Polinômios Geradores de Primos

Geração de sequências finitas de primos por polinômios em $\mathbb{Z}[x]$

Antonio Fornari

14/09/2018

IMECC - UNICAMP

Sumário

Introdução

Definições I

Definição 1.1.

$I_n := \{1, 2, \ldots, n\}$.

Definição 1.2.

$\mathbb{N} := \{1, 2, 3, \ldots\}$.

Definição 1.3.

$\mathbb{N}_0 := \mathbb{N} \cup \{0\}$.

Definição 1.4.

$\mathbb{P} := \{p \in \mathbb{N} : \sum_{d|p} 1 = 2\}$, *conjunto dos número primos.*

Definição 1.5.

A função $\pi(n) : \mathbb{N} \to \mathbb{N}_0$ *retorna o número de primos em* I_n.

Definição 1.6.

Denotamos por $\lfloor x \rfloor$ *o maior inteiro menor que* x.

Existem funções que definem os números primos?

Classificação

É natural que se busquem funções $f(n) : \mathbb{N} \to \mathbb{N}$ que produzam primos. Por praticidade, costuma-se agrupar estas funções em três categorias:

(A) $f(n) = p_n$

(B) $Im(f(x)) \subset \mathbb{P}, n \neq m \iff f(n) \neq f(m)$

(C) $\mathbb{P} = \{f(n) : f(n) > 0\}$

Funções do Tipo A

Fórmula de Willans e fórmula de Mináč:

$$P_n = 1 + \sum_{i=1}^{2^n} \left\lfloor \sqrt[n]{\frac{n}{1+\pi(i)}} \right\rfloor$$

$$\pi(m) = \sum_{i=2}^{m} \left\lfloor \frac{(i-1)!+1}{i} - \left\lfloor \frac{(i-1)!}{i} \right\rfloor \right\rfloor$$

Funções do Tipo B

Função de Mills:

$$M_n = \left\lfloor \theta^{3^n} \right\rfloor$$

Funções do Tipo B

Função de Mills:

$$M_n = \left\lfloor \theta^{3^n} \right\rfloor$$

- $\theta \approx 1.3064$

Funções do Tipo B

Função de Mills:

$$M_n = \left\lfloor \theta^{3^n} \right\rfloor$$

- $\theta \approx 1.3064$
- $\forall\ c > 2.106$ existe um conjunto não enumerável de reais $\theta > 0$ tais que $\left\lfloor \theta^{c^n} \right\rfloor$ é sempre primo.

Funções do Tipo B

Função de Mills:

$$M_n = \left\lfloor \theta^{3^n} \right\rfloor$$

- $\theta \approx 1.3064$
- $\forall\ c > 2.106$ existe um conjunto não enumerável de reais $\theta > 0$ tais que $\left\lfloor \theta^{c^n} \right\rfloor$ é sempre primo.
- Quando $c = 3$, o número θ acima é o menor possível, e é chamado Constante de Mills.

Funções do Tipo C

Tabela 1: Funções polinomiais do tipo C

Variáveis	Grau	Autor	Ano	Observações
24	37	Matijasevič	1971	Não explícito
21	21	Matijasevič	1971	
26	25	J., S., W., W.	1976	Primeiro explícito
42	5	J., S., W., W.	1976	Menor grau
10	$\approx 1.6 \times 10^{45}$	Matijasevič	1977	Menos variáveis

Fim da Introdução

Focaremos em funções do tipo B, que produzirão primos distintos para subconjuntos de $\mathbb{N}$.

Motivação

O polinômio de Euler

Euler percebeu, em 1772, que o polinômio $p(n) = n^2 - n + 41$ produz uma sequência de números primos distintos para $n \in I_{40}$

Tabela 2: Primalidade dos Valores de $P(n)$

n	p(n)	Primo
1	41	Sim
2	43	Sim
3	47	Sim
4	53	Sim
5	61	Sim
⋮	⋮	⋮
39	1523	Sim
40	1601	Sim
41	1681	Não
42	1763	Não
43	1847	Sim
⋮	⋮	⋮

A Pergunta

Sabe-se que o polinômio de Euler não produz números primos indefinidamente, mas seria possível que ele continuasse a os produzir em grandes quantidades?

Algoritmo

```
#include <stdio.h>
#include <math.h>

#define MAX 1000000
#define q 41

int main(){
   int prime=1,counter;
   long long int y,n,i;

   for(n=1, counter=0;n<=MAX;prime=1,n++){
        y = (n*n - n + q);

        for(i=q;prime==1&&i<=sqrt(y);i+=2){
                if(y%i==0)prime=0;
                }
        if(prime==1)counter++;
        }

        printf("%d primes were found",counter);
    return 0;
    }
```

Proporção Imagem/Domínio I

Tabela 3: Primos em n e $P(n)$

n	$\pi(n)$	Nº de Primos na Imagem
40	12	40
10^2	25	86
10^3	168	581
10^4	1229	4149
10^5	9592	31985
10^6	78498	261081

Proporção Imagem/Domínio II

Tabela 4: Proporção Imagem/Domínio

n	Proporção de Primos Imagem/Domínio
40	3.333
10^2	3.480
10^3	3.464
10^4	3.377
10^5	3.335
10^6	3.326

Espiral de Ulam

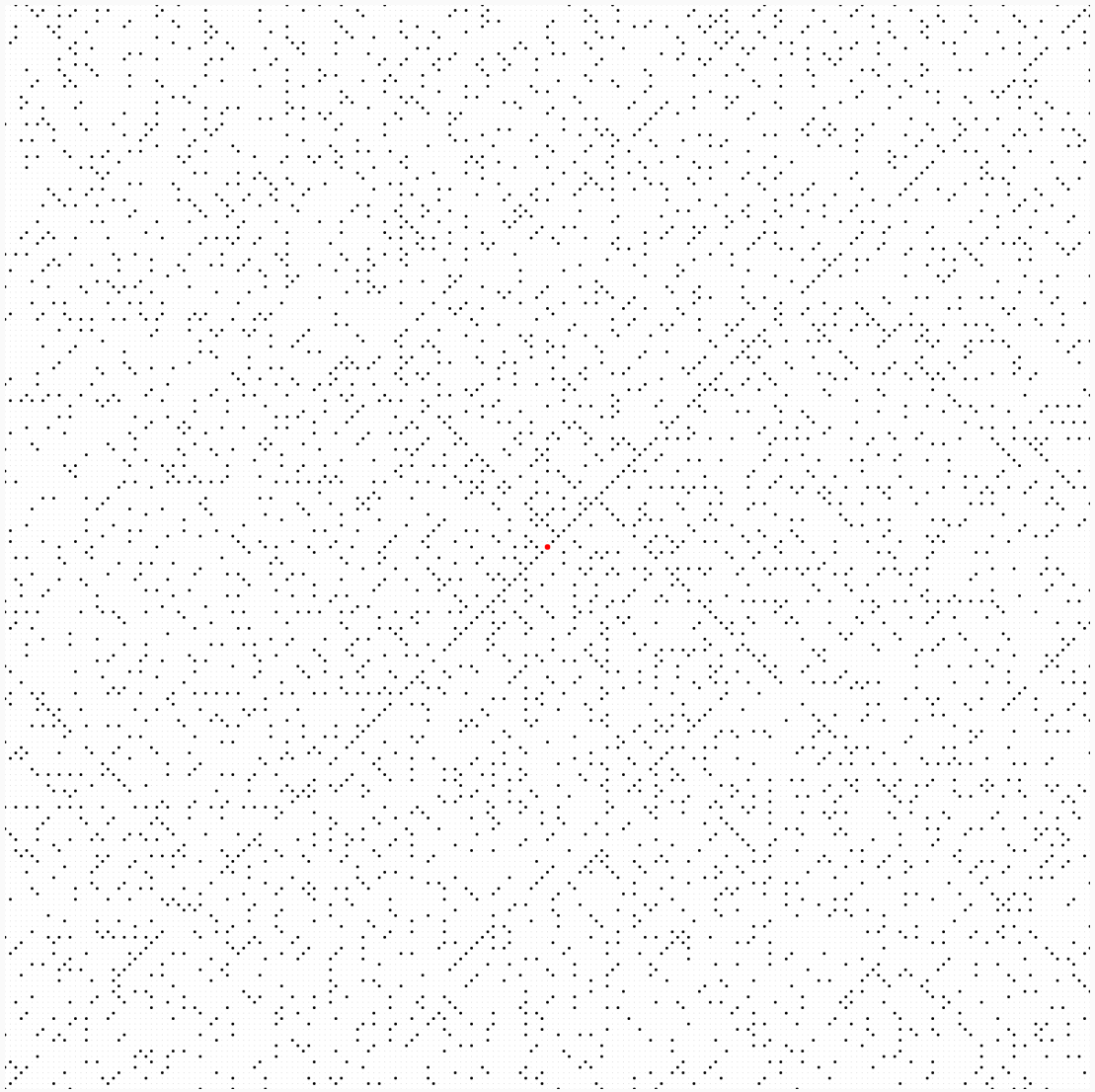

Figura 1: Espiral de Ulam Centrada em 41, 200x200

Fim da Motivação

Vimos que o polinômio de Euler produz primos de maneira bem eficiente para números até a ordem de 10^6, mas sabemos nada sobre as causas deste evento. Há também nenhuma garantia de que este é um comportamento que persistirá para valores grandes de n.

Polinômios Inteiros

Mau Exemplo

$$p(x) = 443 - \frac{126622x}{105} + \frac{663029x^2}{504} - \frac{23194097x^3}{30240} + \frac{77005x^4}{288} - \frac{336347x^5}{5760} + \frac{145x^6}{18} - \frac{4579x^7}{6720} + \frac{65x^8}{2016} - \frac{79x^9}{120960}$$

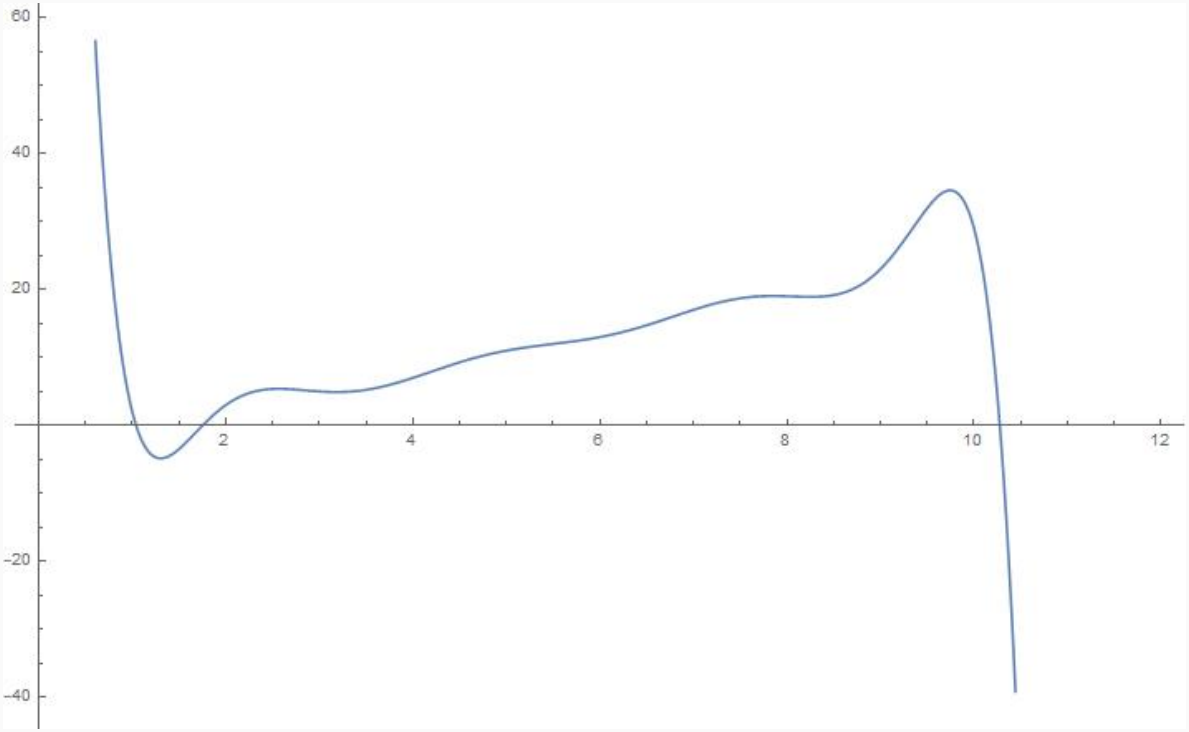

Figura 2: Um polinômio interpolador

Bons Exemplos

Polinômio	Primos de 0 a n	Primos distintos	OEIS	Referência
$\frac{1}{4}(n^5 - 133n^4 + 6729n^3 - 158379n^2 + 1720294n - 6823316)$	56	57		Dress and Landreau (2002), Gupta (2006)
$\frac{1}{36}(n^6 - 126n^5 + 6217n^4 - 153066n^3 + 1987786n^2 - 13055316n + 34747236)$	54	55		Wroblewski and Meyrignac (2006)
$n^4 - 97n^3 + 3294n^2 - 45458n + 213589$	49	49		Beyleveld (2006)
$n^5 - 99n^4 + 3588n^3 - 56822n^2 + 348272n - 286397$	46	47		Wroblewski and Meyrignac (2006)
$-66n^3 + 3845n^2 - 60897n + 251831$	45	46		Kazmenko and Trofimov (2006)
$36n^2 - 810n + 2753$	44	45	A050268	Fung and Ruby
$3n^3 - 183n^2 + 3318n - 18757$	46	43		S. M. Ruiz (pers. comm., Nov. 20, 2005)
$47n^2 - 1701n + 10181$	42	43	A050267	Fung and Ruby
$103n^2 - 4707n + 50383$	42	43		Speiser (pers. comm., Jun. 14, 2005)
$n^2 - n + 41$	40	40	A005846	Euler
$42n^3 + 270n^2 - 26436n + 250703$	39	40		Wroblewski and Meyrignac
$43n^2 - 537n + 2971$	34	35		J. Brox (pers. comm., Mar. 27, 2006)
$8n^2 - 488n + 7243$	61	31		F. Gobbo (pers. comm., Dec. 27, 2005)
$6n^2 - 342n + 4903$	57	29		J. Brox (pers. comm., Mar. 27, 2006)
$2n^2 + 29$	28	29	A007641	Legendre (1798)
$7n^2 - 371n + 4871$	23	24		F. Gobbo (pers. comm., Dec. 26, 2005)
$n^4 + 29n^2 + 101$	19	20		E. Pegg, Jr. (pers. comm., Jun. 14, 2005)
$3n^2 + 39n + 37$	17	18		A. Bruno (pers. comm., Jun. 12, 2009)
$n^2 + n + 17$	15	16	A007635	Legendre
$4n^2 + 4n + 59$	13	14	A048988	Honaker
$2n^2 + 11$	10	11	A050265	
$n^3 + n^2 + 17$	10	11	A050266	

Figura 3: Tabela de bons geradores

Um Importante Teorema

Teorema 3.1.

Se $p(x) \in \mathbb{Z}[x]$ e $\{q, d, r\} \in \mathbb{Z}$, então $p(qd + r) \equiv_d p(r)$.

Demonstração.

□

Um Importante Teorema

Teorema 3.1.

Se $p(x) \in \mathbb{Z}[x]$ e $\{q, d, r\} \in \mathbb{Z}$, então $p(qd + r) \equiv_d p(r)$.

Demonstração.

$$\text{Como se sabe, } \begin{cases} p(x) := \sum_{i=0}^{n} a_i x^i, \ a_i \in \mathbb{Z} \\ (a+b)^n = \sum_{i=0}^{n} \binom{n}{i} a^{n-i} b^i \end{cases}$$

□

Um Importante Teorema

Teorema 3.1.
Se $p(x) \in \mathbb{Z}[x]$ e $\{q, d, r\} \in \mathbb{Z}$, então $p(qd + r) \equiv_d p(r)$.

Demonstração.

$$\text{Como se sabe, } \begin{cases} p(x) := \sum_{i=0}^{n} a_i x^i, \ a_i \in \mathbb{Z} \\ (a+b)^n = \sum_{i=0}^{n} \binom{n}{i} a^{n-i} b^i \end{cases}$$

$$\implies p(qd + r) = \sum_{i=0}^{n} a_i (qd + r)^i = \sum_{i=0}^{n} a_i \sum_{k=0}^{i} \binom{i}{k} (qd)^{i-k} r^k.$$

□

Um Importante Teorema

Teorema 3.1.
Se $p(x) \in \mathbb{Z}[x]$ e $\{q, d, r\} \in \mathbb{Z}$, então $p(qd + r) \equiv_d p(r)$.

Demonstração.

$$\text{Como se sabe, } \begin{cases} p(x) := \sum_{i=0}^{n} a_i x^i, \ a_i \in \mathbb{Z} \\ (a+b)^n = \sum_{i=0}^{n} \binom{n}{i} a^{n-i} b^i \end{cases}$$

$$\implies p(qd + r) = \sum_{i=0}^{n} a_i (qd + r)^i = \sum_{i=0}^{n} a_i \sum_{k=0}^{i} \binom{i}{k} (qd)^{i-k} r^k.$$

$$\implies p(qd + r) \equiv_d \sum_{i=0}^{n} a_i r^i \equiv_d p(r).$$

□

Corolário

Corolário 3.1.

Dado $p(x) \in \mathbb{Z}[x]$, se existe sequência $(n_i)_{i=1}^{d}$ de números inteiros consecutivos para os quais $d \nmid p(n_i), 1 \leqslant i \leqslant d$, então $d \nmid p(n)\ \forall n \in \mathbb{Z}$.

Demonstração.

□

Corolário

Corolário 3.1.

Dado $p(x) \in \mathbb{Z}[x]$, se existe sequência $(n_i)_{i=1}^{d}$ de números inteiros consecutivos para os quais $d \nmid p(n_i), 1 \leqslant i \leqslant d$, então $d \nmid p(n)\ \forall n \in \mathbb{Z}$.

Demonstração.

Dada uma sequência $(n_i)_{i=1}^{d}$ de números inteiros consecutivos para a qual $p(n_i) \not\equiv_d 0, \forall\ 1 \leqslant i \leqslant d$, vê-se com o teorema anterior que a sequência $(p(n_i) \mod d)_{i=1}^{d}$ possui os mesmos elementos que $(p(i) \mod d)_{i=0}^{d-1}$, e que nenhum destes é 0.

□

Corolário

Corolário 3.1.

Dado $p(x) \in \mathbb{Z}[x]$, se existe sequência $(n_i)_{i=1}^{d}$ de números inteiros consecutivos para os quais $d \nmid p(n_i), 1 \leqslant i \leqslant d$, então $d \nmid p(n)\ \forall n \in \mathbb{Z}$.

Demonstração.

Dada uma sequência $(n_i)_{i=1}^{d}$ de números inteiros consecutivos para a qual $p(n_i) \not\equiv_d 0, \forall\ 1 \leqslant i \leqslant d$, vê-se com o teorema anterior que a sequência $(p(n_i) \mod d)_{i=1}^{d}$ possui os mesmos elementos que $(p(i) \mod d)_{i=0}^{d-1}$, e que nenhum destes é 0.

Dado um inteiro k qualquer, aplicando-se o algoritmo de Euclides é possível escrevê-lo como $k = dq + r$, $0 \leqslant r < d$, o que implica em $p(k) \equiv_d p(r)$. Como $0 \leqslant r < d$, $p(r)$ é elemento da sequência $(p(i))_{i=0}^{d-1}$, portanto $p(k) \equiv_d p(r) \not\equiv_d 0\ \forall k \in \mathbb{Z}$.

□

Restrição

O teorema anterior nos permite provar uma afirmação de extrema importância para este estudo: não há polinômio $p \in \mathbb{Z}[x], p : \mathbb{Z} \to \mathbb{Z}$ não constante tal que sua imagem não contenha infinitos números compostos.

Infinidade de Compostos

Teorema 3.2.

Todo polinômio não constante $p \in \mathbb{Z}[x], p : \mathbb{Z} \to \mathbb{Z}$, produz números compostos.

Demonstração.

□

Infinidade de Compostos

Teorema 3.2.

Todo polinômio não constante $p \in \mathbb{Z}[x], p : \mathbb{Z} \to \mathbb{Z}$, produz números compostos.

Demonstração.

Todo polinômio não constante $p(x)$ assume um mesmo valor y apenas um número finito de vezes, caso contrário $g(x) := (p(x) - y)$ seria polinômio não nulo com infinitas raízes.

□

Infinidade de Compostos

Teorema 3.2.

Todo polinômio não constante $p \in \mathbb{Z}[x], p : \mathbb{Z} \to \mathbb{Z}$, produz números compostos.

Demonstração.

Todo polinômio não constante $p(x)$ assume um mesmo valor y apenas um número finito de vezes, caso contrário $g(x) := (p(x) - y)$ seria polinômio não nulo com infinitas raízes.

Dado $p(a) = \mathcal{P}_1$, se $\mathcal{P}_1$ é composto a demonstração acaba.

□

Infinidade de Compostos

Teorema 3.2.

Todo polinômio não constante $p \in \mathbb{Z}[x], p : \mathbb{Z} \to \mathbb{Z}$, produz números compostos.

Demonstração.

Todo polinômio não constante $p(x)$ assume um mesmo valor y apenas um número finito de vezes, caso contrário $g(x) := (p(x) - y)$ seria polinômio não nulo com infinitas raízes.

Dado $p(a) = \mathcal{P}_1$, se $\mathcal{P}_1$ é composto a demonstração acaba.

Se $p(a) = \mathcal{P}_1$ é primo, olhamos a família $S := \{\mathcal{P}_i : \mathcal{P}_i := p(\mathcal{P}i + a)\}$ de elementos da imagem de p(x), que contém apenas múltiplos de $\mathcal{P}_1$. Esta família contém um número infinito de compostos.

□

Irredutibilidade

Além disso, a irredutibilidade em $\mathbb{Z}[x]$ é essencial para que um polinômio $p(x)$ seja bom gerador de primos, pois caso contrário $p(x) = g(x)h(x)$ geraria no máximo $deg(p)$ primos.

Polinômios da forma n^2-n+q

Definições II

Definição 4.1.

A função $\pi^*_{p(x)}(n) : \mathbb{Z}[x] \times \mathbb{N} \to \mathbb{N}_0$ *retorna o número de primos no conjunto* $Im_n(|p(x)|) := \{|p(1)|, |p(2)|, \ldots, |p(n)|\}$.

Definição 4.2.

A função $P_1[n] : \mathbb{N}\backslash\{1\} \to \mathbb{P}$ *retorna o menor número primo divisor de* n.

Definição 4.3.

$P_1[|f(x)|] := \min\{P_1[|f(n)|] : n \in \mathbb{N}\}$.

Definição 4.4.

ℓ_p *denota o maior natural tal que* $\pi^*_{p(x)}(n) = n$. *Usaremos apenas* ℓ *quando não causar ambiguidades.*

Resolução

Buscamos polinômios p tais que $deg(p) \ll \ell_p$. Estudaremos os polinômios $p_q(n) = n^2 - n + q$ pois aparentam ser um bom ponto de partida.

Limitantes para ℓ

Dado um polinômio inteiro de forma $p_q(n) = n^2 - n + q$, tem-se que $p_q(q) = q^2$ não é primo, portanto $\ell \leqslant q - 1$.

Além disso, se q é composto $p(1) = q$ e $\ell = 0$.

Como $p_q(2) - p_q(1) = 2$, $\ell > 1 \iff (q, q+2)$ é par de primos gêmeos.

Números de Heegner

De fato, $\ell_{p_q} = q - 1 \iff q \in \{1, 2, 3, 5, 11, 17, 41\}$, como provado por Rabinowitsch. Essa afirmação provém do fato de que o módulo do discriminante de $p_q(n)$ é um **número de Heegner** nestes casos.

Tabela de Valores Brutos

Tabela 5: Número de primos em I_n e em $Im_1^n(|p_q(x)|)$

n	$\pi(n)$	$\pi^*_{p_2(x)}(n)$	$\pi^*_{p_3(x)}(n)$	$\pi^*_{p_5(x)}(n)$	$\pi^*_{p_{11}(x)}(n)$	$\pi^*_{p_{17}(x)}(n)$	$\pi^*_{p_{41}(x)}(n)$
10^2	25	1	14	30	48	60	86
10^3	168	1	93	165	288	365	581
10^4	1229	1	629	1208	2057	2627	4149
10^5	9592	1	4899	9086	15661	20127	31985
10^6	78498	1	40037	74058	128171	164220	261081

Tabela de Proporções

Tabela 6: Proporção $\pi^*_{p_q(x)}(n)/\pi(n)$ de primos arredondada nos milésimos

n	$q=2$	$q=3$	$q=5$	$q=11$	$q=17$	$q=41$
10^2	0.040	0.560	1.200	1.920	2.400	3.440
10^3	0.006	0.554	0.982	1.714	2.173	3.458
10^4	0.001	0.512	0.983	1.674	2.138	3.376
10^5	0.000	0.511	0.947	1.633	2.098	3.335
10^6	0.000	0.510	0.943	1.633	2.092	3.326

Corolário (novamente)

Corolário 4.1.

Dado $p(x) \in \mathbb{Z}[x]$, se existe sequência $(n_i)_{i=1}^{d}$ de números inteiros consecutivos para os quais $d \nmid p(n_i), 1 \leqslant i \leqslant d$, então $d \nmid p(n)\ \forall n \in \mathbb{Z}$.

Demonstração.

Dada uma sequência $(n_i)_{i=1}^{d}$ de números inteiros consecutivos para a qual $p(n_i) \not\equiv_d 0$, $\forall\ 1 \leqslant i \leqslant d$, vê-se com o teorema anterior que a sequência $(p(n_i) \mod d)_{i=1}^{d}$ possui os mesmos elementos que $(p(i) \mod d)_{i=0}^{d-1}$, e que nenhum destes é 0.

Dado um inteiro k qualquer, aplicando-se o algoritmo de Euclides é possível escrevê-lo como $k = dq + r$, $0 \leqslant r < d$, o que implica em $p(k) \equiv_d p(r)$. Como $0 \leqslant r < d$, $p(r)$ é elemento da sequência $(p(i))_{i=0}^{d-1}$, portanto $p(k) \equiv_d p(r) \not\equiv_d 0\ \forall k \in \mathbb{Z}$. □

Menor Divisor Primo de $p_q(n)$

Como nestes casos $\ell_{p_q} = q - 1$, $P_1[p_q(n)] = q$.

Primos em Progressão Aritmética

Teorema de Dirichlet

Teorema 5.1 (Teorema de Dirichlet).
Dados dois naturais a, b tais que $mdc(a, b) = 1$, $p(n) = an + b$ produz infinitos primos.

Teorema de Green-Tao

Teorema 5.2 (Teorema de Green-Tao).

Para todo $k \in \mathbb{N}$, existe uma progressão aritmética de tamanho k cujos elementos são primos.

Teorema de Green-Tao

Teorema 5.2 (Teorema de Green-Tao).
Para todo $k \in \mathbb{N}$, existe uma progressão aritmética de tamanho k cujos elementos são primos.

Recorde atual: $4314274659571419 1 + (23681770 \times 223092870)n$, *de* $n = 0$ *a* $n = 25$.

Teorema de Tao-Ziegler

Teorema 5.3 (Teorema de Tao-Ziegler).
Sejam $P_1, \ldots, P_k : \mathbb{Z} \to \mathbb{Z}$ polinômios de grau menor ou igual a d, cujos coeficientes líderes sejam todos distintos, para algum $d \geqslant 1$. Suponha que para todo primo p existam n, r tais que $n + P_1(r), \ldots, n + P_k(r)$ são todos não divisíveis por p. Então existem infinitos pares n, r de números naturais tais que $n + P_1(r), \ldots, n + P_k(r)$ são primos.

Perguntas?

Referências I

1. Ribenboim, P. *Números Primos – Velhos Mistérios e Novos Recordes*
   Coleção Matemática Universitária, IMPA
2. Mollin, R.A. *Prime-Producing Quadratics*
   Disponível em: https://www.jstor.org/stable/2975080
   Acesso em: 14 set. 2018
3. Weisstein, E. W. *Prime-Generating Polynomial*
   From MathWorld–A Wolfram Web Resource.
   Disponível em: http://mathworld.wolfram.com/Prime-GeneratingPolynomial.html
   Acesso em: 14 set. 2018

Referências II

4. Tao, T.; Green, B. *The primes contain arbitrarily long arithmetic progressions*
   Disponível em: https://arxiv.org/abs/math/0404188
   Acesso em: 14 set. 2018
5. Tao, T.; Ziegler, T. *Polynomial patterns in the primes*
   Disponível em: https://arxiv.org/abs/1603.07817
   Acesso em: 14 set. 2018