GAZETA DE MATEMÁTICA
N.º 50 — Dezembro de 1951

Sobre fórmulas assintóticas conjecturais referentes à distribuição dos números primos (*)

por **Manuel dos Reis**
Universidade de Coimbra

1.

No 3.º artigo da série *Some problems of «partitio numerorum»*, sub-intitulado *On the expression of a number as a sum of primes* [1], HARDY e LITTLEWOOD tentaram aplicar a este problema, e a alguns outros referentes à distribuição dos números primos, o método analítico que, com tão bons resultados, tinham utilizado no problema de WARING, da partição dum número em potências do mesmo grau. O êxito foi muito menor: numerosas e interessantes, as proposições obtidas eram todas conjecturais, pois de nenhuma o método permitia verdadeira demonstração. A proposição «fraca» de GOLDBACH, segundo a qual todo número ímpar (suficientemente grande) é soma de três primos, e a fórmula assintótica de que essa proposição imediatamente resulta, só puderam HARDY e LITTLEWOOD deduzí-las rigorosamente da célebre hipótese de RIEMANN sobre os zeros da função $\zeta(s)$ e da infinidade de hipóteses correspondentes sobre os zeros das funções $L(s)$ de DIRICHLET, isto é de uma infinidade de conjecturas. Para as outras proposições, por exemplo para a proposição «forte» de GOLDBACH segundo a qual todo número par (pelo menos suficientemente grande) é soma de dois primos, nem isso foi possível.

No 5.º artigo da referida série, publicado pouco depois com o sub-título *A further contribution to the study of Goldbach's problem* [2], HARDY e LITTLEWOOD puderam, da mencionada infinidade de hipóteses, deduzir rigorosamente que quase todos os números pares são somas de dois primos, mas não esclarecer se os números pares, que não são somas de dois primos, se porventura existem, são ou não em número infinito. Sendo impossível no estado actual da ciência, ao que parece, demonstrar aquelas hipóteses ou provar a sua falsidade, o método de HARDY e LITTLEWOOD, nos problemas referidos e em muitos outros relativos à distribuição dos números primos deve considerar-se principalmente, a nosso ver, *as a machine for the production of heuristic formulae* [3], para usar palavras dos próprios autores, e o objectivo da presente nota é mostrar, numa série de exemplos, que essa máquina pode ser substituida por outra muito mais simples: o «crivo de Eratósteneş» prosseguido até um ponto, sempre o mesmo, que proposições analíticamente demonstradas nos indicarão. Desses exemplos, uns são de HARDY e LITTLEWOOD, outro é caso particular de exemplo tratado por eles, outros finalmente são exemplos de que eles se não ocuparam. Na escolha guiámo-nos por um critério de simplicidade e de brevidade, deixando o tratamento geral do assunto para um trabalho posterior.

A citada proposição «fraca» de GOLDBACH foi, com a respectiva fórmula assintótica tal como a tinham obtido HARDY e LITTLEWOOD, demonstrada completamente por VINOGRADOV [4] em 1937, mediante novo método; e a utilização deste método permitiu a VAN DER CORPUT [5] demonstrar a proposição «forte» na sua forma atenuada, isto é para quase todos os números pares. Mas a proposição «forte» para todos os números pares suficientemente grandes, e todas as outras proposições conjecturais de HARDY e LITTLEWOOD, continuam indemonstradas. De resto o teorema de VINOGRADOV apoiará o nosso processo, que fundaremos no célebre «teorema dos números primos» de HADAMARD e de LA VALLÉE POUSSIN relativo à sucessão natural dos números e, mais geralmente, às progressões aritméticas [6].

---

* Recebido em 1951, Novembro, 15.

1) *Acta mathematica*, **44** (1923), págs. 1-70.

2) *Proceedings of the London Mathematical Society* (2), **22** (1924), págs. 46-56.

3) Loc. cit. in (1), pág. 69.

4) *Some theorems concerning the theory of primes*, *Recueil mathématique*, **44** (1937), págs. 179-195. Cf. J. G. VAN DER CORPUT, *Sur la démonstration de l'hypothèse de Goldbach pour les nombres impairs donnée par M. Vinogradow*, Paris 1938.

5) *Sur l'hypothèse de Goldbach pour presque tous les nombres pairs*, *Acta Arithmetica*, **2** (1937), págs. 266-290.

6) Cf. E. LANDAU, *Vorlesungen über Zahlentheorie*, II, págs. 9-28.

2.

Suprimindo, na sucessão dos n primeiros inteiros positivos, os primos não superiores a n^α, com $\frac{1}{2} \leqq \alpha < 1$, e seus múltiplos, restam a unidade e os primos desde n^α até n. E tem-se, como é sabido, designando por $\pi(x)$ e $[x]$, respectivamente, o número de primos que não excedem x e o maior inteiro contido em x,

$$(1)\quad \pi(n) - \pi(n^\alpha) + 1 = n - \left[\frac{n}{2}\right] - \left[\frac{n}{3}\right] - \cdots + \left[\frac{n}{2\cdot 3}\right] + \cdots - \left[\frac{n}{2\cdot 3\cdot 5}\right] - \cdots + \cdots,$$

onde os denominadores que figuram no 2.º membro são os primos não superiores a n^α e os seus produtos dois a dois, três a três, etc. até ao produto de todos esses primos. Ora sendo pelo teorema dos números primos, para $n \to \infty$,

$$\pi(n) \sim \frac{n}{\log n}, \qquad \pi(n^\alpha) \sim \frac{n^\alpha}{\alpha \log n},$$

tem-se evidentemente

$$\pi(n) - \pi(n^\alpha) + 1 \sim \frac{n}{\log n}$$

e portanto é

$$(2)\quad n - \left[\frac{n}{2}\right] - \left[\frac{n}{3}\right] - \cdots + \left[\frac{n}{2\cdot 3}\right] + \cdots - \left[\frac{n}{2\cdot 3\cdot 5}\right] - \cdots + \cdots \sim \frac{n}{\log n}.$$

Por outro lado

$$(3)\quad \begin{aligned} & n - \frac{n}{2} - \frac{n}{3} - \cdots + \frac{n}{2\cdot 3} + \cdots - \\ & - \frac{n}{2\cdot 3\cdot 5} - \cdots + \cdots = \\ & = n\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\left(1-\frac{1}{5}\right)\cdots = \\ & \cdots = n \prod_{p \leq n^\alpha} \left(1 - \frac{1}{p}\right), \end{aligned}$$

onde o produto se estende a todos os primos não superiores a n^α, é um valor aproximado do 2.º membro de (1) e, pelo conhecido teorema de MERTENS, o seu valor assintótico para $n \to \infty$ é

$$n \frac{e^{-\gamma}}{\log n^\alpha} = \frac{e^{-\gamma}}{\alpha} \cdot \frac{n}{\log n},$$

onde e e γ são respectivamente a base dos logaritmos naturais e a constante de EULER[7]; se tomarmos pois

$$(4)\qquad \alpha = e^{-\gamma} = 0{,}561\cdots$$

resulta

$$n - \frac{n}{2} - \frac{n}{3} - \cdots + \frac{n}{2\cdot 3} + \cdots - \frac{n}{2\cdot 3\cdot 5} - \cdots + \cdots \sim \frac{n}{\log n},$$

cujo confronto com (2) mostra que então o 2.º membro de (1) e o seu valor aproximado (3) são assintòticamente iguais. De ora avante α terá sempre a definição (4).

Se portanto o teorema dos números primos não estivesse demonstrado, a hipótese da igualdade assintótica do 2.º membro de (1) e do seu valor aproximado (3) conduziria a

$$\pi(n) - (\pi^\alpha) + 1 \sim n - \frac{n}{2} - \frac{n}{3} - \cdots + \frac{n}{2\cdot 3} + \cdots - \frac{n}{2\cdot 3\cdot 5} - \cdots + \cdots \sim \frac{n}{\log n},$$

donde, claramente,

$$\boxed{\pi(n) \sim \frac{n}{\log n}},$$

isto é, conduziria a uma fórmula assintótica conjectural exacta.

O valor aproximado (3) pode escrever-se directamente mediante conceitos simples de estatística matemática. Havendo em cada conjunto de p inteiros consecutivos um só múltiplo de p, e por isso atribuindo a um múltiplo de p a probabilidade $\frac{1}{p}$ e consequentemente a um não-múltiplo de p a probabilidade $1 - \frac{1}{p}$, será $\prod_{p \leq n^\alpha} \left(1 - \frac{1}{p}\right)$ a probabilidade de um não múltiplo de nenhum dos primos p não superiores a n^α e portanto $n \prod_{p \leq n^\alpha} \left(1 - \frac{1}{p}\right)$ e estimativa estatística do 1.º membro de (1). Esta observação é geral, e muito fácil de verificar na maior parte dos casos.

3.

Generalizando o que precede, consideremos a progressão aritmética de termo geral $ax + b$ $(x = 1, 2, \cdots, l)$, com a e b inteiros positivos primos entre si, e seja $al + b = n$. A congruência

---

[7] $\gamma = \lim_{n \to \infty} \left(1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n} - \log n\right)$.

$ax+b\equiv 0 \pmod p$ não tem raiz se o primo p divide a, isto é se $p\mid a$; e tem uma só raiz no caso contrário, isto é se $p\nmid a$, o que significa que os valores de x que tornam $ax+b$ divisível por p estão em progressão aritmética de razão p. Suprimindo pois na progressão dada os primos $p\nmid a$ não superiores a n^α, e seus múltiplos, restam só primos do intervalo (n^α, n), cujo número é $\pi_a(n)-\pi_a(n^\alpha)$, designando por $\pi_a(\xi)$ o número de primos da progressão dada que não excedem ξ; além disso é $l\prod_{n^\alpha\geq p\nmid a}\left(1-\frac{1}{p}\right)$ a estimativa estatística de $\pi_a(n)-\pi_a(n^\alpha)$, e a hipótese de que estas duas funções de n são assintòticamente iguais para $n\to\infty$ dá

$$\pi_a(n)-\pi_a(n^\alpha)\sim l\prod_{n^\alpha\geq p\nmid a}\left(1-\frac{1}{p}\right)=$$

$$=\frac{n-b}{a}\cdot\frac{\prod_{p\leq n^\alpha}\left(1-\frac{1}{p}\right)}{\prod_{n^\alpha\geq p\mid a}\left(1-\frac{1}{p}\right)};$$

para n suficientemente grande é

$$\prod_{n^\alpha\geq p\mid a}\left(1-\frac{1}{p}\right)=\prod_{p\mid a}\left(1-\frac{1}{p}\right)$$

e tem-se, portanto,

$$\pi_a(n)-\pi_a(n^\alpha)\sim\frac{n-b}{a}\cdot\frac{\prod_{p\leq n^\alpha}\left(1-\frac{1}{p}\right)}{\prod_{p\mid a}\left(1-\frac{1}{p}\right)}=$$

$$=\frac{n-b}{\varphi(a)}\prod_{p\leq n^\alpha}\left(1-\frac{1}{p}\right)\sim\frac{n}{\varphi(a)}\cdot\frac{\alpha}{\log n^\alpha},$$

donde

$$(5)\qquad \boxed{\pi_a(n)\sim\frac{1}{\varphi(a)}\cdot\frac{n}{\log n}};$$

$\varphi(a)$ designa a conhecida função de Euler, isto é o número de inteiros positivos não superiores a a e primos relativamente a a. Ora a relação (5) constitui o teorema dos números primos para a progressão aritmética $ax+b$, e obtivemos uma fórmula assintótica exacta.

4.

Consideremos agora a sucessão dos binários de números ímpares $x, x+k$, onde k é um número par positivo e $x=1,3,5,\cdots,2l-1$, e seja $2l-1+k=n$. As congruências $x\equiv 0 \pmod p$ e $x+k\equiv 0 \pmod p$, onde p é primo ímpar, têm a mesma raiz se $p\mid k$, e raízes diferentes se $p\nmid k$; portanto, em cada conjunto de p binários $x, x+k$ consecutivos, se $p\mid k$ há um só binário em que pelo menos um dos dois números (neste caso ambos) é divisível por p, mas há dois tais binários (com um só dos números divisível por p) se $p\nmid k$. Suprimindo pois na sucessão dada os binários $x, x+k$ em que pelo menos um dos dois números é divisível por algum dos primos não superiores a n^α, restam só binários de primos do intervalo (n^α, n) e possìvelmente o binário $1, 1+k$, em número de $P_k(n)-P_k(n^\alpha)+\varepsilon$, designando por $P_k(\xi)$ o número de binários de diferença k não superiores a ξ e sendo $\varepsilon=0$ ou $\varepsilon=1$; além disso é

$$l\prod_{\substack{3\leq p\leq n^\alpha\\ p\nmid k}}\left(1-\frac{2}{p}\right)\cdot\prod_{\substack{3\leq p\leq n^\alpha\\ p\mid k}}\left(1-\frac{1}{p}\right)$$

a estimativa estatística de $P_k(n)-P_k(n^\alpha)+\varepsilon$, e a hipótese de que estas duas funções são assintòticamente iguais para $n\to\infty$ dá

$$P_k(n)-P_k(n^\alpha)+\varepsilon\sim l\prod_{\substack{3\leq p\leq n^\alpha\\ p\nmid k}}\left(1-\frac{2}{p}\right)\cdot$$

$$\cdot\prod_{\substack{3\leq p\leq n^\alpha\\ p\mid k}}\left(1-\frac{1}{p}\right)=\frac{n-k+1}{2}\cdot$$

$$\cdot\prod_{3\leq p\leq n^\alpha}\left(1-\frac{2}{p}\right)\cdot\prod_{\substack{3\leq p\leq n^\alpha\\ p\mid k}}\frac{p-1}{p-2};$$

para n suficientemente grande é

$$\prod_{\substack{3\leq p\leq n^\alpha\\ p\mid k}}\frac{p-1}{p-2}=\prod_{3\leq p\mid k}\frac{p-1}{p-2};$$

além disso é

$$\prod_{3\leq p\leq n^\alpha}\left(1-\frac{2}{p}\right)=\prod_{3\leq p\leq n^\alpha}\left(1-\frac{1}{p}\right)^2\cdot$$

$$\cdot\prod_{3\leq p\leq n^\alpha}\left\{1-\frac{1}{(p-1)^2}\right\}=4\prod_{p\leq n^\alpha}\left(1-\frac{1}{p}\right)^2\cdot$$

$$\cdot \frac{\prod_{p \geq 3} \left\{1 - \frac{1}{(p-1)^2}\right\}}{\prod_{p > n^\alpha} \left\{1 - \frac{1}{(p-1)^2}\right\}} \sim$$

$$\sim 4 \left(\frac{\alpha}{\log n^\alpha}\right)^2 \cdot \prod_{p \geq 3} \left\{1 - \frac{1}{(p-1)^2}\right\};$$

tem-se portanto

$$P_k(n) - P_k(n^\alpha) + \varepsilon \sim \frac{n}{2} \cdot \frac{4}{\log^2 n} \cdot$$

$$\cdot \prod_{p \geq 3} \left\{1 - \frac{1}{(p-1)^2}\right\} \cdot \prod_{3 \leq p \mid k} \frac{p-1}{p-2},$$

donde

$$\boxed{P_k(n) \sim \frac{2n}{\log^2 n} \prod_{p \geq 3} \left\{1 - \frac{1}{(p-1)^2}\right\} \cdot \prod_{3 \leq p \mid k} \frac{p-1}{p-2},}$$

que é a fórmula assintótica conjectural obtida por Hardy e Littlewood. Em particular é

$$\boxed{P_2(n) \sim \frac{2n}{\log^2 n} \prod_{p \geq 3} \left\{1 - \frac{1}{(p-1)^2}\right\}}$$

a fórmula assintótica conjectural para o número de binários de primos «gémeos» ($k=2$) não superiores a n.

5.

Consideremos a sucessão dos binários de números ímpares $x, x+n$, onde n é um número par positivo e $x = 1-n, 3-n, 5-n, \cdots, (n-1)-n$, portanto $x + n = 1, 3, 5, \cdots, n-1$. As considerações do n.º 4 são quase literalmente aplicáveis a este caso e, designando por $Q(\xi)$ o número de binários de primos da sucessão dada cujos valores absolutos não excedem ξ, a estimativa estatística de $Q(n) - Q(n^\alpha) + \varepsilon$, onde se tem agora $\varepsilon = 0$ ou $\varepsilon = 2$, é

$$\frac{n}{2} \prod_{\substack{3 \leq p \leq n^\alpha \\ p \nmid n}} \left(1 - \frac{2}{p}\right) \cdot \prod_{\substack{3 \leq p \leq n^\alpha \\ p \mid n}} \left(1 - \frac{1}{p}\right),$$

o que dá, procedendo como no n.º 4,

$$\boxed{Q(n) \sim \frac{2n}{\log^2 n} \prod_{p \geq 3} \left\{1 - \frac{1}{(p-1)^2}\right\} \cdot \prod_{3 \leq p \mid n} \frac{p-1}{p-2},}$$

que é a fórmula assintótica conjectural para a proposição «forte» de Goldbach, obtida por Hardy e Littlewood. Com efeito os binários que estamos considerando são de números ímpares de diferença n, mas os diminuidores são negativos; equivalem pois a binários de números impares positivos de soma n.

A fórmula assintótica conjectural que precede, bem como as do n.º 4, foram também obtidas por Stäckel [8] independentemente de Hardy e Littlewood, e por método diferente. As fórmulas obtidas anteriormente por Sylvester e por Brun para $Q(n)$ e $P_2(n)$ estavam erradas por factores constantes [9].

6.

Consideremos a sucessão dos números x^2+k, em que k é inteiro diferente de zero e de quadrado negativo, e $x = 1, 2, 3, \cdots, l$. Seja $l^2+k=n$. A congruência $x^2 + k \equiv 0 \pmod{p}$, onde p é primo, tem uma só raíz se $p=2$ ou se $3 \leqslant p \mid k$; e tem duas raízes ou nenhuma se $3 \leqslant p \nmid k$, conforme $-k$ seja, ou não, resto quadrático de p. Isto conduz, anàlogamente aos n.ºs precedentes, a escrever, designando por $P(n)$ o número de primos da sucessão dada não superiores a n,

$$P(n) \sim l \left(1 - \frac{1}{2}\right) \cdot \prod_{\substack{3 \leq p \leq n^\alpha \\ p \mid k}} \left(1 - \frac{1}{p}\right) \cdot$$

$$\cdot \prod_{\varpi \leq n^\alpha} \left(1 - \frac{2}{\varpi}\right),$$

onde ϖ percorre os primos ímpares não divisores de k de que $-k$ é resto quadrático; ora o 2.º membro pode escrever-se

$$l \cdot \frac{\prod_{p \leq n^\alpha} \left(1 - \frac{1}{p}\right)}{\prod_{\substack{3 \leq p \leq n^\alpha \\ p \nmid k}} \left(1 - \frac{1}{p}\right)} \cdot \prod_{\varpi \leq n^\alpha} \left(1 - \frac{2}{\varpi}\right) =$$

$$= l \prod_{p \leq n^\alpha} \left(1 - \frac{1}{p}\right) \cdot \prod_{\varpi \leq n^\alpha} \frac{\varpi - 2}{\varpi - 1} \cdot \prod_{\varpi' \leq n^\alpha} \frac{\varpi'}{\varpi' - 1},$$

onde ϖ' percorre os primos ímpares não divisores de k, de que $-k$ é não-resto quadrático; será pois

---

8) Cf. P. Stæckel *und* W. Weinreich, *Die Darstellung gerader Zahlen als Differenzen und Summen von Primzahlen, Abh. d. Heidelb. Akad. d. Wiss.* 1922.

9) Cf. Hardy e Littlewood, loc. cit. in 1), pag. 32-37.

$$P(n) \sim l \prod_{p \leq n^\alpha} \left(1-\frac{1}{p}\right) \cdot \prod_{\varpi \leq n^\alpha} \left(1-\frac{1}{\varpi-1}\right) \cdot$$

$$\cdot \prod_{\varpi' \leq n^\alpha} \left(1+\frac{1}{\varpi'-1}\right) = l \prod_{p \leq n^\alpha} \left(1-\frac{1}{p}\right) \cdot$$

$$\cdot \prod_{\substack{3 \leq p \leq n^\alpha \\ p \nmid k}} \left\{1-\left(\frac{-k}{p}\right)\frac{1}{p-1}\right\},$$

onde $\left(\frac{-k}{p}\right)$ é o conhecido símbolo de LEGENDRE, igual a $+1$, ou -1, conforme $-k$ é, ou não, resto quadrático de p; tem-se portanto

$$P(n) \sim \sqrt{n-k} \cdot \prod_{p \leq n^\alpha} \left(1-\frac{1}{p}\right) \cdot$$

$$\cdot \frac{\prod_{3 \leq p \nmid k} \left\{1-\left(\frac{-k}{p}\right)\frac{1}{p-1}\right\}}{\prod_{n^\alpha < p \nmid k} \left\{1-\left(\frac{-k}{p}\right)\frac{1}{p-1}\right\}},$$

isto é

$$\boxed{P(n) \sim \frac{\sqrt{n}}{\log n} \cdot \prod_{3 \leq p \nmid k} \left\{1-\left(\frac{-k}{p}\right)\frac{1}{p-1}\right\}},$$

fórmula assintótica conjectural contida no trabalho de HARDY e LITTLEWOOD citado em 1). Em particular, tem-se conjecturalmente

$$\boxed{P(n) \sim \frac{\sqrt{n}}{\log n} \cdot \prod_{p \geq 3} \left\{1-\left(\frac{-1}{p}\right)\frac{1}{p-1}\right\}}$$

para o número de primos da forma x^2+1 não superiores a n.

7.

Consideremos também a sucessão dos números x^3+k em que k é inteiro não cubo, positivo ou negativo, e $x = 1, 2, \cdots, l$. Seja $l^3+k=n$. A congruência $x^3+k \equiv 0 \pmod p$, onde p é primo, tem uma só raiz se $p=2$, ou $p=3$, ou $p \equiv -1 \pmod 6$, ou $p \equiv 1 \pmod 6$ com $p \mid k$; tem três raizes ou nenhuma se $p \equiv 1 \pmod 6$ com $p \nmid k$, conforme k for, ou não, resto cúbico de p. Isto conduz, designando por $P(n)$ o número de primos da sucessão dada não superiores a n, a escrever

$$P(n) \sim l \left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right) \cdot \prod_{n^\alpha \geq p \equiv -1} \left(1-\frac{1}{p}\right) \cdot$$

$$\cdot \prod_{\substack{n^\alpha \geq p \equiv 1, \\ p \mid k}} \left(1-\frac{1}{p}\right) \cdot \prod_{\varpi \leq n^\alpha} \left(1-\frac{3}{\varpi}\right),$$

onde as congruências se referem ao módulo 6, e ϖ percorre os primos $\equiv 1 \pmod 6$ não divisores de k de que k é resto cúbico; ora o 2.º membro pode escrever-se

$$l \frac{\prod_{p \leq n^\alpha} \left(1-\frac{1}{p}\right)}{\prod_{\substack{n^\alpha \geq p \equiv 1 \\ p \nmid k}} \left(1-\frac{1}{p}\right)} \cdot \prod_{\varpi \leq n^\alpha} \left(1-\frac{3}{\varpi}\right) =$$

$$= l \prod_{p \leq n^\alpha} \left(1-\frac{1}{p}\right) \cdot \prod_{\varpi \leq n^\alpha} \frac{\varpi-3}{\varpi-1} \cdot \prod_{\varpi' \leq n^\alpha} \frac{\varpi'}{\varpi'-1},$$

onde ϖ' percorre os primos $\equiv 1 \pmod 6$ não divisores de k, de que k é não-resto cúbico; será pois

$$P(n) \sim l \prod_{p \leq n^\alpha} \left(1-\frac{1}{p}\right) \cdot \prod_{\varpi \leq n^\alpha} \left(1-\frac{2}{\varpi-1}\right) \cdot$$

$$\cdot \prod_{\varpi' \leq n^\alpha} \left(1+\frac{1}{\varpi'-1}\right) = l \prod_{p \leq n^\alpha} \left(1-\frac{1}{p}\right) \cdot$$

$$\cdot \prod_{\substack{n^\alpha \geq p \equiv 1 \\ p \nmid k}} \left\{1-(k)_p \frac{2}{p-1}\right\},$$

onde $(k)_p$ é 1, ou $-\frac{1}{2}$, conforme k é, ou não, resto cúbico de p; portanto

$$P(n) \sim \sqrt[3]{n-k} \cdot \prod_{p \leq n^\alpha} \left(1-\frac{1}{p}\right) \cdot \frac{\prod_{p \equiv 1, p \nmid k} \left\{1-(k)_p \frac{2}{p-1}\right\}}{\prod_{n^\alpha < p \equiv 1, p \nmid k} \left\{1-(k)_p \frac{2}{p-1}\right\}},$$

isto é

$$\boxed{P(n) \sim \frac{\sqrt[3]{n}}{\log n} \cdot \prod_{\substack{p \equiv 1 \pmod 6 \\ p \nmid k}} \left\{1-(k)_p \frac{2}{p-1}\right\}},$$

que é a fórmula assintótica conjectural obtida por HARDY e LITTLEWOOD para o número de primos x^3+k (k não cubo) não superiores a n.

8.

Consideremos ainda a sucessão dos números x^4+k, em que k é inteiro diferente de zero e de quadrado negativo, e $x=1,2,\cdots,l$. Seja $l^4+k=n$. Utilizemos, se p é primo e $3\leqslant p\nmid k$: o símbolo de LEGENDRE $\left(\frac{-k}{p}\right)$ já usado no n.º 6, igual a ± 1 conforme $-k$ é resto ou não-resto quadrático de p; e, se também $p\equiv 1 \pmod 4$ e $\left(\frac{-k}{p}\right)=1$, o símbolo $\left(\frac{-k}{p}\right)_4$, igual a ± 1 conforme $-k$ é resto não resto biquadrático de p. A congruência $x^4+k\equiv 0 \pmod p$, em que p é primo qualquer, tem uma só raíz se $p=2$ ou $3\leqslant p\mid k$; mas se $3\leqslant p\nmid k$, tem essa congruência: duas raízes se $p\equiv 3 \pmod 4$ com $\left(\frac{-k}{p}\right)=1$; quatro raízes se $p\equiv 1 \pmod 4$ com $\left(\frac{-k}{p}\right)_4=1$; e nenhuma raíz se $p\equiv 3 \pmod 4$ com $\left(\frac{-k}{p}\right)=-1$, ou $p\equiv 1 \pmod 4$ com $\left(\frac{-k}{p}\right)=-1$, ou $p\equiv 1 \pmod 4$ com $\left(\frac{-k}{p}\right)_4=-1$. Isto conduz, designando ainda por $P(n)$ o número de primos da sucessão dada não superiores a n, a escrever

$$P(n)\sim l\left(1-\frac{1}{2}\right)\cdot\prod_{\substack{3\leq p\leq n^\alpha\\ p\mid k}}\left(1-\frac{1}{p}\right)\cdot$$

$$\cdot\prod_{n^\alpha\geq\varpi\equiv 3}\left(1-\frac{2}{\varpi}\right)\cdot\prod_{\mathfrak{p}\leq n^\alpha}\left(1-\frac{4}{\mathfrak{p}}\right),$$

onde a congruência se refere ao módulo 4, ϖ percorre os primos ímpares não divisores de k de que $-k$ é resto quadrático, e $\mathfrak{p}$ percorre os primos $\equiv 1 \pmod 4$ não divisores de k de que $-k$ é resto biquadrático. Ora tem-se

$$\prod_{\mathfrak{p}\leq n^\alpha}\left(1-\frac{4}{\mathfrak{p}}\right)=\prod_{n^\alpha\geq\varpi\equiv 1}\left(1-\frac{2}{\varpi}\right)\cdot$$

$$\cdot\prod_{\mathfrak{p}'\leq n^\alpha}\frac{\mathfrak{p}'}{\mathfrak{p}'-2}\cdot\prod_{\mathfrak{p}\leq n^\alpha}\frac{\mathfrak{p}-4}{\mathfrak{p}-2},$$

onde a congruência se refere ao módulo 4, e $\mathfrak{p}'$ percorre os primos $\equiv 1 \pmod 4$ não divisores de k de que $-k$ é resto quadrático mas não biquadrático; portanto

$$\prod_{\mathfrak{p}\leq n^\alpha}\left(1-\frac{4}{\mathfrak{p}}\right)=\prod_{n^\alpha\geq\varpi\equiv 1}\left(1-\frac{2}{\varpi}\right)\cdot\prod_{\mathfrak{p}'\leq n^\alpha}\left(1+\frac{2}{\mathfrak{p}'-2}\right)\cdot$$

$$\cdot\prod_{\mathfrak{p}\leq n^\alpha}\left(1-\frac{2}{\mathfrak{p}-2}\right)=\prod_{n^\alpha\geq\varpi\equiv 1}\left(1-\frac{2}{\varpi}\right)\cdot$$

$$\cdot\prod_{n^\alpha\geq\varpi\equiv 1}\left\{1-\left(\frac{-k}{\varpi}\right)_4\frac{2}{\varpi-2}\right\}.$$

Por conseguinte é

$$P(n)\sim l\left(1-\frac{1}{2}\right)\prod_{\substack{3\leq p\leq n^\alpha\\ p\mid k}}\left(1-\frac{1}{p}\right)\cdot\prod_{\varpi\leq n^\alpha}\left(1-\frac{2}{\varpi}\right)\cdot$$

$$\cdot\prod_{n^\alpha\geq\varpi\equiv 1}\left\{1-\left(\frac{-k}{\varpi}\right)_4\frac{2}{\varpi-2}\right\},$$

o que, segundo cálculos efectuados no n.º 6, dá

$$P(n)\sim l\prod_{p\leq n^\alpha}\left(1-\frac{1}{p}\right)\cdot\prod_{\substack{3\leq p\leq n^\alpha\\ p\nmid k}}\left\{1-\left(\frac{-k}{p}\right)\frac{1}{p-1}\right\}\cdot$$

$$\cdot\prod_{n^\alpha\geq\varpi\equiv 1}\left\{1-\left(\frac{-k}{\varpi}\right)_4\frac{2}{\varpi-2}\right\}$$

e portanto, anàlogamente a n.ºs precedentes,

$$\boxed{P(n)\sim\frac{\sqrt[4]{n}}{\log n}\cdot\prod_{3\leq p\nmid k}\left\{1-\left(\frac{-k}{p}\right)\frac{1}{p-1}\right\}\cdot\prod_{\substack{p\equiv 1 \pmod 4\\ \left(\frac{-k}{p}\right)=1,\ p\nmid k}}\left\{1-\left(\frac{-k}{p}\right)_4\frac{2}{p-2}\right\}},$$

fórmula assintótica conjectural para o número de primos x^4+k ($-k$ não quadrado) não superiores a n. Em particular é

$$\boxed{P(n)\sim\frac{\sqrt[4]{n}}{\log n}\cdot\prod_{p\geq 3}\left\{1-\left(\frac{-1}{p}\right)\frac{1}{p-1}\right\}\cdot\prod_{p\equiv 1 \pmod 4}\left\{1-\left(\frac{-1}{p}\right)_4\frac{2}{p-2}\right\}}$$

a fórmula assintótica conjectural para o número de primos x^4+1 não superiores a n. Anàlogamente a estas fórmulas, que julgamos novas, muitas outras poderiam obter-se.

9.

O exemplo que segue pertence a um tipo de problemas que, ao que cremos, não tem sido considerado, salvo no caso linear de que demos o exemplo do n.º 4. Seja dada a equação $y=x^2+k$, e ocupemo-nos do número de soluções dela com $x=1,2,\cdots,l$ nas quais x e y sejam ambos primos (o exemplo do n.º 4 equivale a problema análogo para a equação $y=x+k$. Seja $n=l^2+k$. Como no n.º 6, k será inteiro diferente de zero e de quadrado negativo; e será par, para que x e y possam ser simultâneamente ímpares; além disso será $k\not\equiv -1 \pmod 3$, senão $x\equiv\pm 1 \pmod 3$ daria $y\equiv 0 \pmod 3$, isto é um dos dois números x, y seria necessáriamente divisível por 3. As congruências $x\equiv 0 \pmod p$ e $x^2+k\equiv 0 \pmod p$, onde p é primo, têm uma só e mesma raíz se $p=2$ ou $3\leqslant p|k$; se $3\leqslant p\nmid k$ têm ao todo três raizes diferentes quando $\left(\frac{-k}{p}\right)=1$, e uma só raíz (da primeira) quando $\left(\frac{-k}{p}\right)=-1$. Podemos pois escrever, designando por $R(n)$ o número de soluções em questão,

$$R(n)\sim l\left(1-\frac{1}{2}\right)\prod_{\substack{3\leq p\leq n^\alpha\\ p\mid k}}\left(1-\frac{1}{p}\right)\cdot$$

$$\cdot\prod_{\varpi'\leq n^\alpha}\left(1-\frac{1}{\varpi'}\right)\cdot\prod_{\varpi\leq n^\alpha}\left(1-\frac{3}{\varpi}\right),$$

onde, como no n.º 6, ϖ ou ϖ' percorrem respectivamente os primos ímpares não divisores de k de que $-k$ é, ou não, resto quadrático; portanto

$$R(n)\sim\frac{l}{2}\prod_{3\leq p\leq n^\alpha}\left(1-\frac{2}{p}\right)\cdot\prod_{\substack{3\leq p\leq n^\alpha\\ p\mid k}}\frac{p-1}{p-2}\cdot$$

$$\cdot\prod_{\varpi'\leq n^\alpha}\frac{\varpi'-1}{\varpi'-2}\cdot\prod_{\varpi\leq n^\alpha}\frac{\varpi-3}{\varpi-2}=\frac{l}{2}\prod_{3\leq p\leq n^\alpha}\left(1-\frac{1}{p}\right)^2\cdot$$

$$\cdot\prod_{3\leq p\leq n^\alpha}\left\{1-\frac{1}{(p-1)^2}\right\}\cdot\prod_{\substack{3\leq p\leq n^\alpha\\ p\mid k}}\frac{p-1}{p-2}\cdot$$

$$\cdot\prod_{\varpi'\leq n^\alpha}\left(1+\frac{1}{\varpi'-2}\right)\cdot\prod_{\varpi\leq n^\alpha}\left(1-\frac{1}{\varpi-2}\right)=$$

$$=2\,l\prod_{p\leq n^\alpha}\left(1-\frac{1}{p}\right)^2\cdot\prod_{3\leq p\leq n^\alpha}\left\{1-\frac{1}{(p-1)^2}\right\}\cdot$$

$$\cdot\prod_{\substack{3\leq p\leq n^\alpha\\ p\mid k}}\frac{p-1}{p-2}\cdot\prod_{\substack{3\leq p\leq n^\alpha\\ p\nmid k}}\left\{1-\left(\frac{-k}{p}\right)\frac{1}{p-2}\right\},$$

e tem-se por conseguinte a fórmula assintótica conjectural

$$\boxed{R(n)\sim\frac{2\sqrt{n}}{\log^2 n}\cdot\prod_{p\leq 3}\left\{1-\frac{1}{(p-1)^2}\right\}\cdot \cdot\prod_{3\leq p\nmid k}\left\{1-\left(\frac{-k}{p}\right)\frac{1}{p-2}\right\}\cdot\prod_{3\leq p\mid k}\frac{p-1}{p-2}}$$

para o número de soluções de $y=x^2+k$ (k inteiro diferente de zero e de quadrado negativo, par e $\not\equiv -1 \pmod 3$) não superiores a n, com x e y ambos primos.

10.

Consideremos finalmente as diversas representações dum número ímpar como soma de três números ímpares. Pode figurar-se cada uma destas representações por um ponto do plano, cujas coordenadas trilineares são as três parcelas respectivas. Sendo $n>0$ o número ímpar dado, e adoptando como triângulo fundamental um triângulo equilátero cujos vértices são os pontos, $(n,0,0)$, $(0,n,0)$, e $(0,0,n)$, então os pontos que figuram aquelas representações são os duma rede de triângulos equiláteros, constituída por rectas paralelas aos lados do triângulo fundamental cujas distâncias a estes lados são os números ímpares; e os pontos da rede interiores ao triângulo fundamental figuram as representações de n como soma de três números ímpares positivos. A estas últimas representações nos limitaremos aqui.

Suprimindo os pontos da rede situados nas rectas cujas distâncias aos lados do triângulo fundamental são os primos ímpares não superiores a n^α e seus múltiplos, restam os pontos figurativos das representações de n como soma de três parcelas, cada uma das quais é um primo de intervalo $(n^\alpha, n-2)$ ou a unidade. O número de pontos suprimidos utilizando um só primo ímpar $p\leq n^\alpha$ é, como se verifica sem dificuldade:

a) para $n=hp+2k$, h inteiro, $k=1,2\cdots,\frac{p-1}{2}$,

$$\sigma_a=3\left\{k+(k+p)+\cdots+\left(k+\frac{h-1}{2}p\right)\right\}-$$

$$-3\left(1+2+\cdots+\frac{h-1}{2}\right)=3(p-1)\frac{h^2-1}{8}+$$

$$+3k\frac{h+1}{2};$$

b) para $n=hp+2k$, h inteiro, $k=\frac{p+1}{2},\frac{p+3}{2},\cdots,p-1$,

$$\sigma_b=3\left\{k+(k+p)+\cdots+\left(k+\frac{h-1}{2}p\right)\right\}-$$

$$-3\left(1+2+\cdots+\frac{h+1}{2}\right)=3(p-1)\frac{h^2-1}{8}+$$

$$+3(k-1)\frac{h+1}{2};$$

c) para $n=hp$, k inteiro,

$$\sigma_c=3\left(p+2p+\cdots+\frac{h-1}{2}p\right)-$$

$$-2\left(1+2+\cdots+\frac{h-1}{2}\right)=(3p-2)\frac{h^2-1}{8}.$$

O número total de pontos da rede é o número triangular de ordem $\frac{n-1}{2}$, isto é $\frac{n^2-1}{8}$. Portanto o quociente da divisão do número de pontos não suprimidos, utilizando só o primo p, pelo número total é, em cada um dos três casos precedentes, para $n\to\infty$:

$$\nu_a=1-\frac{\sigma_a}{\frac{n^2-1}{8}}=1-\frac{3(p-1)(h^2-1)+12k(h+1)}{p^2h^2+4kph+4k^2-1}=$$

$$=1-\frac{3}{p}+\frac{3}{p^2}+O\left(\frac{1}{n}\right);$$

$$\nu_b=1-\frac{\sigma_b}{\frac{n^2-1}{8}}=1-\frac{3(p-1)(h^2-1)+12(k-1)(h+1)}{p^2h^2+4kph+4k^2-1}=$$

$$=1-\frac{3}{p}+\frac{3}{p^2}+O\left(\frac{1}{n}\right);$$

$$\nu_c=1-\frac{\sigma_c}{\frac{n^2-1}{8}}=1-\frac{(3p-2)(h^2-1)}{p^2h^2-1}=1-\frac{3}{p}+$$

$$+\frac{2}{p^2}+O\left(\frac{1}{n^2}\right).$$

Atribuindo pois a um ponto da rede, não suprimido utilizando um só primo ímpar p, a probabilidade ν_a ou ν_b, conforme o caso, se $p\nmid n$, ou a probabilidade ν_c se $p\mid n$, a estimativa estatística do número de pontos, não suprimidos utilizando todos os primos ímpares não superiores a n^α, é

$$\frac{n^2-1}{8}\cdot\prod_{\substack{3\le p\le n^\alpha\\ p\nmid k}}\left\{1-\frac{3}{p}+\frac{3}{p^2}+O\left(\frac{1}{n}\right)\right\}\cdot$$

$$\cdot\prod_{n^\alpha\ge p\mid n}\left\{1-\frac{3}{p}+\frac{2}{p^2}+O\left(\frac{1}{n^2}\right)\right\}\sim$$

$$\sim\frac{n^2}{8}\cdot\prod_{\substack{3\le p\le n^\alpha\\ p\nmid n}}\left(1-\frac{3}{p}+\frac{3}{p^2}\right)\cdot\prod_{n^\alpha\ge p\mid n}\left(1-\frac{3}{p}+\frac{2}{p^2}\right)=$$

$$=\frac{n^2}{8}\cdot\prod_{3\le p\le n^\alpha}\left(1-\frac{3}{p}+\frac{3}{p^2}\right)\cdot\prod_{n^\alpha\ge p\mid n}\frac{p^2-3p+2}{p^2-3p+3}$$

$$=\frac{n^2}{8}\cdot\prod_{3\le p\le n^\alpha}\left(1-\frac{1}{p}\right)^3\cdot\prod_{3\le p\le n^\alpha}\left\{1+\frac{1}{(p-1)^3}\right\}\cdot$$

$$\cdot\prod_{n^\alpha\ge p\mid n}\frac{p^2-3p+2}{p^2-3p+3}$$

$$=n^2\prod_{p\le n^\alpha}\left(1-\frac{1}{p}\right)^3\cdot\prod_{3\le p\le n^\alpha}\left\{1+\frac{1}{(p-1)^3}\right\}\cdot$$

$$\cdot\prod_{n^\alpha\ge p\mid n}\frac{p^2-3p+2}{p^2-3p+3};$$

assintòticamente igual a este resultado devemos considerar também, portanto, o número de representações de n como soma de três parcelas, cada uma das quais é um primo do intervalo $(n^\alpha,\ n-2)$ ou a unidade, e por conseguinte o número de representações de n como soma de três primos ímpares. Designando este último número por $R(n)$ tem-se pois

$$\boxed{R(n)\sim\frac{n^2}{\log^3 n}\cdot\prod_{p\ge 3}\left\{1+\frac{1}{(p-1)^3}\right\}\cdot\prod_{p\mid n}\frac{p^2-3p+2}{p^2-3p+3}},$$

que é a fórmula assintótica de Hardy e Littlewood que Vinogradov conseguiu demonstrar rigorosamente. O facto de, não só nos exemplos considerados nos n.os 2 e 3 mas também neste, se obter uma fórmula assintótica exacta confere alto grau de probabilidade, cremos nós, à exactidão das fórmulas assintóticas conjecturais obtidas nos n.os 4-9, e de muitas outras que pelo mesmo processo se podem obter, e portanto da hipótese que a este processo serve de base.[1]

---

[1] Vários n.os do presente artigo foram extraídos, com modificações, duma comunicação que apresentámos ao Congresso Luso-Espanhol para o Progresso das Ciências reunido em Lisboa em 1950, ainda não publicada.