Polos Olímpicos de Treinamento

Curso de Teoria dos Números - Nível 3

Carlos Gustavo Moreira

Aula 19

Polinômios ciclotômicos e primos

0.1 Alguns resultados e conjecturas sobre primos

Veremos o enunciado de alguns resultados clássicos sobre números primos. Também veremos vários problemas em aberto famosos.

Teorema 1 (Dirichlet). *Dados naturais a, d com $\mathrm{mdc}(a,d) = 1$, existem infinitos primos da forma $a + dn$ (com n natural).*

A demonstração usual deste teorema usa variáveis complexas. Muitos casos particulares admitem demonstrações elementares mais ou menos simples. O leitor não deve ter dificuldade em demonstrar, por exemplo, que existem infinitos primos da forma $4n + 3$ ou $6n + 5$.

A seguir mostramos um caso particular do teorema de Dirichlet, no qual usaremos ferramentas elementares para sua prova. Usaremos o *polinômio ciclotômico* $\phi_m(x)$ definido, para cada inteiro $m \geq 1$, pela fórmula

$$\phi_m(x) = \prod_{0 \leq k < m, \mathrm{mdc}(k,m)=1} (x - e^{2k\pi i/m}).$$

definido indutivamente pela fórmula

$$\prod_{\ell | m} \phi_\ell(x) = x^m - 1.$$

Assim, $\phi_m(x)$ é o polinômio mônico de grau $\varphi(m)$ cujas raízes são $e^{2k\pi i/m}$, $0 \leq k < m$, $\mathrm{mdc}(k,m) = 1$. Verifica-se facilmente que os polinômios $\phi_m(x)$ satisfazem a fórmula

$$\prod_{\ell | m} \phi_\ell(x) = \prod_{0 \leq k < m} (x - e^{2k\pi i/m}) = x^m - 1.$$

Daí segue, por indução, que $\phi_m(x) \in \mathbb{Z}[x]$ para todo $m \geq 1$.

Temos por exemplo $\phi_1(x) = x-1$, $\phi_2(x) = x+1$, $\phi_3(x) = x^2+x+1$, $\phi_4(x) = x^2+1$ e, para todo primo p, $\phi_p(x) = (x^p-1)/(x-1) = x^{p-1}+x^{p-2}+\cdots+x+1$.

Lembramos a noção de *derivada* de um polinômio: se $p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = \sum_{j=0}^{n} a_j x^j$, definimos sua derivada $p'(x)$ como sendo o polinômio $p'(x) = na_n x^{n-1} + (n-1)a_{n-1}x^{n-2} + \cdots + a_1 = \sum_{j=1}^{n} j a_j x^{j-1}$. Se os coeficientes a_j de $p(x)$ estão em um anel A entãoo os coeficientes de $p'(x)$ também estão em A. Temos também a *regra do produto*: se $p(x) = \sum_{j=0}^{m} a_j x^j$ e $q(x) = \sum_{r=0}^{n} b_r x^r$ são polinômios, e $f(x) = p(x)q(x)$ então $f'(x) = p'(x)q(x) + p(x)q'(x)$. Para provar isso, note que, por linearidade, basta considerar o caso em que $p(x) = x^j$ (depois multiplicamos pelos a_j e somamos). E, nesse caso, novamente por linearidade, basta considerar o caso em que $q(x) = x^r$ (depois multiplicamos pelos b_r e somamos). Finalmente, se $p(x) = x^j$ e $q(x) = x^r$, temos $f(x) = p(x)q(x) = x^{j+r}$ e $p'(x)q(x) + p(x)q'(x) = jx^{j-1} \cdot x^r + x^j \cdot r x^{r-1} = (j+r)x^{j+r-1} = f'(x)$.

Teorema 2. *Para todo inteiro positivo d, existem infinitos primos na progressão aritmética $S = \{dn+1\}_{n\in\mathbb{N}}$.*

Demonstração. Suponhamos que em S existe apenas um número finito de primos $p_1, \ldots, p_l$ e definamos $a = dp_1 \cdots p_l$. Seja q um divisor primo de $\phi_d(a)$. Dado que $q \mid \phi_d(a) \mid a^d - 1$, temos que $a^d \equiv 1 \pmod{q}$. Mostremos que $d = \operatorname{ord}_q a$. De fato, se $e = \operatorname{ord}_q a$ é um divisor próprio de d, como o polinômio $(x^e - 1)\phi_d(x)$ divide $x^d - 1$, teremos $x - a \mid x^e - 1$ (pois $a^e \equiv 1 \pmod{q}$, e logo a é raiz de $x^e - 1$ em $x^d - 1 \in \mathbb{Z}/(q)[x]$). Também temos $x - a \mid \phi_d(x)$ em $x^d - 1 \in \mathbb{Z}/(q)[x]$. Assim, $a \bmod q$ será raiz dupla de $x^d - 1 \in \mathbb{Z}/(q)[x]$, ou seja, existe um polinômio $p(x) \in \mathbb{Z}/(q)[x]$ tal que $x^d - 1 = (x-a)^2 p(x) \in \mathbb{Z}/(q)[x]$. Derivamos, temos $dx^{d-1} = (x-a)^2 p'(x) + 2(x-a)p(x)$ em $\mathbb{Z}/(q)[x]$, donde, fazendo $x = a$, temos $da^{d-1} = 0$ em $\mathbb{Z}/(q)$, ou seja, $q \mid da^{d-1}$. Mas $q \mid a^d - 1$ e $d \mid a$ implica $q \nmid d$ e $q \nmid a$, absurdo.

Portanto $d = \operatorname{ord}_q a$ e assim $d \mid q - 1$, isto é, $q = nd + 1 \in S$, mas $q \neq p_j$ pois $q \mid a^d - 1 \implies q \nmid a$, logo $q \notin S$, o que é uma contradição. □

Aproveitamos para provar um importante fato algébrico sobre polinômios ciclotômicos:

Teorema 3. *Para todo $m \geq 1$ o polinômio $\phi_m(x)$ é irredutível.*

Demonstração. Suponhamos por absurdo que $\phi_m(x) = f(x)g(x)$ com $f(x)$ e $g(x)$ polinômios mônicos não-constantes com coeficientes inteiros e $f(x)$ irredutível. Se para toda raiz α de $f(x)$ e para todo primo q que não divide m temos que α^q também é raiz de $f(x)$, teríamos que $e^{2k\pi i/m}$, $0 \leq k < m$, $\operatorname{mdc}(k, m) = 1$ seriam todos raízes de $f(x)$, e logo $f(x) = \phi_m(x)$, absurdo. Sejam então α raiz de $f(x)$ e q um primo que não divide m tal que α^q não é raiz de $f(x)$. Assim, α^q é raiz de $g(x)$, e logo α é raiz de $g(x^q)$ (e também de $f(x)$), e, como $f(x)$ é irredutível, $f(x) | g(x^q)$.

Vamos agora considerar os polinômios não em $\mathbb{Z}[x]$, mas em $\mathbb{Z}/(q)[x]$. Em $\mathbb{Z}/(q)[x]$, temos $g(x^q) = g(x)^q$, e assim $f(x) | g(x)^q$ em $\mathbb{Z}/(q)[x]$. Seja $h(x)$ um fator irredutível de $f(x)$ em $\mathbb{Z}/(q)[x]$. Então $h(x) | g(x)^q$, donde $h(x) | g(x)$, e logo $h(x)^2 | f(x)g(x) = \phi_m(x) | x^m - 1$, donde $x^m - 1 = h(x)^2 p(x)$ para algum polinômio $p(x) \in \mathbb{Z}/(q)[x]$. Derivando os dois lados da igualdade, temos $mx^{m-1} = 2h(x)h'(x)p(x) + h(x)^2 p'(x) = h(x)(2h'(x)p(x) + h(x)p'(x))$. Assim,

$h(x)|x^m-1$ e $h(x)|mx^{m-1}$, donde, como $\text{mdc}(m,q)=1$, $h(x)|x^{m-1}$ em $\mathbb{Z}/(q)[x]$, donde $h(x)|x^m$ e $h(x)|x^m-(x^m-1)=1$ em $\mathbb{Z}/(q)[x]$, absurdo. □

Existem vários refinamentos conhecidos do teorema de Dirichlet. Definimos $\pi_{d,a}(x)$ como sendo o número de primos da forma $a+dn$ no intervalo $[2,x]$. De la Vallée Poussin provou que

$$\lim_{x\to+\infty}\frac{\pi_{d,a}(x)}{\pi(x)}=\frac{1}{\varphi(d)},$$

isto é, todas as possíveis classes módulo d têm aproximadamente a mesma proporção de primos. Uma prova deste resultado, utilizando variáveis complexas, encontra-se no apêndice.

Por outro lado, Tchebychev observou que para valores pequenos de x, $\pi_{3,2}(x)-\pi_{3,1}(x)$ e $\pi_{4,3}(x)-\pi_{4,1}(x)$ são positivos. Um teorema de Littlewood, entretanto, demonstra que estas funções mudam de sinal infinitas vezes. Em 1957, Leech demonstrou que o menor valor de x para o qual $\pi_{4,3}(x)-\pi_{4,1}(x)=-1$ é 26861 e em 1978 Bays e Hudson demonstraram que o menor valor de x para o qual $\pi_{3,2}(x)-\pi_{3,1}(x)=-1$ é 608981813029.

Seja $p(d,a)$ o menor primo da forma $a+dn$, n inteiro e

$$p(d)=\max\{p(d,a)\mid 0<a<d,\text{mdc}(a,d)=1\}.$$

Linnik (1944) provou que existe $L>1$ com $p(d)<d^L$ para todo d suficientemente grande. A melhor estimativa conhecida para L é $L\leq 5,5$, devida a Heath-Brown (1992), que também conjecturou que

$$p(d)\leq Cd(\log d)^2.$$

Por outro lado, não se sabe demonstrar que existam infinitos primos da forma n^2+1; aliás, não existe nenhum polinômio P em uma variável e de grau maior que 1 para o qual se saiba demonstrar que existem infinitos primos da forma $P(n)$, $n\in\mathbb{Z}$. Mas, existem muitos polinômios em mais de uma variável que assumem infinitos valores primos: por exemplo, prova-se facilmente que todo primo da forma $4n+1$ pode ser escrito também na forma a^2+b^2, $a,b\in\mathbb{Z}$. Recentemente, Friedlander e Iwaniec provaram um resultado muito mais difícil: que existem infinitos primos da forma a^2+b^4.

Um dos problemas em aberto mais famosos da Matemática é a conjectura de Goldbach: todo número par maior ou igual a 4 é a soma de dois primos. Chen demonstrou que todo número par suficientemente grande é a soma de um primo com um número com no máximo dois fatores primos. Vinogradov demonstrou que todo ímpar suficientemente grande (por exemplo, maior do que $3^{3^{15}}$) é uma soma de três primos. Mais recentemente, H. Helfgott anunciou ([9]) uma demonstração de que todo ímpar maior do que 5 é soma de três primos.

Seja p_n o n-ésimo número primo. O teorema dos números primos equivale a dizer que

$$\lim_{n\to\infty}\frac{p_n}{n\log n}=1.$$

Por outro lado, sabe-se muito pouco sobre o comportamento da função $d_n = p_{n+1} - p_n$. Por exemplo, a conjectura de que existem infinitos primos gêmeos equivale a dizer que $\liminf d_n = 2$. Seja

$$L = \liminf \frac{d_n}{\log p_n};$$

Erdős provou que $L < 1$ e Maier que $L \leq 0,248$. Apenas em 2005, D. A. Goldston, J. Pintz e C. Y. Yıldırım provaram que $L = 0$ (ver [5]). De fato eles provaram bem mais (ver [6]): por exemplo, temos

$$\liminf \frac{d_n}{\sqrt{\log p_n}(\log\log p_n)^2} < \infty.$$

E, em 2013, Y. Zhang realizou um avanço muito importante, provando que $\liminf d_n < 70000000$ (ver [11]). Erdős também provou que o conjunto dos pontos de acumulação de $d_n/\log p_n$ tem medida positiva. Por outro lado, pelo postulado de Bertrand, sempre existe pelo menos um primo entre m e $2m$, ou seja, $d_n < p_n$. Em 1931, Westzynthius provou que

$$\limsup \frac{d_n}{\log p_n} = \infty,$$

e em 1963 Rankin, completando um trabalho de Erdős, mostrou que

$$\limsup \frac{d_n(\log\log\log p_n)^2}{\log p_n \cdot \log\log p_n \cdot \log\log\log\log p_n} \geq e^\gamma \approx 1,78107$$

onde γ é a já mencionada constante de Euler-Mascheroni. Este resultado foi melhorado por Pomerance e posteriormente por Pintz, que provou que o lado esquerdo é maior do que ou igual a $2e^\gamma$ (ver [10]). Conjetura-se que

$$\limsup \frac{d_n}{(\log p_n)^2} = C$$

para alguma constante positiva C. Observamos que a primeira vez que $d_n > 1000$ ocorre para $p_n = 1693182318746371$, quando $d_n = 1132$, o que foi descoberto recentemente por T. Nicely e D. Nyman.

Outra conjectura famosa é que sempre há pelo menos um primo entre n^2 e $(n+1)^2$. Por outro lado, sabe-se que existe um primo entre n^3 e $(n+1)^3$ para todo $n > e^{e^{15}}$ (ver [4]). Mais ainda, para x suficientemente grande, sempre existe um primo no intervalo $(x, x + x^w)$ onde $w = 0.525$ (ver [3]).

Ben Green e Terence Tao provaram em [7] que existem progressões aritméticas arbitrariamente grandes formadas exclusivamente por números primos (veja [1] para um texto expositório sobre este teorema e outros resultados relacionados). A maior progressão aritmética conhecida formada exclusivamente por números primos, que tem 26 termos, é

$$43142746595714191 + 5283234035979900 \cdot n =$$
$$43142746595714191 + 23681770 \cdot 23\# \cdot n,$$

para $n = 0, 1, \ldots, 25$, onde $n\#$ denota o produto dos primos menores do que ou iguais a n. Esta progressão aritmética foi descoberta em 12 de abril de 2010 por Benoãt Perichon usando um programa desenvolvido por Jaroslaw Wroblewski em Geoff Reynolds, em um projeto distribuído do *PrimeGrid*, que é um projeto cooperativo para procurar primos grandes de diversos tipos - veja `http://www.primegrid.com/` para mais informações.

Sierpinski provou que existem infinitos números naturais k tais que $k \cdot 2^n + 1$ é composto para todo natural n e Riesel provou o mesmo resultado para $k \cdot 2^n - 1$. Conjetura-se que os menores valores de k com as propriedades acima são respectivamente 78557 e 509203. Há um projeto cooperativo, que consiste em procurar primos grandes, para demonstrar estas conjecturas (veja observação a seguir).

Também existem infinitos naturais ímpares k que são simultaneamente números de Sierpinski e de Riesel, os chamados *números de Brier*. O menor número de Brier conhecido é 14366558304535079309865 7. Veja

`http://oeis.org/A076335`

e as páginas e referências lá mencionadas para mais informações.

O leitor interessado em aprender mais sobre problemas em aberto em teoria dos números pode consultar [8].

Observação 4. *Um sumário de vários projetos cooperativos para encontrar primos grandes pode ser visto em* `http://www.prothsearch.net/` *Projetos ativos que pretendem provar que* 78557 *e* 509203 *são os menores números de Sierpinski e Riesel podem ser encontrados respectivamente em*

`http://www.seventeenorbust.com/` *e* `http://www.rieselsieve.com/`.

O projeto Seventeen or Bust tem obtido resultados particularmente bons nos últimos anos. O fato de que 78557 *é um número de Sierpinski foi provado em* 1962 *por John Selfridge (veja o exercício* **??***). Quando o projeto começou, em* 2002*, havia* 17 *números menores que* 78557 *sobre os quais não se sabia se eram números de Sierpinski ou não:* 4847*,* 5359*,* 10223*,* 19249*,* 21181*,* 22699*,* 24737*,* 27653*,* 28433*,* 33661*,* 44131*,* 46157*,* 54767*,* 55459*,* 65567*,* 67607 *e* 69109*.*

Desde então, os participantes do projeto encontraram os seguintes primos

Primo	Descubridor	Data
$46157 \cdot 2^{698207} + 1$	S. Gibson	27/11/2002
$65567 \cdot 2^{1013803} + 1$	J. Burt	3/12/2002
$44131 \cdot 2^{995972} + 1$	equipe *deviced*	6/12/2002
$69109 \cdot 2^{1157446} + 1$	S. DiMichele	7/12/2002
$54767 \cdot 2^{1337287} + 1$	P. Coels	22/12/2002
$5359 \cdot 2^{5054502} + 1$	R. Sundquist	6/12/2003
$28433 \cdot 2^{7830457} + 1$	equipe *TeamPrimeRib*	30/11/2004
$27653 \cdot 2^{9167433} + 1$	D. Gordon	8/06/2005
$4847 \cdot 2^{3321063} + 1$	R. Hassler	15/10/2005
$19249 \cdot 2^{13018586} + 1$	K. Agafonov	5/05/2007
$33661 \cdot 2^{7031232} + 1$	S. Sunde	17/10/2007

Sobraram portanto os 6 *números* 10223, 21181, 22699, 24737, 55459 *e* 67607. *Veja* `http://www.seventeenorbust.com/` *para mais informações (em particular sobre como participar do projeto).*

1 Fórmulas para Primos

Não se conhece nenhuma fórmula simples para gerar primos arbitrariamente grandes. Uma palavra imprecisa mas importante nesta frase é "simples". Existem fórmulas que geram números primos, mas que são tão complicadas que não ajudam muito nem a gerar números primos explicitamente nem a responder perguntas teóricas sobre a distribuição dos primos. Um exemplo de fórmula para p_n, o n-ésimo primo, é

$$p_n = \left\lfloor 1 - \frac{1}{\log 2} \log \left(-\frac{1}{2} + \sum_{d|P_{n-1}} \frac{\mu(d)}{2^d - 1} \right) \right\rfloor,$$

onde $P_{n-1} = p_1 p_2 \cdots p_{n-1}$; deixamos a demonstração a cargo do leitor. Outra fórmula é

$$p_n = \lfloor 10^{2^n} c \rfloor - 10^{2^{n-1}} \lfloor 10^{2^{n-1}} c \rfloor,$$

onde

$$c = \sum_{n=1}^{\infty} \frac{p_n}{10^{2^n}} = 0.0203000500000007\ldots.$$

A inutilidade desta última fórmula vem do fato que para calcular c devemos encontrar todos os primos; a fórmula se tornaria mais interessante se existisse outra interpretação para o número real c, o que parece muito improvável.

Por outro lado, Mills provou que existem números reais $A > 1$ tal que $\lfloor A^{3^n} \rfloor$ é primo para todo $n \in \mathbb{N}$. Mais geral ainda,

Teorema 5. *Se $S = \{a_n\} \subset \mathbb{N}$ é uma sequência com a propriedade que: existem números reais x_0 e w com $0 < w < 1$, tais que para todo $x > x_0$ o intervalo aberto $(x, x + x^w)$ contém um elemento de S. Então para todo número real $c > \min\{1/(1-w), 2\}$, existe um número A tal que $\lfloor A^{c^n} \rfloor$ é uma subsequência de S.*

Demonstração. Definamos uma subsequência $\{b_n\}$ de S recursivamente por

1. b_1 o menor elemento de S tal que $b_1^c \geq x_0$.
2. b_{n+1} o menor elemento de S que satisfaz $b_n^c < b_{n+1} < b_n^c + b_n^{wc}$.

Como $c \geq \frac{1}{1-w}$ e $c \geq 2$, segue que

$$b_n^c < b_{n+1} < 1 + b_{n+1} < 1 + b_n^c + b_n^{wc} < 1 + b_n^c + b_n^{c-1} \leq (1 + b_n)^c.$$

tomando a $c^{-(n+1)}$-ésima potência na desigualdade anterior temos que

$$b_n^{c^{-n}} < b_{n+1}^{c^{-(n+1)}} < (1 + b_{n+1})^{c^{-(n+1)}} \leq (1 + b_n)^{c^{-n}},$$

o que mostra que a sequência $\{b_n^{c^{-n}}\}$ converge para um número real A. Segue que $b_n < A^{c^n} < 1 + b_n$ e portanto $b_n = \lfloor A^{c^n} \rfloor$. □

Corolário 6 (Mills). *Existe uma constante A tal que $\lfloor A^{3^n} \rfloor$ é primo para todo $n \in \mathbb{N}$.*

Demonstração. Pelo teorema anterior tomando S a sequência de primos, é conhecido (ver [3]) que entre $(x, x + x^w)$ sempre existe um primo com x suficientemente grande e $w = 0.525$. □

Um tipo de fórmula para primos, de certa forma mais intrigante, são polinômios de coeficientes inteiros em S variáveis com a seguinte propriedade quase mágica: a intersecção da imagem de $\mathbb{N}^S$ com $\mathbb{N}$ é exatamente o conjunto dos números primos. Note que se tomarmos um ponto de $\mathbb{N}^S$ "ao acaso", o valor do polinômio neste ponto quase certamente será negativo; assim, é difícil usar o polinômio para gerar primos. A título de curiosidade, vejamos um exemplo de polinômio com estas propriedades; aqui $S = 26$, o valor do polinômio é P, as variáveis chamam-se $a, b, \ldots, z$ e $A, B, \ldots, N$ são expressões auxiliares:

$$
\begin{aligned}
P &= (k+2)(1 - A^2 - B^2 - C^2 - \cdots - N^2),\\
A &= wz + h + j - q,\\
B &= (gk + 2g + k + 1)(h + j) + h - z,\\
C &= 16(k+1)^3(k+2)(n+1)^2 + 1 - f^2,\\
D &= 2n + p + q + z - e,\\
E &= e^3(e+2)(a+1)^2 + 1 - o^2,\\
F &= (a^2 - 1)y^2 + 1 - x^2,\\
G &= 16r^2y^4(a^2 - 1) + 1 - u^2,\\
H &= ((a + u^2(u^2 - a))^2 - 1)(n + 4dy)^2 + 1 - (x + cu)^2,\\
I &= (a^2 - 1)l^2 + 1 - m^2,\\
J &= ai + k + 1 - l - i,\\
K &= n + l + v - y,\\
L &= p + l(a - n - 1) + b(2an + 2a - n^2 - 2n - 2) - m,\\
M &= q + y(a - p - 1) + s(2ap + 2a - p^2 - 2p - 2) - x,\\
N &= z + pl(a - p) + t(2ap - p^2 - 1) - pm.
\end{aligned}
$$

Algumas observações simples: a única forma de P ser positivo é se $A = B = \cdots = N = 0$; neste caso seu valor será $k + 2$. Vemos assim que para produzir um número primo P com este polinômio devemos antes de mais nada tomar $k = P - 2$. As expressões auxiliares viram equações: como $A = 0$ temos $q = wz + h + j$. Assim, dado k para o qual $k + 2$ é primo, precisamos procurar valores para as outras letras que satisfaçam estas equações. Estes valores de certa forma *codificam* uma demonstração de que $P = k + 2$ é primo.

Referências

[1] A. Arbieto, C. Matheus e C. G. Moreira, *Aspectos Ergódicos da Teoria dos Números*, XXVI Colóquio Brasileiro de Matemática, IMPA (2007).

[2] F. E. Brochero Martinez, C. G. Moreira, N. C. Saldanha, E. Tengan - Teoria dos Números - um passeio com primos e outros números familiares pelo mundo inteiro, Projeto Euclides, IMPA, 2010.

[3] R. C. Baker, G. Harman e J. Pintz, *The difference between consecutive primes, II*, Proc. London Math. Soc. 83 (2001), 532–562.

[4] Y. Cheng, *Explicit estimate on primes between consecutive cubes*, Rocky Mountain J. Math 40, no. 1, 1–47 (2010). Também em `http://arxiv.org/abs/0810.2113v1`.

[5] D. A. Goldston, J. Pintz e C. Y. Yıldırım, *Primes in tuples I*, Ann. of Math. 170, 819–862 (2009). Também em `arxiv:math/0508185`.

[6] D. A. Goldston, J. Pintz e C. Y. Yıldırım, *Primes in tuples II*, Acta Math. 204, no. 1, 1–47 (2010). Também em `arxiv:0710.2728`.

[7] B. Green e T. Tao, *The primes contain arbitrarily long arithmetic progressions*, Annals of Math. 167, no. 2 (2008), 481–548.

[8] R. K. Guy, *Unsolved Problems in Number Theory*, Springer-Verlag (1994).

[9] H. Helfgott, *Major arcs for Goldbach's problem*, preprint em `http://arxiv.org/pdf/1305.2897.pdf`.

[10] J. Pintz, *Very large gaps between consecutive primes*, J. Number Theory 63 (1997), no. 2, 286–301.

[11] Y. Zhang, *Bounded gaps between primes*, aceito para publicação no Ann. of Math.. Mais informações disponíveis em `http://annals.math.princeton.edu/articles/7954`.