria da qualidade do ensino de matemática no Brasil.

REFERÊNCIAS BIBLIOGRÁFICAS

Costa, Eduardo, S. (2007). As equações diofantinas lineares e o professor de matemática do ensino médio. 119 f. Dissertação (Mestrado em Educação Matemática) – Centro de Ciências Exatas e Tecnologias, Pontifícia Universidade Católica de São Paulo – PUC/SP.

Courant, R. & Robbins, H. (2000). O que é matemática? Tradução de: Adalberto da Silva Brito. Rio de Janeiro: Ciência Moderna.

Coutinho, Severino. C. (2009). Números Inteiros e Criptografia RSA. Rio de Janeiro: IMPA. 2ª ed.

Dante, Luiz R. (1990). Restos, Congruência e Divisibilidade. Revista do professor de matemática, SBM, volume 10. p. 1-8.

D'Amore, B. (2007). Elementos de didática da matemática. Tradução de: Maria Cristina Bonomi. São Paulo: Livraria da Física.

Dupas Penteado, H. & Garrido, E. (2010). Pesquisa-ensino: A comunicação escolar na formação do professor. São Paulo, Edições Paulinas.

Groenwald, Claudia, L. O.; Nunes, Giovanni, S.; Sauer, Lisandra, O.; Franke, Rosvita, F. (2009). Teoria dos Números no Ensino Básico – desenvolvendo o pensamento aritmético. In: Maranhão, C. (org.). Educação Matemática nos anos finais do ensino fundamental e ensino médio: pesquisas e perspectivas. São Paulo: Musa Editora, cap. 4, p. 27-44.

Lins, Rômulo, C. & Gimenez, J. (2006). Perspectivas em Aritmética e Álgebra para o século XXI. Campinas, SP: Papirus.

Ludke, M. & André, Marli, E. D. A. (1986). Pesquisa em educação: abordagens qualitativas. São Paulo: EPU.

Maranhão, C. (org.) & Pires, Célia, M. C. et al. (2009). Educação Matemática nos anos finais do ensino fundamental e ensino médio: pesquisas e perspectivas. São Paulo: Musa Editora.

Milies, César. P. & Coelho, Sônia. P. (2006). Números: Uma introdução à matemática. São Paulo: ed^{USP}. 3ª ed.

Moreira, Plínio, C. & David, Maria, M. M. S. (2005). O conhecimento matemático do professor: formação e prática docente na escola básica. Revista Brasileira de Educação, n° 28.

Parra, C.(org.) & Saiz, I. (org.) & Lerner, D. et al. (1996). Didática da matemática: Reflexões Psicopedagógicas. Tradução: Juan Acuna Llorens. Reimpressão 2008. Porto Alegre: Artmed.

Portanova, Ruth (org.) & Nina, Clarissa, T. D. et al. (2005). Um currículo de matemática em movimento. Porto Alegre: EDIPUCRS.

Resende, Marilene, R. (2007). Re-significando a disciplina teoria dos números na formação do professor de matemática na licenciatura. 281 f. Tese (Doutorado em Educação Matemática) – Centro de Ciências Exatas e Tecnologias, Pontifícia Universidade Católica de São Paulo – PUC/SP.

Sá, Ilydio, P. (2007). A magia da matemática. Rio de Janeiro: Ciência Moderna.

Santos, Leandra, G. (2007). Introdução do pensamento algébrico: um olhar sobre professores e livros didáticos de matemática. 231 f. Dissertação (Mestrado em Educação) – Centro de Educação, Universidade Federal do Espírito Santo – UFES.

Smole, K. S. & Diniz, M. I. (2001). Ler, escrever e resolver problemas: Habilidades básicas para aprender matemática. Reimpressão 2007. Porto Alegre: Artmed.

D'Ambrosio, Ubiratan, (1996). Educação Matemática: da teoria à prática. Campinas, São Paulo: Papirus Editora. 16ª ed.

Vasconcelos, Claudia, C. (2000). Ensino-Aprendizagem de matemática: velhos problemas, novos desafios. Millenium on. Line, n° 20. (Extraído de http://www.ipv.pt./millenium/20ect.htm acessado em 18/08/2010.