Percursos investigativos para o trabalho com números primos: uma proposta com o emprego de crivos de primalidade

Rubens Vilhena Fonseca. UEPA. e-mail: rubens@uepa.br

Resumo

Na apresentação dos números primos uma questão natural é a de determinar todos os números primos até certo limite dado. Um procedimento simples que é mostrado no ensino fundamental é o chamado Crivo de Eratosthenes e este procedimento, na maioria dos casos, segue sendo o único empregado até mesmo nos cursos de licenciatura em Matemática. Neste artigo, justifica-se a importância de se introduzir outros crivos, como os de Atkin e Sundaram, e a relevância, no ensino superior, não apenas de se determinar certa quantidade de primos usando os crivos, como também a questão fundamental de se discutir a primalidade de um inteiro positivo ímpar.

Palavras-chave: Crivos de primalidade; didática da matemática; teoria das situações didáticas.

Introdução

Este trabalho tem por finalidade descrever uma pesquisa em andamento, ligada ao grupo Processo de Ensino e Aprendizagem em Matemática (PEA-MAT), e que procura investigar o trabalho didático com números primos entre licenciandos em Matemática, por meio do emprego de diferentes crivos, como os de Eratosthenes, Sundaram e Atkin. Neste relato, além dos aportes teóricos e metodológicos, são trazidas as descrições dos crivos, que servirão à elaboração das sequências didáticas para o trabalho com os sujeitos da pesquisa.

A justificativa desta pesquisa repousa, essencialmente, na relevância do tema no âmbito da aprendizagem dos números naturais. De fato, as crianças, ao chegarem à escola, não encaram os números e as operações elementares relativas a eles como fatos inéditos. Justamente neste sentido, afirmam Friederich, Kruger e Nehring:

> As crianças ao chegarem à escola, já possuem certa noção dos números e algumas operações básicas, portanto o estudo dos números, como objeto matemático, precisa envolver o reconhecimento da existência de diferentes tipos de números e de suas representações e classificações, exemplo os números primos, compostos, pares, ímpares, fracionários etc. É importante salientar que partir dos conhecimentos que as crianças possuem não significa restringir-se a eles, pois é papel da escola ampliar esse universo de conhecimento e dar condições a elas de estabelecerem vínculos entre o que conhecem e os novos conteúdos que vão construir, possibilitando uma aprendizagem significativa (FRIEDERICH, KRUGER E NEHRING, 2009, p. 4).

Os sistemas escolares preveem a introdução do conhecimento relativo aos números primos geralmente no sexto ano do ensino fundamental. De fato, os Parâmetros Curriculares do Ensino Fundamental (Brasil, 1998) recomendam, naquilo que chamam de terceiro ciclo (os atuais sexto e sétimo anos) um trabalho continuado com os números naturais "em situações de contagem, de ordenação, de codificação em que tenha oportunidade de realizar a leitura e escrita de números 'grandes' e desenvolver uma compreensão mais consistente das regras que caracterizam o sistema de numeração que utiliza" (BRASIL, 1998, p.66).

Neste contexto, a introdução dos números primos não pode surgir de forma descolada em relação ao princípio multiplicativo, nem exposta sem a contextualização proposta por situações problema:

> Conceitos como os de 'múltiplo' e 'divisor' de um número natural ou o conceito de 'número primo' podem ser abordados neste ciclo como uma

> ampliação do campo multiplicativo, que já vinha sendo construído nos ciclos anteriores, e não como assunto novo, desvinculado dos demais. Além disso, é importante que tal trabalho não se resuma à apresentação de diferentes técnicas ou de dispositivos práticos que permitem ao aluno encontrar, mecanicamente, o mínimo múltiplo comum e máximo divisor comum sem compreender as situações-problema que esses conceitos permitem resolver (BRASIL, 1998, p.66).

Em atenção a esta proposição, o Currículo do Estado de São Paulo (São Paulo, 2010) propõe a introdução do conceito de números primos no 6º ano do Ensino Fundamental. Como é possível observar na próxima figura, o conteúdo está relacionado não à mera identificação dos primos, mas ao seu significado.

5ª série/6º ano do Ensino Fundamental		
	Conteúdos	**Habilidades**
1º Bimestre	**Números** Números naturais • Múltiplos e divisores • Números primos • Operações básicas (+, –, . , ÷) • Introdução às potências Frações • Representação • Comparação e ordenação • Operações	• Compreender as principais características do sistema decimal: significado da base e do valor posicional • Conhecer as características e propriedades dos números naturais: significado dos números primos, de múltiplos e de divisores • Saber realizar operações com números naturais de modo significativo (adição, subtração, multiplicação, divisão, potenciação) • Compreender o significado das frações na representação de medidas não inteiras e da equivalência de frações • Saber realizar as operações de adição e subtração de frações de modo significativo

Fonte: Currículo do Estado de São Paulo (Matemática e suas Tecnologias – Ensino Fundamental Ciclo II e Ensino Médio), p.57

Em relação ao conceito de primalidade, os alunos devem receber subsídios para perceberem que alguns números são o produto de outros, como $6 = 2 \times 3$, $30 = 5 \times 6$, etc., ou seja, são números compostos. Os demais números são aqueles que não têm outros fatores além deles mesmos e da unidade. Em outras palavras, número primo é todo número, maior do que 1, que é divisível somente por si mesmo e pela unidade. Os primeiros números primos são 2, 3, 5, 11, 13, 17, 19, 23, 29, 31, 37, 41, etc. Da mesma forma, quando um número não é primo ele pode ser decomposto em fatores primos, como $12 = 2 \times 2 \times 3$, $30 = 2 \times 3 \times 5$, $935 = 5 \times 11 \times 17$. Pelo seu caráter basilar no estudo dos números, essa propriedade é conhecida como o Teorema Fundamental da Aritmética. Ela significa que os números primos são, por assim dizer, os "átomos" ou "tijolos" da construção numérica pela multiplicação.

Assim, é preciso pensar na maneira como podem ser construídos elementos didáticos que estimulem o trabalho com os primos, o que se descreve a seguir.

Aportes teóricos e metodológicos

A construção da aprendizagem relacionada aos números primos representa um desafio para o professor, à medida que os processos relacionados ao significado deste tema precisam fornecer elementos para que o estudante não apenas compreenda as características intrínsecas destes números e a importância da apropriação do conhecimento relativo aos mesmos no âmbito da aritmética, como também desenvolvam competência para o emprego das propriedades destes números em situações matemáticas contextuais, caracterizadas por argumentações, demonstrações, provas e usos específicos (compreensão de códigos criptográficos é um caso típico).

No âmbito da didática francesa, que serve de referência a este estudo, existe a proposição de que o aluno pode aprender a partir do engajamento em um processo investigativo de tal forma que as etapas deste esforço possam representar uma simulação do trabalho do matemático quando se debruça sobre problemas específicos – este trabalho é, portanto, uma produção que denota, dialeticamente, um percurso de construção de um conhecimento a partir da assunção da possibilidade de aprendizado autônomo e independente (Oliveira, 2009). Esta abordagem é tratada teoricamente no âmbito da teoria das situações didáticas (TSD), proposta por Guy Brousseau (1986).

Para Oliveira e Silva (2013), de acordo com o autor francês, a TSD pode ser encarada como uma proposta interacional, envolvendo um aprendiz e um meio específico, denominado *milieu*, e que, de certa maneira, condiciona o processo de aquisição de dado conhecimento, o que costuma ocorrer no contexto de propostas que procuram provocar desequilíbrio cognitivo e um movimento de reorganização das estruturas mentais a partir da compreensão, pela via investigativa, dos conceitos incluídos em uma proposta de ensino. Desta forma, uma situação didática representaria uma rede de processos de interação entre o aluno, o professor e o saber, que é organizada no âmbito dos espaços de ensino (a sala de aula, por exemplo) tendo por contexto significativo um *milieu* antagônico e por constituintes algumas fases, entendidas como dialéticas, e certas estratégias, baseadas, essencialmente, em problematizações.

Uma situação didática é constituída por interações de caráter didático entre professor, aluno e saber por meio do desenvolvimento de atividades voltadas ao ensino e aprendizagem de um determinado conteúdo. No entendimento de Almouloud (2007, p. 33), "o objetivo central da teoria das situações é a situação didática".

Além disso, compõe a proposta da teoria das situações o fato de que, entre o momento de aceitação do problema e das dialéticas envidadas para sua resolução, a participação do professor limite-se à mediação das interações entre os sujeitos e não incida de forma diretiva em relação ao saber em jogo. Em outras palavras, o professor não intervém nas decisões dos estudantes, evitando incorrer em efeitos deletérios do contrato didático ali estabelecido (Brousseau, 1986). O docente tem como um dos elementos efetivos de sua mediação a elaboração de problemas adequados que, no âmbito da situação, serão os elementos que possibilitarão abordar o conhecimento pretendido. Todo o processo é, assim, justificado pela lógica interna da situação e pela elaboração de resoluções adequadas às problemáticas sugeridas. De acordo com Oliveira e Silva (2013), a esta proposta, Brousseau (1997) denomina situação adidática. Para o autor francês, "as situações adidáticas são aquelas situações de aprendizagem nas quais o professor foi bem sucedido na remoção de sua vontade" e de quaisquer indicações mais diretas a respeito do conteúdo do saber a ser trabalhado, de forma que "elas ocorrem sem a intervenção do professor no que se refere ao conhecimento" (BROUSSEAU, 1997, p.47).

O que deve ser destacado em relação à situação adidática é que o aluno não deve perceber a intencionalidade didática do professor, mesmo considerando que a mesma exista. É justamente por isso que se pode afirmar que cabe ao aluno aceitar a responsabilidade pelo processo de investigação e pela descoberta de resoluções que são, em última instância, o conhecimento que se pretende construir. O êxito dos alunos ao trabalharem com as situações adidáticas condiciona a construção dos conhecimentos mobilizados autonomamente por eles durante a resolução dos problemas arrolados (Oliveira e Silva, 2013).

Outro fator de bastante importância reside, justamente, na ideia de que as respostas procuradas representem o conhecimento que se pretendia quando da elaboração da situação. Sobre isto, Perrin-Glorian (1999) denomina *situação fundamental* ao conjunto de situações adidáticas que proporcionam a construção de conhecimentos apoiados em uma epistemologia científica. Desta forma, pode-se dizer que a situação fundamental se refere a um conjunto característico de um saber e/ou conhecimento, de forma que os distintos valores atribuídos às variáveis didáticas devem permitir gerir as situações que representam, de forma ampla, o saber em questão (Oliveira e Silva, 2013).

Em uma situação adidática, o docente não deve declinar antecipadamente o que deseja como resposta do aluno, mas deve ter o cuidado de propor a aceitação da responsabilidade, por parte

do estudante, pela construção de propostas que venham a atender os problemas apresentados. Este movimento, a partir do qual o professor procura fazer que o aluno assuma a responsabilidade por uma situação de aprendizagem (adidática), inclusive pelas consequências desta transferência, Brousseau (2008, p.91) denomina *devolução*. Deve ser destacar que o aluno não distingue imediatamente, no contexto da situação, os elementos de origem didática daqueles de origem adidática. Para Brousseau (2008, p.89), em relação às contribuições esperadas durante a fase de devolução, "o ensino tem por objetivo principal o funcionamento do conhecimento como produção livre do aluno em suas relações com o meio adidático". Justamente por isso, o mesmo autor, (2008, p.90) indica que "o aluno adquire conhecimentos por meio de diversas formas de adaptação às restrições de seu entorno", ressaltando que "o valor dos conhecimentos adquiridos dessa forma depende da qualidade do meio como motivador de um funcionamento 'real', cultural, do saber".

Ainda sobre os fundamentos da TSD, Brousseau (1986) denominado de *milieu*, que deve ser organizado pelo docente, ao sistema sobre o qual os aprendizes agem e, se detiver caráter antagônico, retroage justamente em relação a estas ações, fornecendo elementos para que surjam aprendizagens. Para o autor, o *milieu* sem intencionalidade didática não é adequado ao processo de construção do conhecimento. Para Oliveira e Silva (2013), o *milieu* notadamente antagonista deve permitir ao aluno agir de modo autônomo em relação às situações que participa e em relação às interações junto ao professor, dando condições ao aluno de refletir sobre seus posicionamentos e ações. Desse modo, o aluno aprende corrigindo suas ações e antecipando os efeitos, justamente a partir de retroações em relação ao *milieu*. Assim, as situações e em que os alunos estão inseridos (com intuito didático) são para eles o *milieu* de referência, sobre o qual exercem a sua capacidade de construir conhecimento e aprendizado (Oliveira e Silva, 2013).

Para Almouloud (2007, p. 36), o processo de análise proposto na TSD é decomposto em quatro fases, em relação às quais o saber ostenta diferentes funções, e que reservam ao estudante distintas relações com este mesmo saber. Para o autor:

> Brousseau modela as situações adidáticas em termos de um jogo. Uma situação suscetível de provocar uma aprendizagem será tal que o aluno dispõe de uma estratégia básica para começar a jogar. Tal estratégia deve permitir ao sujeito compreender o problema e as regras do jogo. No entanto, as retroações fornecidas pelo *milieu* lhe permitem também perceber que essa estratégia não permitirá ganhar o jogo ou então que seu custo didático ou cognitivo é muito grande. Uma estratégia ótima deveria ser criada ou

> viabilizada utilizando-se [do] conhecimento visado (ALMOULOUD, 2007, p.36).

Dentre as fases indicadas, na lógica do jogo supramencionada, na de *ação*, o aluno é levado a tomar decisões e os saberes passam a ser colocados em prática a fim de solucionar o problema proposto. Na fase de *formulação*, as estratégias para solucionar o problema são explicitadas, enquanto que a fase de *validação* ocorre visando uma correção cultural ou empírica, para garantir a pertinência, adequação, adaptação ou conformidade dos conhecimentos mobilizados. Por fim, na *institucionalização*, o professor retoma o que foi realizado no trabalho de pesquisa dos estudantes, em sessões coletivas, e sintetiza este saber, fixando o estatuto válido do conhecimento matemático (Oliveira e Silva, 2013).

Em um contexto mais geral, no âmbito das interações que ocorrem durante uma situação construída para proporcionar a aquisição de certo conhecimento, as fases mencionadas aqui estão profundamente interligadas, permitindo ao aluno a responsabilidade pela gestão de sua relação com o saber nas dialéticas de ação, formulação e validação. Ao professor, cabe a responsabilidade pelas atividades relativas à institucionalização. Para Oliveira e Silva (2013), analisar o processo compreendido pelo trabalho dos agentes da relação didática em relação ao saber em todas estas fases possibilita um melhor entendimento de como o conhecimento é construído no decorrer da situação em que está inserido. Assim, em um primeiro momento, o saber está ligado ao contexto da situação; posteriormente, é descontextualizado, ganhando assim um *status* de objeto de estudo, e, finalmente, é recontextualizado, passando a ser uma ferramenta para ser usada em outras situações (Oliveira e Silva, 2013).

Com base nestes pressupostos, o objetivo deste estudo é o de constituir situações de aprendizagem, compostas por construções adidáticas nas quais se inserem problemas relativos ao uso de diferentes crivos aplicáveis aos números primos. A situação fundamental, que condicionará o conhecimento que se pretende construir, será permeada pela consolidação de saberes relativos aos números primos e ao teorema fundamental da aritmética, bem como a aplicação destes conhecimentos como ferramentas para a resolução de outros problemas, como os relativos à criptografia.

Os sujeitos em relação aos quais as situações serão propostas são alunos de licenciatura em Matemática da Universidade Estadual do Pará, ou seja, futuros professores de Matemática, que deverão, por sua vez, ter conhecimentos suficientes para trabalharem com este conteúdo

no Ensino Básico. As interações e respostas obtidas serão analisadas sob a abordagem qualitativa, por meio de uma proposta descritiva e interpretativa, que considera a importância do processo mais do que de resultados quantitativos, propriamente ditos, ainda que leve estes últimos em consideração (Bogdan e Bliken, 1994).

É neste contexto que os futuros professores de Matemática, sujeitos desta pesquisa, irão trabalhar. Entretanto, seus conhecimentos não deveriam ser limitados àqueles compatíveis com os estudantes do Ensino Fundamental, mas serem mais amplos, de modo que tenham competência para a compreensão e elaboração de atividades que estimulem a investigação que leve à apropriação, por exemplo, dos conhecimentos proporcionados pelos crivos, apresentados a seguir.

Crivos de primalidade

O Crivo de Eratosthenes

A rigor, Crivos são essencialmente geradores de números primos. Cada um tem sua importância de acordo com sua simplicidade, velocidade e implementação computacional. Neste artigo, adapta-se o funcionamento de cada crivo para torná-los um tipo de critério para testar a primalidade de um inteiro positivo ímpar. Claro que por ser uma adaptação, deve se usar de forma muito criteriosa.

O Teorema que diz "se um inteiro positivo a > 1 é composto, então a possui um divisor primo $p \leq \lfloor \sqrt{a} \rfloor$ e seu corolário: "se um número a não possui nenhum fator primo *p*, tal que $2 \leq p \leq \lfloor \sqrt{a} \rfloor$, então a é número é primo", fornecem um processo que permite reconhecer se um dado inteiro $a > 1$ é primo ou é composto, para o que basta dividir *a* sucessivamente pelos primos que não excedem o valor $\lfloor \sqrt{a} \rfloor$. Tal resultado é a base do chamado Crivo de Eratosthenes.

Nicômaco, em sua Aritmética, publicada por volta do ano 1000 d.C., introduz o crivo de Eratosthenes da seguinte forma:

> O método para obter números primos é chamado por Eratosthenes uma peneira, porque tomamos números ímpares misturados de maneira indiscriminada e, por este método, como se fosse pelo uso de um instrumento ou peneira separamos os primos ou indecomponíveis dos secundários ou compostos.[ ] (COUTINHO, 2000, p. 62)

A construção de uma tabela de números primos que não excedam um dado inteiro ímpar *n* usando o Crivo de Eratosthenes consiste no seguinte: escrevem-se, na ordem natural, todos os

inteiros ímpares a partir de 3 até *n* (só listamos os ímpares, pois 2 é o único primo par). O primeiro número da lista é o 3; risca-se (o que equivale a eliminar) os múltiplos de 3 maiores que ele próprio. Em seguida procuramos o menor elemento da lista, maior que 3, que não tenha sido riscado; que é o 5. Risca-se os múltiplos de 5 maiores que ele próprio. Em seguida procuramos o menor elemento da lista, maior que 5, que não tenha sido riscado; que é o 7. Risca-se os múltiplos de 7 maiores que ele próprio. Em seguida procuramos o menor elemento da lista, maior que 7, que não tenha sido riscado; que é o 11. E assim por diante, até chegar a *n*; por fim, adiciona-se o 2 à lista.

Como exemplo no método supramencionado, segue a construção da tabela de números primos menores que 100.

Como $\lfloor\sqrt{100}\rfloor = 10$, basta eliminar sucessivamente da tabela os números que são múltiplos dos primos *p* menores que ou iguais a 10, ou seja, 3, 5 e 7 e restarão os seguintes primos: 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97.

Considerando o objetivo de usar os crivos como critério para testar a primalidade, o crivo de Eratosthenes pode ser usado da seguinte maneira: Se *n* é um ímpar em relação ao qual se pretende verificar se é ou não primo, o crivo sugere o seguinte procedimento:

- Extrai-se o piso da raiz quadrada de *n*: $\lfloor\sqrt{n}\rfloor$;
- Divide-se *n* por todos os primos *p* menores que ou iguais a *n*;
- Se *n* não for divisível por nenhum dos primos *p*, então *n* é primo.

- **Estabelecendo o critério de Eratosthenes para verificar se 1073 é primo**

Para responder a esta questão, é preciso possuir acesso a uma determinada quantidade de primos que satisfaçam a necessidade do problema, isto é, para saber se um número é realmente primo, de início, precisa-se de alguns primos. Ou seja, ao extrair o piso da raiz quadrada de 1073, $\lfloor\sqrt{1073}\rfloor = 32$, deve-se conhecer todos os primos menores ou iguais a 32 $(2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31)$; caso 1073 não seja divisível por nenhum desses primos, então ele é primo. Entretanto, $1073 = 29\ x\ 37$, ou seja, é divisível por 29, logo não é primo. Note que o outro fator, $37 > \lfloor\sqrt{1073}\rfloor$, não chega a ser testado.

Crivo de Sundaram

O Crivo de Sundaram baseia-se numa matriz formada a partir de números em progressões aritméticas (*PA*). Em outras palavras, sequências de números em que os números da sucessão estão a uma determinada distância fixa, chamada de razão da *PA*.

Por exemplo, tome-se a sequência infinita em que os números da sucessão formam uma *PA* de razão $r_1 = 3$ e primeiro termo $a_1 = 4$: 4, 7, 10, 13, 16, 19, 22, 25, ...

Em seguida, uma **segunda** *PA* de razão = $2 + r_1 = 5$, cujo primeiro termo é o **segundo** termo $a_2=7$ da primeira PA, isto é, 7, 12, 17, 22, 27, 32, 37, 42, ...

Agora, uma **terceira** *PA* de razão = $2 + r_2 = 7$, cujo primeiro termo é o **terceiro** termo $a_3=10$ da primeira *PA*, ou seja, 10, 17, 24, 31, 38, 45, 52, 59, ...

Pode-se perceber o padrão emergente: Cada linha *i*, tem como primeiro termo o termo a_i da primeira PA e a razão de uma *PA* na linha i e dada por $3+2(i-1)$.

Escrevendo as sequências aritméticas uma abaixo da outras, na forma de uma matriz infinita *S*, tem-se:

4	7	10	13	16	19	22	25	28
7	12	17	22	27	32	37	42	47
10	17	24	31	38	45	52	59	66
13	22	31	40	49	58	67	76	85
16	27	38	49	60	71	82	93	104
19	32	45	58	71	84	97	110	123
22	37	52	67	82	97	112	127	142...

A matriz apresenta a seguinte estrutura: a primeira linha é igual a primeira coluna, a segunda linha é igual a segunda coluna, a terceira linha é igual a terceira coluna e assim sucessivamente, cada linha é uma progressão aritmética, e as razões das progressões consecutivas formam uma sequência 3, 5, 7, 9, 11, 13, 15, 17, ..., que também é uma *PA* de razão 2.

Em seguida, escolhe-se qualquer número nesta matriz, multiplica-se por 2 e adiciona-se 1, verificando se o número resultante é primo. Na verdade, repetindo o procedimento algumas vezes, será possível constatar que, não importa o número eleito dentro da matriz, um número primo jamais será obtido.

O que poderia ser dito em relação aos números que não estão na matriz, por exemplo, 5, 6 e 8? Para um número q que não está na matriz, o número $2q+1$ é primo.

Desta forma, de acordo com o Crivo de Sundaram, pode-se dizer que:

- Se q encontra-se na matriz S, então $2q+1$ não é primo;
- Se q não se encontra na matriz S, então $2q+1$ é primo.

Podem-se resumir essas duas proposições em uma só: $2q+1$ é primo, se e somente se, q não está na matriz S.

De outra forma, segue a demonstração:

Pode-se começar determinando uma fórmula de entrada na matriz S. O primeiro termo na n-ésima linha é $4+3(n-1) = 3n+1$. A diferença comum na progressão aritmética compreendida na n-ésima linha é $2n+1$; assim, o m-ésimo número na n-ésima coluna é

$$3n + 1 + (m - 1)(2n + 1) = (2m + 1)n + m$$

Então, se q aparece na matriz S, então $q = (2m + 1)n + m$ para algum par de inteiros m e n. Assim, $2q + 1 = 2(2m+1)n + 2m + 1 = (2m + 1)(2n + 1)$ é composto. Mostra-se, agora, que, se q não aparece na matriz S, então $2q + 1$ é primo, ou de modo equivalente, se $2q + 1$ não é primo, então c aparece na matriz. Então, suponha-se que $2q + 1 = a.b$, onde a, b são inteiros maiores que 1.

Uma vez que $2q + 1$ é ímpar, a e b devem ser ímpares também, logo

$$a = 2p + 1 \text{ e } b = 2t + 1.$$

Assim,

$$2q + 1 = a.b = (2p + 1)(2t + 1) = 2p(2t + 1) + 2t + 1$$

e

$$q = (2t + 1)p + t.$$

Isso significa que q é o t-ésimo número da p-ésima linha na matriz S.

Conclui-se que $2q + 1$ é um número primo se, e somente se, q não aparece na matriz S.

Teste de Primalidade de Sundaram

O crivo de Sundaram estabelece apenas que se um número q estiver na matriz de Sundaram, então $2q + 1$ não é primo, mas se q não aparece na matriz, então $2q + 1$ é primo. Considera-se a situação contrária. Analisa-se se um número p é ou não primo, tentando determinar se $q = (p - 1)/2$ está ou não na matriz.

Como exemplo, quer-se verificar se 2573 é primo pelo crivo de Sundaram.

De acordo com o crivo de Sundaram, para garantir que 2573 seja primo, é necessário assegurar que, na matriz de Sundaram, não exista nenhum número q, tal que $2q + 1 = 2573 \rightarrow q = 1286$ não esteja na matriz e também que não exista m e n inteiros positivos tais que $(2m + 1)(2n + 1) = 2573$, que indicaria uma linha e uma coluna onde q se encontraria.

$(2m + 1)(2n + 1) = 2573$

$$4mn + 2m + 2n + 1 = 2573$$

$4mn + 2m + 2n = 2572$

$$2(2mn + m + n) = 2572$$

$2mn + m + n = 1286$

Se existirem tais valores de $m > 0$ e $n > 0$, eles são menores que q. Testando vários valores de m, obtêm-se os seguintes valores de n:

m	$2m + 1$	$\frac{p}{2m+1} = 2n + 1$	n
1	3	$\frac{2573}{3} = 857{,}666\ldots$	$428{,}333\ldots$
2	5	$\frac{2573}{5} = 514{,}6$	$256{,}8$
3	7	$\frac{2573}{7} = 367{,}571\ldots$	$183{,}286\ldots$
4	9	$\frac{2573}{9} = 285{,}888\ldots$	$142{,}444\ldots$
5	11	$\frac{2573}{11} = 233{,}909\ldots$	$116{,}455\ldots$

6	13	$\frac{2573}{13} = 197{,}923\ldots$	$98{,}4615\ldots$
7	15	$\frac{2573}{15} = 171{,}533\ldots$	$85{,}2667\ldots$
8	17	$\frac{2573}{17} = 151{,}353\ldots$	$75{,}1765\ldots$
9	19	$\frac{2573}{19} = 135{,}421\ldots$	$67{,}2105\ldots$
10	21	$\frac{2573}{21} = 122{,}524\ldots$	$60{,}7619\ldots$
11	23	$\frac{2573}{23} = 111{,}87\ldots$	$55{,}4348\ldots$
12	25	$\frac{2573}{25} = 102{,}92$	$50{,}96$
13	27	$\frac{2573}{27} = 95{,}2963\ldots$	$47{,}1481\ldots$
14	29	$\frac{2573}{29} = 88{,}7241\ldots$	$43{,}8621\ldots$
15	31	$\frac{2573}{31} = 83$	41

Como $m = 15$ e $n = 41$ satisfazem a equação $(2m + 1)(2n + 1) = 2573$, logo q = 1286 aparece na matriz de Sundaram na linha 15 e coluna 41 e vice-versa. Por conseguinte, 2573 não é primo.

Crivo de Atkin

Em seu artigo *Prime Sieves Using binary Quadratic Forms*, Atkin e Bernstein (2003), apresentaram um engenhoso algoritmo para gerar números primos que ficou conhecido como Crivo de Atkin. Apesar deste crivo não ser um teste de primalidade, pode-se mostrar que é possível adaptá-lo para se transformar, dentro do possível, em um teste eficiente se for utilizado de trás para frente. Isto é, a partir de um inteiro positivo ímpar, determinar valores intermediários *x* e *y* que satisfaçam as condições do algoritmo criado por Atkin e Bernstein.

O crivo de Atkin tenta representar um inteiro candidato *n* em três formas possíveis:

$$n = 4x^2 + y^2$$

$$n = 3x^2 + y^2$$

$$n = 3x^2 - y^2$$

com x e y variando entre 1 e $\sqrt{l}$, onde l é o limite superior até onde se pretende verificar as soluções inteiras positivas para uma das equações acima.

Para a escolha da equação diofantinas quadráticas, é necessário verificar se n deixa alguns restos específicos, módulo doze:

- $n = 4x^2 + y^2$, se $n \equiv 1 (\mathrm{mod}\, 12)$ ou $n \equiv 5 (\mathrm{mod}\, 12)$
- $n = 3x^2 + y^2$, se $n \equiv 7 (\mathrm{mod}\, 12)$
- $n = 3x^2 - y^2$, se $n \equiv 11 (\mathrm{mod}\, 12)$ e $x > y$

Então, de acordo com a teoria do Crivo de Atkin, se n tiver uma quantidade ímpar de de soluções (x, y) positivas, dentro de um intervalo específico, então n é considerado um número primo.

Teste de Primalidade de Atkin

Basicamente, o crivo de Atkin gera números primos a partir da contagem de soluções positivas (x, y), dentro de um intervalo determinado, em determinadas equações diofantinas quadráticas. Cada número n que se queira testar deve ser associado à uma equação que está relacionada com um resto de n na divisão por 12, que seja relativamente primo com 12; os restos da divisão por 12 que são relativamente primos com 12 são 1, 5, 7 e 11.

Logo, se o objetivo for utilizar o crivo de Atkin como teste de primalidade, então é necessário verificar qual o resto deixado por um número ímpar $n > 1$ ao ser dividido por 12 e testá-lo na equação correspondente.

Como exemplo, mostra-se o critério de Atkin para verificar se 1069 é primo.

Dividindo 1069 por 12, obtém-se resto 1 e de acordo com o que foi visto, deve-se contar o número de soluções inteiras positivas (x, y) existentes na equação diofantina quadrática $4x^2 + y^2 = 1069$, num certo intervalo.

Para esta equação, pode-se considerar o seguinte: o produto $4x^2$ é sempre par; logo, y^2 é ímpar, pois a soma de uma parcela par com uma parcela ímpar resulta em 1069, que é ímpar.

Como y^2 é ímpar, então y também é ímpar. A princípio, nada se pode afirmar sobre a paridade de x. Entretanto, $0 < x < 16$, como mostrado a seguir:

$4x^2 + y^2 = 1069$

$y^2 = 1069 - 4x^2$

$y = \sqrt{1069 - 4x^2}$

$1069 - 4x^2 > 0$

$1069 > 4x^2$

$x^2 < \frac{1069}{4}$

$x^2 < 267{,}25$

$x < 16{,}34$

Por inspeção, $x = 15$, o que resulta em $y = 13$, única possibilidade de (x, y) inteiros positivos.

O crivo de Atkin alterna a condição de primalidade de um número de acordo com o número de soluções positivas que possui na sua equação diofantina quadrática num determinado intervalo. Como sempre haverá pelo menos uma solução inteira positiva, o número passa a ser considerado primo; porém, ao se obter uma segunda solução, o número passa a ser considerado composto e assim sucessivamente.

Em resumo, para que o número seja considerado primo, de acordo com esse teste, deve possuir uma quantidade ímpar de soluções positivas dentro do intervalo estabelecido. Neste exemplo, provou-se que 1069 é primo, pois há somente uma solução positiva (x, y) para a sua equação diofantina quadrática.

Considerações Finais

Atualmente, a pesquisa está na fase de elaboração das sequências didáticas, buscando adaptar as características dos crivos apresentados às investigações que os estudantes serão levados a fazer. As sequências serão aplicadas no ambiente da Universidade do Estado do Pará, com sujeitos voluntários, em regime extracurricular. A partir daí serão organizadas as análises, usando como suporte o cabedal teórico e metodológico apresentado neste trabalho.

Referências

ATKIN, Arthur L.; BERNSTEIN, Daniel J. **Prime sieves using binary quadratic forms,** 2003. Disponível em: http://cr.yp.to/papers/primesieves-19990826.pdf. Acesso em: 11 de julho de 2013.

ALMOULOUD, Saddo Ag. **Fundamentos da didática da matemática**. 1. Ed. Curitiba: Ed. UFPR, 2007.

BOGDAN, Robert; BLIKEN, Sari. **Investigação qualitativa em educação**: uma introdução à teoria e aos métodos. Porto: Porto Editora,1994.

BROUSSEAU, Guy. **La théorisation des phénomènes d'enseignement des mathématiques**. Thèse d'état, 1986. Disponível em: http://guy-brousseau.com/46/resume-de-la-these-detat-1986/. Acesso em: 15 de fevereiro de 2012.

BROUSSEAU, Guy. **Introdução ao estudo das situações didáticas:** Conteúdos e métodos de ensino. 1. ed. São Paulo: Ática, 2008.

BROUSSEAU, Guy. **La théorie des situations didactiques**. In : Université de montréal, 1997. Disponível em: http://guy-brousseau.com/1694/la-theorie-des-situations-didactiques-le-cours-de-montreal-1997. Acesso em: 13 de mar. 2012.

COUTINHO, Severino Collier; **Números Inteiros e Criptografia RSA**; Rio de Janeiro: Série Computação e matemática, IMPA; 2000.

OLIVEIRA, Gerson P; SILVA, Eliza S. **Transformação linear em um curso de licenciatura em matemática: uma proposta didática em estudo**. Anais do XI ENEM. Curitiba: PUC/PR, 2013.

PERRIN-GLORIAN, Marie-Jeanne. **Problèmes d´articulaton de cadres théoriques:** l'exemplie du concept de milieu. Recherches em didactique dês mathématiques. Vol.19, nº3, pp. 279-322, 1999.

Recebido em: 06/12/2013
Aceito para publicação em: 26/12/2013