Matemática Universitária Nº 15, dezembro de 1993, 1-12

Existem funções que geram os números primos?

Paulo Ribenboim*

Começamos listando alguns números primos: $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, $p_4 = 7$, $p_5 = 11$, $p_6 = 13$, $p_7 = 17$, $p_8 = 19$, $p_9 = 23$, $p_{10} = 29$,... .

Todos nós conhecemos a definição de um número primo:

"Um número primo é um número natural maior que 1 cujos únicos divisores são 1 e ele próprio".

O conjunto dos números primos é portanto um subconjunto do conjunto *IN* dos números naturais. Nós nos propomos estudar um subconjunto de *IN*, para cuja definição necessitamos apenas da multiplicação enquanto que para o conjunto *IN* necessitamos da *adição,* da *multiplicação* e de uma *relação de ordem.*

Sempre que desejamos estudar um subconjunto de um conjunto, nos ocorrem várias questões bastante naturais tais como:

1) *Quanto?* Isto é quantos números primos existem?

2) *Como gerá-los?* Existem meios de produzir números primos? Em outros termos, é possível encontrar fórmulas que geram os números primos?

3) *Como reconhecer um número primo?* Dado um número natural é possível dizer se ele é primo ou não? Como fazê-lo?

Existem outras questões relativas à *distribuição* dos números primos:

4) Como são repartidos os números primos entre os números naturais? Quantos números primos existem entre 1 e um milhão? Entre 1 e um bilhão? Como se determina os números primos em um intervalo dado, por exemplo, [a, 2a]? Existem aqui dois aspectos a considerar: a primeira questão é um problema *global* de distribuição; a segunda é um problema *local.* Não trataremos disto nestas notas.

Retornemos à primeira questão. Observa-se imediatamente que ela não é evidente a priori pois o subconjunto dos números primos é dado pela propriedade:

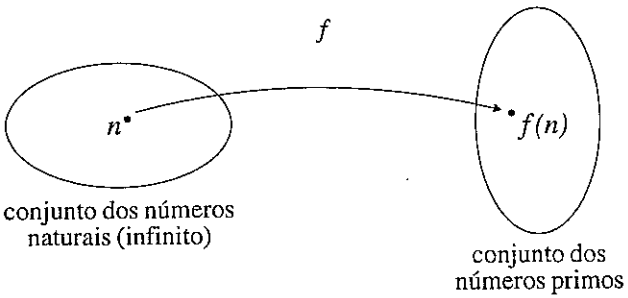
---

* Traduzido do francês pelo Professor Antônio Paques, a quem os editores consignam aqui seus agradecimentos.

"n é primo se não tem divisores exceto 1 e ele próprio".

Inicialmente, recordemos um velho resultado muito bonito, devido à EUCLIDES, que assegura a existência de uma infinidade de números primos. Como mostramos que um conjunto é infinito? Podemos fazê-lo de duas maneiras essencialmente diferentes:

a) Podemos compará-lo com um outro conjunto infinito, encontrando uma *injeção* tal como:



$$f: n \longmapsto f(n) \text{ primo}$$

Abordaremos este método direto posteriormente.

b) É impossível que o conjunto dos números primos seja finito pois, se este for o caso, é possível mostrar que existe um outro número primo maior que todos os inicialmente considerados. Este método de demonstração é indireto, ele é baseado em uma contradição. De fato, foi por absurdo que EUCLIDES procedeu. Analisaremos esta demonstração, de onde poderemos tirar alguns problemas interessantes.

A demonstração de EUCLIDES é a seguinte:

Suponhamos que $q_1, q_2, \ldots, q_n$ sejam todos os números primos sem exceção. Vamos construir um outro número primo diferente de todos esses. Para isso consideremos o número

$$N = q_1 \cdot q_2 \cdot \ldots \cdot q_n + 1.$$

Temos então duas alternativas:

- N é primo e neste caso nada mais resta a verificar pois N é maior que todos os outros e portanto diferente deles.

- N não é primo. Por definição, ele possue um fator primo q necessariamente menor que ele. Nestas condições:

$$N = q \cdot m = q_1 \cdot q_2 \cdot \ldots \cdot q_n + 1.$$

q divide N e não pode ser nenhum dos fatores $q_1, q_2, \ldots, q_n$, pois, nesse caso, dividiria 1 que é a diferença entre $q.\ m$ e $q_1 \cdot q_2 \cdot \ldots \cdot q_n$. Portanto q é um número primo diferente daqueles considerados inicialmente.

Este estudo é bem conhecido. Entretanto, analisemos as alternativas que ocorrem na demonstração.

No primeiro caso, temos um procedimento muito simples de se obter um novo número primo: efetua-se o produto dos números primos inicialmente dados e adiciona-se 1 ao resultado. Podemos portanto imaginar esse procedimento aplicado uma infinidade de vezes e obter dessa forma um processo construtivo para produzir uma infinidade de números primos. Isto é muito interessante.

No segundo caso, observamos que é possível obter uma infinidade de números primos mas o caráter construtivo desaparece. Não se conhece o divisor de N. Há, portanto, neste caso, uma indeterminação. Esta questão tem despertado o interesse de muitos.

Denotemos por $p^{\#}$ o produto de todos os primos $q \leq p$.

Questão: Existem uma infinidade de números p tais que $p^{\#} + 1$ seja primo?

Eis, portanto, uma questão cujo enunciado é elementar e pode ser estudada com o auxílio de micro-computadores. É suficiente fazer os cálculos para ver o que se passa experimentalmente. A partir da observação experimental pode-se fazer hipóteses e conjecturas e tentar demonstrar estas de maneira rigorosa. Devo confessar-lhes que isto é difícil. O maior número primo conhecido e obtido dessa maneira é $4787^{\#} + 1$. É o maior obtido até o momento e entre os números de mesmo tipo existem somente dez primos inferiores a este. $4787^{\#} + 1$ é portanto o décimo primeiro. Tem-se, portanto, muito pouco. "Ter-se muito pouco" não quer dizer nada ou, mais exatamente, quer dizer que existe uma densidade fraca. As questões relativas à procura de conjuntos com baixa densidade são evidentemente muito difíceis. A moral de tudo isto é que não é, de forma alguma, fácil encontrar processos para gerar números primos e isto nos conduz à nossa segunda grande questão: Como gerá-los?

Todos nós já procuramos, em algum momento, encontrar uma fórmula para descrever os números primos. Não sei se vocês sabem o que significa: "Encontrar uma fórmula." Vou expor três significados possíveis.

Antes, recordo que existem conjuntos de números que são gerados mecanicamente por recorrência. Por exemplo, os números de FIBONACCI. Vocês começam por $u_0 = 1$ e $u_1 = 1$ e aplicam a regra:

$$u_n = u_{n-1} + u_{n-2}.$$

Se vocês conhecem dois, vocês conhecem o seguinte. Trata-se de uma

geração por recorrência de segunda ordem. Existe alguma coisa semelhante para os números primos? Já vimos que para os números primos, seguramente, não há nada assim tão simples, mas existe, talvez, algo ainda que mais complicado?

Vou propor-lhes três questões:

Para alguém muito otimista, pode-se propor como problema:

a) Encontrar uma função f tal que:

$\forall\, n \quad f(n) = p_n$ onde p_n é o n-ésimo número primo.

Para alguém um pouco menos exigente:

b) Encontrar uma função f tal que:

$\forall n \quad f(n)$ é primo e se $n \neq m$ então $f(n) \neq f(m)$.

O problema b) requer encontrar uma forma de gerar uma infinidade de números primos enquanto que o problema a) requer encontrar todos os números primos em uma certa ordem. É, de fato, exigir muito. Em b) requer-se encontrar uma infinidade de números primos mas não em uma boa ordem e talvez nem todos. O que seria portanto uma nova demonstração da existência de uma infinidade de números primos por um método direto como já manifestado anteriormente.

A terceira maneira de propor o problema provém de uma certa verificação das duas primeiras. Nós vamos ver que para chegar às duas primeiras há a necessidade de funções muito complicadas. As funções complicadas não são desejáveis porque ao procurar descrever os números primos por meio de coisas que não se conhece muito bem, muito pouco, ou nada, há a se ganhar. O que se deseja é estudar coisas que são difíceis descrevendo-as através de coisas que são mais fáceis. Se os números são expressos, por exemplo, em termos de logaritmos ou de outras funções mais complexas, as quais não se pode nem mesmo calcular - o que vem a ser o caso - então nada se ganha. Resta, contudo, as funções mais simples: os polinômios. Seria desejável poder-se descrever os números primos através deles. Daí, portanto, a terceira formulação:

c) Descrever o conjunto de números primos por meio de polinômios.

Vocês perceberam que existem diferentes níveis de exigência ao se considerar o problema: "Como gerá-los?". Vou apresentar-lhes, a título de exemplo, no que concerne à questão a), algumas fórmulas absolutamente inúteis. Vocês podem se surpreender mas vou mostrar-lhes em que elas são totalmente inúteis e esta é a única razão porque lhes observo isto.

Para citar a primeira, é necessário, inicialmente, recordar um belo teorema. Este teorema é verdadeiro para os números inteiros que são primos e é falso para todos os outros, o que é, de qualquer forma, muito raro. Trata-se do teorema de WILSON:

Consideremos o número $N = (n-1)! + 1$

Duas coisas podem ocorrer:

* N é divisível por n.

* N não é divisível por n.

O primeiro caso ocorre se e somente se n primo. Isto é fácil de demonstrar. O matemático inglês WILSON fez essa demonstração no século XVIII. Esse teorema nos permite descrever a primeira fórmula:

$$F(1) = 1$$

$$F(j) = \left[\cos^2 \frac{\pi ((j-1)! + 1)}{j} \right], \quad \text{onde } [x] \text{ denota a parte inteira de } x.$$

De acordo com o teorema de WILSON temos portanto:

$$F(j) = \begin{cases} 1 & \text{se } j = 1 \text{ ou } j \text{ é primo} \\ 0 & \text{caso contrário .} \end{cases}$$

Se desejamos fazer a soma dos F(j) de 1 a 1000, cada vez que obtemos um 1 isto significa que encontrarmos um número primo e que, portanto, devemos contar 1 tantas vezes quantos são os números primos de 1 a 1000. Isto é descrito pela seguinte fórmula:

$$\sum_{j=1}^{m} F(j) = 1 + \Pi(m) \ .$$

A função Π é a famosa função da teoria de números primos que conta os números primos até m. Por exemplo $\Pi(29) = 10$; eu não conheço $\Pi(100)$ mas é possível calculá-lo. Esta função é fundamental no estudo da distribuição de números primos.

Ainda no que concerne ao problema a), a fórmula dada por WILLANS em 1964 é a seguinte:

$$p_n = 1 + \sum_{m=1}^{2^n} \left[\sqrt[n]{\frac{n}{1 + \Pi(m)}} \right] , \text{ onde } [x] \text{ é a parte inteira de } x.$$

Ela é um pouco miraculosa. Nela ocorrem somas muito complicadas e ela fornece o n-ésimo número primo. Ela é inútil mas é bonita! Por exemplo, para $n = 10$ temos:

$$29 = p_{10} = 1 + \sum_{m=1}^{1024} \left[\sqrt[n]{\frac{10}{1 + \Pi(m)}} \right]$$

Observemos como essa fórmula é engraçada! Se desejamos saber qual é o décimo primo, devemos contar quantos primos existem até 1024(!!). Certamente existem muito mais que até 29(!).

Eu acho que existem pessoas preocupadas pela lógica para saber como a aritmética é "feita". Os lógicos sentem-se satisfeitos em poder dizer que é possível obter o n-ésimo número primio efetuando-se as operações perfeitamente definidas.

Vou exibir-lhes duas outras fórmulas utilizando outros tipos de funções e que são, talvez, mais agradáveis. Foi o matemático indo-americano GANDHI que demonstrou em 1971, a fórmula

$$p_n = \left[1 + \frac{1}{ln2} ln \left(-\frac{1}{2} + \sum_{d \mid P} \frac{\mu(d)}{2^d - 1} \right) \right] \text{, onde } P = p_1 \cdot p_2 \cdot \ldots \cdot p_{n-1}$$

μ é a função de MÖBIUS
$[x]$ é a parte inteira de x
$d \mid P$ significa d divide P.

Existem nessa fórmula muitos ingredientes:

ln é o logaritmo neperiano.
μ é a função de MÖBIUS, que é muito importante na teoria de números

$$\mu : \begin{cases} \mu(1) = 1 \\ \mu(d) = (-1)^m \text{ quando } d \text{ possue } m \text{ fatores 2 à 2 distintos} \\ \mu(d) = 0 \text{ nos outros casos} \end{cases}$$

Por exemplo $\mu(15) = (-1)^2 = 1$ pois $15 = 3 \cdot 5$
$\mu(20) = 0$ pois $20 = 2 \cdot 2 \cdot 5$

Nessa fórmula o número P possue muitos divisores e se desejássemos calcular, por exemplo, p_{10} seria necessário conhecer μ (d) para muitíssimos d e de novo recairíamos em uma fórmula impraticável. Mas há talvez alguma coisa escondida nesta fórmula e, sem dúvida, algum dia ela será melhor compreendida.

Vou apresentar-lhes agora uma segunda fórmula..., ou melhor, não vou fazê-lo! Vou somente dizer-lhes que existem outras fórmulas e isto é suficiente. Vocês compreenderam que a exigência do a) de encontrar o n-ésimo número primo por meio de uma fórmula explícita não nos conduziu, até agora, e não nos conduzirá, talvez jamais, à coisas interessantes.

A exigência do b) não é tão ruim assim. Dado um número inteiro, digamos 10, vou utilizar uma fórmula e o que sairá do outro lado é um número primo mas não o décimo. Se é dado o número 11, teremos um outro número primo e assim sucessivamente. Essa fórmula permite obter um número primo à partir de cada número inteiro mas ela apresenta de novo um defeito grave. Ela se escreve:

$$f(n) = \left[2^{2^{2^{\cdot^{\cdot^{\cdot^{2^{\omega}}}}}}} \right] \text{, onde [x], sempre a parte inteira de x,}$$

$2^{2^{2^{\cdot^{\cdot^{\cdot^{2^{\omega}}}}}}}$ representa n etapas de expoentes e $\omega = 1{,}92827800 \ldots$.

A existência de ω foi demonstrada e até o cálculo foi feito, mas com uma certa aproximação. É este o defeito desta fórmula. Além disso, decimais de ω são conhecidos e vocês podem calculá-los. Se não o conhecemos muito bem, podem ocorrer erros grosseiros que se superpõem e acabamos por obter um número que não é primo. Esta fórmula é devida à WRIGHT (1954). Ela faz parte de toda uma família de teoremas do mesmo tipo. WRIGHT é muito conhecido como o co-autor de um excelente livro de teoria de números: "An Introduction to the Theory of Numbers" de HARDY-WRIGHT. Este livro é extraordinário pois ele parte de questões muito simples. HARDY é um dos grandes matemáticos da teoria de números do século XX.

Até o momento não estamos muito contentes pois, como vimos até agora, para descrever os números primos somos obrigados a recorrer à fórmulas muito complicadas. Mas eu já havia observado: "os polinômios são muito mais agradáveis".

Podemos perguntar se não existe um polinômio de grau suficientemente grande, com várias indeterminadas, que possa dar um número primo toda vez que substituirmos as indeterminadas por números inteiros positivos. Para os polinômios de uma variável isto não acontece devido ao teorema seguinte:

"Se $f(X)$ é um polinômio à coeficientes inteiros com grau $d \geq 1$ e seu coeficiente dominante é maior ou igual a 1, então existe uma infinidade de inteiros n, maiores ou iguais a 1, tais que $f(n)$ é composto."

Vejamos uma demonstração rápida:

Seja $f(X) = a_0 X^d + a_1 X^{d-1} + \cdots + a_d$, a_i inteiros, $a_0 \geq 1$, $d \geq 1$.

Temos $\lim_{x \to \infty} f(x) \to +\infty$.

Desejamos mostrar que existe uma infinidade de números inteiros n para os quais $f(n)$ é composto.

Primeira alternativa:

$\forall n$ $f(n)$ é composto; nada mais resta a demonstrar!

Segunda alternativa:

$\exists n_0$ $f(n_0) = p$, p primo.

Devido ao limite infinito, o valor de f supera, a partir de um certo momento, o valor p. Então, existe n_1, que se pode tomar maior que n_0, tal que $\forall n \geq n_1$ $f(n) > p$. Vamos tentar, agora, encontrar valores compostos. Mais preci-

samente, tentaremos encontrar grandes valores n para os quais $f(n)$ é múltiplo de p.

Calculemos:

$$\begin{aligned} f(n_0 + hp) &= a_0 (n_0 + hp)^d + a_1(n_0 + hp)^{d-1} + \cdots + a_d \\ &= (a_0 n_0^d + a_1 n_0^{d-1} + \cdots + a_d) + \text{múltiplo de } p \\ &= p + \text{múltiplo de } p. \end{aligned}$$

Se tomamos h muito grande, $n_0 + hp$ vai superar n_1. Portanto, $n = n_0 + hp > n_1$ e $f(n)$ é múltiplo de p superior à p e, por conseqüência, $f(n)$ é composto. Como existe uma infinidade de h que dá tais inteiros n, a demonstração está terminada.

Acabamos de mostrar que não é possível obter o que desejávamos com os polinômios de uma variável à coeficientes inteiros. A ciência nos ensina a ser modestos! Nem sempre é possível obter-se *muitos* números primos? O que significa a palavra "muito"? Vejamos!

Sobre a questão de gerar primos por meio de polinômios conhece-se coisas muito interessantes, graças à EULER que muito contribuiu para a teoria de números. Ele sabia calcular e fez inúmeras observações, que ele não explicou. Mas estas observações despertaram a curiosidade dos matemáticos e o que ele não podia explicar na época sabe-se fazê-lo atualmente e com métodos muito poderosos da teoria de números.

Começamos pelo mais famoso polinômio de EULER:

$f(X) = X^2 + X + 41.$

Este polinômio é tal que para $n = 0,1,2,3,...,39$ $f(n)$ é primo, mas para $n = 40$

$f(40) = 40(40 + 1) + 41 = 41 \cdot 41$.

Euler encontrou outros polinômios desse tipo, que produziam números primos dando-se à variável valores inteiros sucessivos à partir do zero. O polinômio acima citado é o "maior", aquele que forneceu o maior número de primos que EULER tenha encontrado. Isto nos leva ao problema seguinte:

Para q primo, encontrar os polinômios $f(X) = X^2 + X + q$ tais que $f(n)$ seja primo, para $n = 0,1,..., q - 2$.

Uma resposta positiva a este problema seria muito bem vinda pois permitiria obter muitos números primos, não somente com um só polinômio, como já vimos que não é possível, mas com a coleção dos polinômios $X^2 + X + q$.

Após EULER a questão se torna: "Existem números primos $q > 41$ verificando o problema?" EULER não os encontrou, mas procurar e não encontrar não é prova de não existência. Todos os números que se pode examinar, por tentativa empírica, são sempre, em um certo sentido, "pequenos", pois após há tantos outros!! Torna-se necessário, portanto, encontrar uma demonstração. Isto se faz

relacionando-se esta questão à outras questões, em um contexto sobre o qual eu vou dizer duas palavras.

Existe uma relação muito direta com a teoria de classificação das formas binárias - portanto com o estudo dos corpos imaginários - e a determinação dos corpos que têm um número de classe igual a 1. São conhecidos alguns exemplos de tais corpos, dos quais o "maior" correspondendo à $X^2 + X + 41$ é $\varphi(\sqrt{-163})$.

Foi necessário aguardar HEEGNER em1952, completado por BAKER em 1966 e STARK em 1971, os quais utilizaram métodos muito sofisticados da teoria de formas modulares elípticas, para estabelecer que $\varphi(\sqrt{-163})$ é de fato o "maior".

Este é portanto um problema resolvido. Este problema, que acabo de fazer surgir de meu chapéu tal como um mágico, não aparece por "acaso". Para que um problema seja interessante é necessário colocá-lo em um contexto e observar que ele é apenas um dos problemas possíveis em meio a questões múltiplas.

Trabalhamos até agora com polinômios de grau 2 particulares. Poderíamos, é claro, procurar outros tipos de polinômios de grau 2, com coeficientes mais complicados - fazendo, por exemplo, mudanças de variáveis - mas pode-se mostrar que o problema se reduz essencialmente ao estudo dos polinômios $X^2 + X + q$.

Mas porque não se interessar por polinômios de grau 1 e após, talvez, passar aos polinômios cúbicos? Eu retorno sempre a esta questão!

Vejamos o caso dos polinômios de grau 1 da forma $f(X) = aX + b$. Naturalmente, $f(0)$ deve ser primo e portanto nos interessam os polinômios da forma $f(X) = aX + q$, onde q é um primo dado. Queremos saber se este polinômio terá valores primos para X = 1,2,... Observemos ainda que $f(q)$ não é primo e que na melhor situação possível teremos $f(0), f(1),..., f(q-1)$ primos. Existem tais polinômios? Isto reduz-se finalmente a procurar um inteiro a tal que $q, q + a, q + 2a,..., q + (q - 1)a$ sejam primos. Em outros termos:

Existe uma progressão artimética começando por q tendo q termos, cada um primo?

Este é o mesmo problema que tínhamos com $X^2 + X + 41$. Progressões aritméticas, números primos; isto lembra-nos alguma coisa: um teorema muito importante que relaciona progressão aritmética e números primos. Este teorema é devido à DIRICHLET e diz que dado uma progressão aritmética que começa por q e de razão a tal que $mdc(q,a) = 1$, é possível encontrar na progressão $q, q + a, q + 2a,...$ uma infinidade de números primos. Mas não é sabido onde eles se encontram. Por exemplo, para $q = 1$, $a = 1$ obtém-se a seqüência dos números naturais que contém uma infinidade de números primos!

O que desejamos agora é muito mais exigente. Desejamos somente um número finito de primos e desejamos obtê-los rapidamente. Se fosse sabido que as progressões aritméticas fornecem primos rapidamente, poder-se-ia resolver o primeiro caso do problema de FERMAT.

Vamos, de qualquer forma, começar a resolver nosso problema.

Para $q = 3$, é necessário encontrar três números primos.

Tentemos $a = 2$: 3,5,7. Conseguimos!

Para $q = 5$, procuremos cinco números primos.

Tentemos $a = 2$: 5,7,9; não é bom!

Tentemos $a = 4$: 5,9; tampouco é bom!

Vocês vêem a que somos levados? A tentar!

Existe um teorema que diz que não é necessário tentar números muito pequenos.

Vejamos o 6: 5, 11, 17, 23, 29; este funciona!

Continuemos.

Para $q = 7$, devemos encontrar sete números primos. O teorema ao qual me referi acima - trata-se de um teorema de LAGRANGE, muito elementar - nos diz que é necessário tentar uma razão a pelo menos igual ao produto dos primos que precedem 7 isto é, pelo menos igual a $2 \cdot 3 \cdot 5 = 30$.

Tentemos 30: 7, 37, 67, 97, 127, 157, 187 = 11.7. Que azar!

Tentemos um número maior que 30. O primeiro que se encontra é 150. Este nos dá: 7,157,307, 457,607, 757, 907, sete números primos. Este funciona, mas isto começa a ficar ruim porque, de imediato, já é necessário tentar uma razão muito grande. Eu procurei para $q = 11$ mas não pude encontrar uma razão a que fosse conveniente. Contudo, conheço um calculador muito bom na Alemanha. Ele encontrou o resultado seguinte:

$$a = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 7315048 = 1536160080 .$$

Para 11 a razão a é grande demais!

Para q = 13, a razão a é maior ainda!

$$a = 9918821194590$$

Que lição tiramos de tudo isto?

O assunto é extremamente difícil. O problema é saber se é possível encontrar um número, tão grande quanto se deseje, de primos em progressão aritmética. Se vocês me perguntam se é possível encontrar treze primos sucessivos em progressão aritmética, eu respondo que sim. É sabido fazê-lo até mesmo para 19. Mas isto conduz a cálculos astronômicos e não se sabe demonstrar que para todo q, existem q primos em progressão aritmética.

Isto tudo nos leva a uma questão bem mais modesta: aquela dos polinômios tendo ao menos um valor primo, que pode ser enunciada assim:

É verdade que para todo polinômio $f(X)$, tendo seus coeficientes inteiros com mdc igual a 1, de grau maior ou igual a 1, existe um número natural n tal que $f(n)$ seja primo?

Esta é a conjectura de SCHINZEL e SIERPINSKI. Ninguém sabe demonstrá-la. Uma conjectura é uma coisa que não se conseguiu demonstrar mas deseja-se

que seja verdade. Então assume-se que ela seja verdade e *tira-se conseqüências.* As conseqüências são deduzidas rigorosamente desta hipótese e quando se recai em uma conseqüência evidentemente falsa então rejeita-se a hipótese. Mas quando se recai em conseqüências que não se sabe se são falsas ou verdadeiras costuma-se dizer: "Eis o que se poderia demonstrar se nossa primeira hipótese fosse verdade". Estas são as matemáticas conjecturais e se faz muito disso na pesquisa!

No que concerne à conjectura de SIERPINSKI existem indícios que mostram que a questão é difícil - muito difícil. De fato, se temos um polinômio, nós podemos talvez, fazendo muitos cálculos, chegar a encontrar um valor que seja primo. E se tomamos um outro polinômio nós podemos, pelo *mesmo tipo de cálculo*, encontrar ainda um valor primo, mas isto é bem menos provável. Em todo caso, é praticamente impossível encontrar um método de cálculo *uniforme* que permita encontrar os valores primos para todos os polinômios. De qualquer modo, quando fazemos cálculos, de maneira empírica, com um polinômio e depois com um outro, só podemos realizar esses cálculos para um número finito de polinômios e, portanto, não teremos uma demonstração para todos os polinômios.

Esses cálculos são difíceis porque mesmo com um polinômio "pequeno" pode ocorrer que este produza valores primos muito lentamente. Vejamos um exemplo devido à SHENG JINGRUN:

$f(X) = X^6 + 1061$

$f(x)$ é composto para todo número natural inferior à 3906 e $f(3906)$ é primo!

De fato, estuda-se muito esse gênero de polinômios que fornecem poucos números primos, o que mostra que a conjectura de SIERPINSKI é difícil.

Pode-se igualmente prever a dificuldade pelas conseqüências que esta conjectura implica. Vou dar-lhes duas:

A primeira é que existe uma infinidade de números primos gêmeos tais como 3 e 5, 5 e 7, 17 e 19, etc. Até o momento não existe demonstração deste fato.

A segunda é que o polinômio $X^2 + 1$ assume uma infinidade de valores primos (como por exemplo $4^2 + 1 = 17$) e isto não se sabe demonstrar.

Vemos portanto que toda uma série de resultados sobre os números primos decorre desta conjectura e é por isto que ela é muito estudada atualmente.

Antes de concluir, retornemos a exigência c) referente à geração de números primos. Há um resultado extremamente surpreendente que diz a coisa seguinte: existe um polinômio (que pode ser escrito explicitamente) de grau 25 à 26 variáveis tal que, quando se substitui as variáveis por inteiros positivos, obtém-se inteiros que quando são positivos são também primos e obtém-se assim todos os números primos. Dito de outra forma:

O conjunto dos números primos é o conjunto dos valores positivos de um

polinômio de grau 25 e de 26 variáveis.

Este resultado surpreendente é devido à MATIJASEVIC que resolveu assim, pela negativa, o décimo problema de HILBERT. Este décimo problema é o seguinte: fabriquemos uma máquina - uma máquina teórica - tal que colocando-se nessa máquina uma equação dita diofantina e fazendo-a funcionar, ela indique se a equação possue ou não soluções inteiras. Era um sonho de HILBERT encontrar uma tal máquina capaz de dizer se uma equação diofantina possue ou não soluções. Pois bem, em 1970 MATIJASEVIC mostrou que uma tal máquina não pode existir ou, dito de outra forma, que qualquer que seja o algoritmo inventado para mostrar a existência de soluções para equações diofantinas, existe sempre pelo menos uma equação que lhe "escapa". É um resultado negativo, mas podemos vê-lo sob um aspecto positivo: para nós, ele mostra que sempre existirá problemas à resolver dentro da teoria de números.

Segue abaixo uma mini-bibliografia para os curiosos que quizerem ir um pouco mais além.

Ribenboim P., *The book of Prime Numbers Records,* Springer Verlag, New York,1988.

Ribenboim P., *Algebraic Numbers,* Willey - Interscience, New York, 1972.

Borevich Z. I., Chafarevitch I. R., *Théorie de Nombres,* Gauthier- Villars, Paris, 1966.

Ellison W. J., (en collaboration avec Mendes-France M.) *Les nombres premiers,* Hermann, Paris, 1975.

Department of Mathematics
Queen's University
Kingston, Ontario K7L 3N6,
Canada