Jak zgarnąć dwa miliony z milenijnego stołu

czyli co potrafi funkcja

M.Skałba

57 SMP, 26.01.2018

Zakodować ciąg

Theorem

Rozważmy ciąg $1, 1, 1, \ldots$; *ogólnie* $a_n = 1$ *dla każdego* n. *Wówczas*

$$\sum_{n=1}^{\infty} a_n x^n = 1 \cdot x^1 + 1 \cdot x^2 + \ldots 1 \cdot x^n + \ldots$$

Zakodować ciąg

Theorem

Rozważmy ciąg $1, 1, 1, \ldots$; *ogólnie* $a_n = 1$ *dla każdego* n. *Wówczas*

$$\sum_{n=1}^{\infty} a_n x^n = 1 \cdot x^1 + 1 \cdot x^2 + \ldots 1 \cdot x^n + \ldots$$

$$= \frac{x}{1-x} \; dla \; |x| < 1.$$

Wziąć funkcję

Teraz odwrotnie - zaczynamy od funkcji

$$\frac{1}{1-x-x^2} = \sum_{n=0}^{\infty} F_n x^n.$$

Co można powiedzieć o ciągu współczynników (F_n)?

Wziąć funkcję

Teraz odwrotnie - zaczynamy od funkcji

$$\frac{1}{1-x-x^2} = \sum_{n=0}^{\infty} F_n x^n.$$

Co można powiedzieć o ciągu współczynników (F_n)? Mamy

$$(1-x-x^2)\cdot(F_0+F_1x+F_2x^2+\cdots) = 1 =$$

Wziąć funkcję

Teraz odwrotnie - zaczynamy od funkcji

$$\frac{1}{1-x-x^2} = \sum_{n=0}^{\infty} F_n x^n.$$

Co można powiedzieć o ciągu współczynników (F_n)? Mamy

$$(1-x-x^2)\cdot(F_0 + F_1 x + F_2 x^2 + \cdots) = 1 =$$

$$= 1x^0 + 0\cdot x^1 + 0\cdot x^2 \cdots$$

Porównujemy współczynniki:

$$F_0 = 1,$$

Wziąć funkcję

Teraz odwrotnie - zaczynamy od funkcji

$$\frac{1}{1-x-x^2} = \sum_{n=0}^{\infty} F_n x^n.$$

Co można powiedzieć o ciągu współczynników (F_n)? Mamy

$$(1-x-x^2)\cdot(F_0+F_1x+F_2x^2+\cdots) = 1 =$$

$$= 1x^0 + 0\cdot x^1 + 0\cdot x^2 \cdots$$

Porównujemy współczynniki:

$$F_0 = 1,$$

$$F_0 = 1,\ F_1 - F_0 = 0,$$

Wziąć funkcję

Teraz odwrotnie - zaczynamy od funkcji

$$\frac{1}{1-x-x^2} = \sum_{n=0}^{\infty} F_n x^n.$$

Co można powiedzieć o ciągu współczynników (F_n)? Mamy

$$(1-x-x^2)\cdot(F_0+F_1x+F_2x^2+\cdots) = 1 =$$

$$= 1x^0 + 0\cdot x^1 + 0\cdot x^2 \cdots$$

Porównujemy współczynniki:

$$F_0 = 1,$$

$$F_0 = 1,\ F_1 - F_0 = 0,$$

$$F_0 = 1,\ F_1 - F_0 = 0, F_2 - F_1 - F_0 = 0 \text{ itd...}$$

funkcja ζ Riemanna

Określamy

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} \text{ dla } s > 1.$$

funkcja ζ Riemanna

Określamy

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} \text{ dla } s > 1.$$

Obliczyłem na komputerze

$$\zeta(2) \approx \sum_{n=1}^{10} \frac{1}{n^2} = \frac{1968329}{1270080} \approx 1,54977$$

funkcja ζ Riemanna

Określamy

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} \text{ dla } s > 1.$$

Obliczyłem na komputerze

$$\zeta(2) \approx \sum_{n=1}^{10} \frac{1}{n^2} = \frac{1968329}{1270080} \approx 1,54977$$

I co z tego?

funkcja ζ Riemanna

Określamy

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} \text{ dla } s > 1.$$

Obliczyłem na komputerze

$$\zeta(2) \approx \sum_{n=1}^{10} \frac{1}{n^2} = \frac{1968329}{1270080} \approx 1,54977$$

I co z tego? Euler udowodnił, że

$$\zeta(2) = \frac{\pi^2}{6}.$$

ζ a liczby pierwsze

Euler udowodnił ponadto tożsamość

$$\zeta(s) = (1 + \frac{1}{2^s} + \frac{1}{4^s} + \ldots)(1 + \frac{1}{3^s} + \frac{1}{9^s} + \ldots)(1 + \frac{1}{5^s} + \frac{1}{25^s} + \ldots) \cdot \ldots =$$

ζ a liczby pierwsze

Euler udowodnił ponadto tożsamość

$$\zeta(s) = (1 + \frac{1}{2^s} + \frac{1}{4^s} + \ldots)(1 + \frac{1}{3^s} + \frac{1}{9^s} + \ldots)(1 + \frac{1}{5^s} + \frac{1}{25^s} + \ldots) \cdot \ldots =$$

$$= \prod_{p \in \mathbb{P}} (1 + \frac{1}{p^s} + \frac{1}{p^{2s}} + \ldots) = \prod_{p \in \mathbb{P}} \frac{1}{1 - \frac{1}{p^s}} \text{ dla } s > 1.$$

ζ a liczby pierwsze

Euler udowodnił ponadto tożsamość

$$\zeta(s) = (1 + \frac{1}{2^s} + \frac{1}{4^s} + \ldots)(1 + \frac{1}{3^s} + \frac{1}{9^s} + \ldots)(1 + \frac{1}{5^s} + \frac{1}{25^s} + \ldots) \cdot \ldots =$$

$$= \prod_{p \in \mathbb{P}} (1 + \frac{1}{p^s} + \frac{1}{p^{2s}} + \ldots) = \prod_{p \in \mathbb{P}} \frac{1}{1 - \frac{1}{p^s}} \text{ dla } s > 1.$$

Widać związek funkcji $\zeta(s)$ z liczbami pierwszymi!

co zrobił Riemann?

Riemann określił funkcję $\zeta(s)$ nie tylko dla liczb rzeczywistych $s > 1$, ale dla wszystkich liczb zespolonych $s \neq 1$: jeśli $s = \sigma + ti$ to σ nazywamy częścią rzeczywistą liczby zespolonej s; natomiast t nazywamy częścią urojoną liczby s.

co zrobił Riemann?

Riemann określił funkcję $\zeta(s)$ nie tylko dla liczb rzeczywistych $s > 1$, ale dla wszystkich liczb zespolonych $s \neq 1$: jeśli $s = \sigma + ti$ to σ nazywamy częścią rzeczywistą liczby zespolonej s; natomiast t nazywamy częścią urojoną liczby s. Co to jest $1/n^s$ dla liczby zespolonej s?

co zrobił Riemann?

Riemann określił funkcję $\zeta(s)$ nie tylko dla liczb rzeczywistych $s > 1$, ale dla wszystkich liczb zespolonych $s \neq 1$: jeśli $s = \sigma + ti$ to σ nazywamy częścią rzeczywistą liczby zespolonej s; natomiast t nazywamy częścią urojoną liczby s. Co to jest $1/n^s$ dla liczby zespolonej s?

$$n^s = n^\sigma(\cos(t \log n) + i \cdot \sin(t \log n)),$$

co zrobił Riemann?

Riemann określił funkcję $\zeta(s)$ nie tylko dla liczb rzeczywistych $s > 1$, ale dla wszystkich liczb zespolonych $s \neq 1$: jeśli $s = \sigma + ti$ to σ nazywamy częścią rzeczywistą liczby zespolonej s; natomiast t nazywamy częścią urojoną liczby s. Co to jest $1/n^s$ dla liczby zespolonej s?

$$n^s = n^\sigma(\cos(t \log n) + i \cdot \sin(t \log n)),$$

gdzie $\log n$ oznacza tzw. logarytm naturalny z liczby n:

$$e^{\log n} = n \text{ gdzie } e \approx 2,718281828.$$

liczba liczb pierwszych $\pi(x)$

Niech dla $x \geq 2$, $\pi(x)$ oznacza liczbę liczb pierwszych p spełniających $p \leq x$.

liczba liczb pierwszych $\pi(x)$

Niech dla $x \geq 2$, $\pi(x)$ oznacza liczbę liczb pierwszych p spełniających $p \leq x$. Mamy np. $\pi(10) = 4$, gdyż wszystkie liczby poniżej 10 to $2, 3, 5, 7$.

liczba liczb pierwszych $\pi(x)$

Niech dla $x \geq 2$, $\pi(x)$ oznacza liczbę liczb pierwszych p spełniających $p \leq x$. Mamy np. $\pi(10) = 4$, gdyż wszystkie liczby poniżej 10 to $2, 3, 5, 7$.Podobnie

$$2, 3, 4, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41,$$

$$43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97$$

to wszystkie liczby pierwsze mniejsze równe 100,

liczba liczb pierwszych $\pi(x)$

Niech dla $x \geq 2$, $\pi(x)$ oznacza liczbę liczb pierwszych p spełniających $p \leq x$. Mamy np. $\pi(10) = 4$, gdyż wszystkie liczby poniżej 10 to $2, 3, 5, 7$.Podobnie

$$2, 3, 4, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41,$$

$$43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97$$

to wszystkie liczby pierwsze mniejsze równe 100,zatem $\pi(100) = 25$.

liczba liczb pierwszych $\pi(x)$

Niech dla $x \geq 2$, $\pi(x)$ oznacza liczbę liczb pierwszych p spełniających $p \leq x$. Mamy np. $\pi(10) = 4$, gdyż wszystkie liczby poniżej 10 to $2, 3, 5, 7$.Podobnie

$$2, 3, 4, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41,$$

$$43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97$$

to wszystkie liczby pierwsze mniejsze równe 100,zatem $\pi(100) = 25$. Można tez obliczyć, że $\pi(10^3) = 168$

liczba liczb pierwszych $\pi(x)$

Niech dla $x \geq 2$, $\pi(x)$ oznacza liczbę liczb pierwszych p spełniających $p \leq x$. Mamy np. $\pi(10) = 4$, gdyż wszystkie liczby poniżej 10 to $2, 3, 5, 7$.Podobnie

$$2, 3, 4, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41,$$

$$43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97$$

to wszystkie liczby pierwsze mniejsze równe 100,zatem $\pi(100) = 25$. Można tez obliczyć, że $\pi(10^3) = 168$ i dalej

$$\pi(10^4) = 1229, \pi(10^5) = 9592, \pi(10^6) = 78498, \pi(10^7) = 664579,$$

liczba liczb pierwszych $\pi(x)$

Niech dla $x \geq 2$, $\pi(x)$ oznacza liczbę liczb pierwszych p spełniających $p \leq x$. Mamy np. $\pi(10) = 4$, gdyż wszystkie liczby poniżej 10 to $2, 3, 5, 7$.Podobnie

$$2, 3, 4, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41,$$

$$43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97$$

to wszystkie liczby pierwsze mniejsze równe 100,zatem $\pi(100) = 25$. Można tez obliczyć, że $\pi(10^3) = 168$ i dalej

$$\pi(10^4) = 1229, \pi(10^5) = 9592, \pi(10^6) = 78498, \pi(10^7) = 664579,$$

$$\pi(10^8) = 5761455, \pi(10^9) = 50847534, \pi(10^{10}) = 455052511.$$

liczba liczb pierwszych $\pi(x)$

x	$\pi(x)$	$x/\log x$	Li(x)
10^2	25	21.71	29.08
10^3	168	144.76	176.56

liczba liczb pierwszych $\pi(x)$

x	$\pi(x)$	$x/\log x$	Li(x)
10^2	25	21.71	29.08
10^3	168	144.76	176.56
10^4	1229	1085.74	1245.09
10^5	9592	8685.89	9628.76
10^6	78498	72382.4	78626.5

liczba liczb pierwszych $\pi(x)$

x	$\pi(x)$	$x/\log x$	Li(x)
10^2	25	21.71	29.08
10^3	168	144.76	176.56
10^4	1229	1085.74	1245.09
10^5	9592	8685.89	9628.76
10^6	78498	72382.4	78626.5
10^7	664579	620421	664917
10^8	5761455	5428680	5762210

liczba liczb pierwszych $\pi(x)$

Zachodzi słynne

Theorem (twierdzenie o liczbach pierwszych)

Mamy

$$\lim_{x\to\infty} \frac{\pi(x)}{x/\log x} = 1.$$

Dowód (wg. J. Hadamard, Ch. J. de la Vallee-Poussin, 1896r.)

liczba liczb pierwszych $\pi(x)$

Zachodzi słynne

Theorem (twierdzenie o liczbach pierwszych)

Mamy

$$\lim_{x\to\infty} \frac{\pi(x)}{x/\log x} = 1.$$

Dowód (wg. J. Hadamard, Ch. J. de la Vallee-Poussin, 1896r.)Tylko główna myśl dowodu:)

liczba liczb pierwszych $\pi(x)$

Zachodzi słynne

Theorem (twierdzenie o liczbach pierwszych)

Mamy

$$\lim_{x\to\infty} \frac{\pi(x)}{x/\log x} = 1.$$

Dowód (wg. J. Hadamard, Ch. J. de la Vallee-Poussin, 1896r.)Tylko główna myśl dowodu:) Trzeba pokazać, że

$$\zeta(\sigma + ti) \neq 0 \text{ dla } \sigma \geq 1.$$

Z tego granica w twierdzeniu wynika już standardowo.

liczba liczb pierwszych $\pi(x)$

Zachodzi słynne

Theorem (twierdzenie o liczbach pierwszych)

Mamy

$$\lim_{x\to\infty} \frac{\pi(x)}{x/\log x} = 1.$$

Dowód (wg. J. Hadamard, Ch. J. de la Vallee-Poussin, 1896r.)Tylko główna myśl dowodu:) Trzeba pokazać, że

$$\zeta(\sigma + ti) \neq 0 \text{ dla } \sigma \geq 1.$$

Z tego granica w twierdzeniu wynika już standardowo. Najtrudniejszy jest przypadek $\sigma = 1$.

Hipoteza Riemanna

HIPOTEZA (Riemann, 1859) Jeśli $\sigma > 0$ oraz $\zeta(\sigma + ti) = 0$ to

Hipoteza Riemanna

HIPOTEZA (Riemann, 1859) Jeśli $\sigma > 0$ oraz $\zeta(\sigma + ti) = 0$ to

$$\sigma = 1/2.$$

Hipoteza Riemanna

HIPOTEZA (Riemann, 1859) Jeśli $\sigma > 0$ oraz $\zeta(\sigma + ti) = 0$ to

$$\sigma = 1/2.$$

Wynika z niej następujące wzmocnienie twierdzenia o liczbach pierwszych:

Hipoteza Riemanna

HIPOTEZA (Riemann, 1859) Jeśli $\sigma > 0$ oraz $\zeta(\sigma + ti) = 0$ to

$$\sigma = 1/2.$$

Wynika z niej następujące wzmocnienie twierdzenia o liczbach pierwszych:
Niech dla $x \geq 2$, $Li(x)$ o znacza całkę

$$Li(x) = \int_2^x \frac{dt}{\log t}.$$

Hipoteza Riemanna

HIPOTEZA (Riemann, 1859) Jeśli $\sigma > 0$ oraz $\zeta(\sigma + ti) = 0$ to

$$\sigma = 1/2.$$

Wynika z niej następujące wzmocnienie twierdzenia o liczbach pierwszych:
Niech dla $x \geq 2$, $Li(x)$ o znacza całkę

$$Li(x) = \int_2^x \frac{dt}{\log t}.$$

Wówczas mamy oszacowanie

$$|\pi(x) - Li(x)| < C\sqrt{x}\log x$$

dla pewnego $C > 0$ i wszystkich $x \geq 2$.

Hipoteza Riemanna

HIPOTEZA (Riemann, 1859) Jeśli $\sigma > 0$ oraz $\zeta(\sigma + ti) = 0$ to

$$\sigma = 1/2.$$

Wynika z niej następujące wzmocnienie twierdzenia o liczbach pierwszych:
Niech dla $x \geq 2$, $Li(x)$ o znacza całkę

$$Li(x) = \int_2^x \frac{dt}{\log t}.$$

Wówczas mamy oszacowanie

$$|\pi(x) - Li(x)| < C\sqrt{x}\log x$$

dla pewnego $C > 0$ i wszystkich $x \geq 2$.
Jest to najważniejsza hipoteza w matematyce teoretycznej, gdyż liczby pierwsze są najważniejsze!

wyniki częściowe w kierunku HR

Jeżeli

wyniki częściowe w kierunku HR

Jeżeli

$$\sigma \geq 1 - \frac{c}{(\log|t|)^{2/3}(\log\log|t|)^{1/3}}$$

wyniki częściowe w kierunku HR

Jeżeli

$$\sigma \geq 1 - \frac{c}{(\log|t|)^{2/3}(\log\log|t|)^{1/3}}$$

to

$$\zeta(\sigma + it) \neq 0$$

wyniki częściowe w kierunku HR

Jeżeli

$$\sigma \geq 1 - \frac{c}{(\log|t|)^{2/3}(\log\log|t|)^{1/3}}$$

to

$$\zeta(\sigma + it) \neq 0$$

Wynika stąd następujące ulepszenie TLP

wyniki częściowe w kierunku HR

Jeżeli

$$\sigma \geq 1 - \frac{c}{(\log|t|)^{2/3}(\log\log|t|)^{1/3}}$$

to

$$\zeta(\sigma + it) \neq 0$$

Wynika stąd następujące ulepszenie TLP

$$|\pi(x) - Li(x)| < Cx\exp(-c(\log x)^{3/5}(\log\log x)^{-1/5})$$

Co najmniej 40% wszystkich zer funkcji $\zeta(s)$ w pasie $0 < \sigma < 1$ spełniają $\sigma = 1/2$

wyniki częściowe w kierunku HR

Jeżeli

$$\sigma \geq 1 - \frac{c}{(\log|t|)^{2/3}(\log\log|t|)^{1/3}}$$

to

$$\zeta(\sigma + it) \neq 0$$

Wynika stąd następujące ulepszenie TLP

$$|\pi(x) - Li(x)| < Cx\exp(-c(\log x)^{3/5}(\log\log x)^{-1/5})$$

Co najmniej 40% wszystkich zer funkcji $\zeta(s)$ w pasie $0 < \sigma < 1$ spełniają $\sigma = 1/2$ (J.B. Conrey 1989).

twierdzenie Woronina (1975)

Niech $0 < r < 1/4$ będzie ustalone a $g(s)$ będzie funkcją ciągłą w kole $K_r = \{s \in \mathbb{C} || s| \leq r\}$ i holomorficzną w jego wnętrzu taką, że

$$g(s) \neq 0 \quad \text{dla każdego } s \in K_r.$$

twierdzenie Woronina (1975)

Niech $0 < r < 1/4$ będzie ustalone a $g(s)$ będzie funkcją ciągłą w kole $K_r = \{s \in \mathbb{C} || s| \leq r\}$ i holomorficzną w jego wnętrzu taką, że

$$g(s) \neq 0 \quad \text{dla każdego } s \in K_r.$$

Wówczas dla każdego $\varepsilon > 0$ istnieje liczba dodatnia τ, taka, że

$$\max_{s \in K_r} |\zeta(\frac{3}{4} + s + \tau i) - g(s)| < \varepsilon.$$

twierdzenie Woronina (1975)

Niech $0 < r < 1/4$ będzie ustalone a $g(s)$ będzie funkcją ciągłą w kole $K_r = \{s \in \mathbb{C} || s| \leq r\}$ i holomorficzną w jego wnętrzu taką, że

$$g(s) \neq 0 \quad \text{dla każdego } s \in K_r.$$

Wówczas dla każdego $\varepsilon > 0$ istnieje liczba dodatnia τ, taka, że

$$\max_{s \in K_r} |\zeta(\frac{3}{4} + s + \tau i) - g(s)| < \varepsilon.$$

Ponadto zbiór tych τ ma dolną gęstość dodatnią.

Nawet tego nie wiadomo

Nawet tego nie wiadomo

Nie wiadomo nawet

Nawet tego nie wiadomo

Nie wiadomo nawet czy zachodzi:

Nawet tego nie wiadomo

Nie wiadomo nawet czy zachodzi:
Jeśli $\sigma \geq 0,999$ *to* $\zeta(\sigma + it) \neq 0$.

Nawet tego nie wiadomo

Nie wiadomo nawet czy zachodzi:
Jeśli $\sigma \geq 0,999$ *to* $\zeta(\sigma + it) \neq 0$.
Jest to zresztą równoważne (von Koch (1901)) następującej wersji TLP:

$$|\pi(x) - Li(x)| < C(\varepsilon)x^{0,999+\varepsilon}$$

dla każdego $\varepsilon > 0$, przy odpowiednim doborze $C(\varepsilon)$.

hipoteza Birch'a-Swinnertona-Dyer'a, lata 60-te XX wieku

Hipoteza Birch'a oraz Swinnerton'a-Dyer'a dotyczy punktów wymiernych na krzywych eliptycznych postaci

$$y^2 = x^3 + Ax + B, \text{ gdzie } A, B \in \mathbb{Z} \text{ oraz } 4A^3 + 27B^2 \neq 0.$$

hipoteza Birch'a-Swinnertona-Dyer'a, lata 60-te XX wieku

Hipoteza Birch'a oraz Swinnerton'a-Dyer'a dotyczy punktów wymiernych na krzywych eliptycznych postaci

$$y^2 = x^3 + Ax + B, \text{ gdzie } A, B \in \mathbb{Z} \text{ oraz } 4A^3 + 27B^2 \neq 0.$$

Naturalne pytanie: czy powyższe równanie ma nieskończenie wiele rozwiązań w liczbach wymiernych x, y?

hipoteza Birch'a-Swinnertona-Dyer'a, lata 60-te XX wieku

Hipoteza Birch'a oraz Swinnerton'a-Dyer'a dotyczy punktów wymiernych na krzywych eliptycznych postaci

$$y^2 = x^3 + Ax + B, \text{ gdzie } A, B \in \mathbb{Z} \text{ oraz } 4A^3 + 27B^2 \neq 0.$$

Naturalne pytanie: czy powyższe równanie ma nieskończenie wiele rozwiązań w liczbach wymiernych x, y? Dla każdej liczby pierwszej p niech N_p oznacza liczbę rozwiązań kongruencji

$$y^2 \equiv x^3 + Ax + B \pmod{p}.$$

przykład

Rozważmy jako przykład krzywą zadaną równaniem

$$y^2 = x^3 + 7x + 13.$$

Łatwo sprawdzić, że poniższa lista zawiera wszystkie rozwiązania kongruencji

$$y^2 \equiv x^3 + 7x + 13 \pmod{31}.$$

$$\{(2,2),(2,-2),(5,7),(5,-7),(7,8),(7,-8),(13,10),$$

$$(13,-10),(16,6),(16,-6),(18,9),(18,-9),(20,0),(21,11),$$

$$(21,-11),(26,15),(26,-15),(27,13),(27,-13),(30,6),(30,-6)\}.$$

Tutaj $N_{31} = 21$.

L-funkcja Hasse-Weil'a

Określamy funkcję

$$L(s) = \prod_{p*} \left(1 - \frac{p - N_p}{p^s} + \frac{1}{p^{2s-1}}\right)^{-1}.$$

L-funkcja Hasse-Weil'a

Określamy funkcję

$$L(s) = \prod_{p*} \left(1 - \frac{p - N_p}{p^s} + \frac{1}{p^{2s-1}}\right)^{-1}.$$

Dla naszej przykładowej krzywej $y^2 = x^3 + 7x + 13$ czynnik odpowiadający $p = 31$ wynosi

$$\left(1 - \frac{10}{31^s} + \frac{1}{31^{2s-1}}\right)^{-1}.$$

L-funkcja Hasse-Weil'a

Określamy funkcję

$$L(s) = \prod_{p*} \left(1 - \frac{p - N_p}{p^s} + \frac{1}{p^{2s-1}}\right)^{-1}.$$

Dla naszej przykładowej krzywej $y^2 = x^3 + 7x + 13$ czynnik odpowiadający $p = 31$ wynosi

$$\left(1 - \frac{10}{31^s} + \frac{1}{31^{2s-1}}\right)^{-1}.$$

Powyższy iloczyn nieskończony definiujący $L(s)$ jest zbieżny dla $s > 3/2$.

hipoteza Birch'a-Swinnertona-Dyer'a, lata 60-te XX wieku

Równanie $y^2 = x^3 + Ax + B$ ma nieskończenie wiele rozwiązań w liczbach wymiernych x, y wtedy i tylko wtedy, gdy $L(1) = 0$.

hipoteza Birch'a-Swinnertona-Dyer'a, lata 60-te XX wieku

Równanie $y^2 = x^3 + Ax + B$ ma nieskończenie wiele rozwiązań w liczbach wymiernych x, y wtedy i tylko wtedy, gdy $L(1) = 0$.
(a) To, że funkcja $L(s)$ jest okreslona dla $s = 1$ wiadomo dopiero od ok. 2001 roku (Breuil i inni, wg pomysłów A. Wiles'a)

hipoteza Birch'a-Swinnertona-Dyer'a, lata 60-te XX wieku

Równanie $y^2 = x^3 + Ax + B$ ma nieskończenie wiele rozwiązań w liczbach wymiernych x, y wtedy i tylko wtedy, gdy $L(1) = 0$.
(a) To, że funkcja $L(s)$ jest okreslona dla $s = 1$ wiadomo dopiero od ok. 2001 roku (Breuil i inni, wg pomysłów A. Wiles'a)
(b) Dla konkretnej krzywej mozna obliczyc na komputerze przybliżoną wartość $L(1)$; w przypadku $L(1) \neq 0$ wnioskujemy, że powyższe równanie ma co najwyżej skończenie wiele rozwiązań; wtedy łatwo je wyznaczyć;

hipoteza Birch'a-Swinnertona-Dyer'a, lata 60-te XX wieku

Równanie $y^2 = x^3 + Ax + B$ ma nieskończenie wiele rozwiązań w liczbach wymiernych x, y wtedy i tylko wtedy, gdy $L(1) = 0$.
(a) To, że funkcja $L(s)$ jest okreslona dla $s = 1$ wiadomo dopiero od ok. 2001 roku (Breuil i inni, wg pomysłów A. Wiles'a)
(b) Dla konkretnej krzywej mozna obliczyc na komputerze przybliżoną wartość $L(1)$; w przypadku $L(1) \neq 0$ wnioskujemy, że powyższe równanie ma co najwyżej skończenie wiele rozwiązań; wtedy łatwo je wyznaczyć;
(c) Gdy wyjdzie $L(1) \approx 0$ to mamy kłopot:); szukamy rozwiązania (x, y), z którego można wyprodukować nieskończenie wiele rozwiązań.

przykład 1

Nasza stara krzywa $y^2 = x^3 + 7x + 13$.

przykład 1

Nasza stara krzywa $y^2 = x^3 + 7x + 13$. Dla niej $L(1) \approx 2,361\ldots \neq 0$. O ile hipoteza BSD jest prawdziwa dla tej krzywej to liczba punktów wymiernych na niej powinna być skończona.

przykład 1

Nasza stara krzywa $y^2 = x^3 + 7x + 13$. Dla niej $L(1) \approx 2,361\ldots \neq 0$. O ile hipoteza BSD jest prawdziwa dla tej krzywej to liczba punktów wymiernych na niej powinna być skończona. Można udowodnić, że równanie

$$y^2 = x^3 + 7x + 13$$

nie ma rozwiązań w liczbach wymiernych x, y.

przykład 2

Niech teraz krzywa ma równanie $y^2 = x^3 + 17$. Obliczamy na komputerze $L(1)$ i otrzymujemy

$$L(1) \approx -5,55169904\ldots \cdot 10^{-28}$$

przykład 2

Niech teraz krzywa ma równanie $y^2 = x^3 + 17$. Obliczamy na komputerze $L(1)$ i otrzymujemy

$$L(1) \approx -5,55169904\ldots \cdot 10^{-28}$$

Zatem prawdopodobnie $L(1) = 0$ i równanie

$$y^2 = x^3 + 17$$

ma (prawdopodobnie) nieskończenie wiele rozwiązań w liczbach wymiernych x, y.

przykład 2

Niech teraz krzywa ma równanie $y^2 = x^3 + 17$. Obliczamy na komputerze $L(1)$ i otrzymujemy

$$L(1) \approx -5,55169904\ldots \cdot 10^{-28}$$

Zatem prawdopodobnie $L(1) = 0$ i równanie

$$y^2 = x^3 + 17$$

ma (prawdopodobnie) nieskończenie wiele rozwiązań w liczbach wymiernych x, y. Łatwo zgadnąć rozwiązania

$$P_1 = (-2, 3),$$

przykład 2

Niech teraz krzywa ma równanie $y^2 = x^3 + 17$. Obliczamy na komputerze $L(1)$ i otrzymujemy

$$L(1) \approx -5,55169904\ldots \cdot 10^{-28}$$

Zatem prawdopodobnie $L(1) = 0$ i równanie

$$y^2 = x^3 + 17$$

ma (prawdopodobnie) nieskończenie wiele rozwiązań w liczbach wymiernych x, y. Łatwo zgadnąć rozwiązania

$$P_1 = (-2, 3),\ P_2 = (-1, 4),$$

przykład 2

Niech teraz krzywa ma równanie $y^2 = x^3 + 17$. Obliczamy na komputerze $L(1)$ i otrzymujemy

$$L(1) \approx -5,55169904\ldots \cdot 10^{-28}$$

Zatem prawdopodobnie $L(1) = 0$ i równanie

$$y^2 = x^3 + 17$$

ma (prawdopodobnie) nieskończenie wiele rozwiązań w liczbach wymiernych x, y.Łatwo zgadnąć rozwiązania

$$P_1 = (-2, 3),\ P_2 = (-1, 4),\ P_3 = (4, -9), \ldots (?)$$

Mamy tu $P_3 = P_1 \oplus P_2$ oraz

$$L(s) = (s-1)^2 \cdot a + (s-1)^3 \cdot b + \ldots$$

przykład 2 koniec:)

Punkt

$$P = (\frac{-2228}{961}, \frac{-63465}{29791})$$

też należy do krzywej $y^2 = x^3 + 17\ldots$

przykład 2 koniec:)

Punkt

$$P = (\frac{-2228}{961}, \frac{-63465}{29791})$$

też należy do krzywej $y^2 = x^3 + 17\ldots$ i ∞ wiele innych.

wyniki częściowe

wyniki częściowe

Twierdzenie (J. Coates, A. Wiles, 1977). Jeśli krzywa eliptyczna E ma mnożenie zespolone oraz $L(1) \neq 0$ to leży na niej co najwyżej skończenie wiele punktów wymiernych.

Twierdzenie (J. Coates, A. Wiles, 1977). Jeśli krzywa eliptyczna E ma mnożenie zespolone oraz $L(1) \neq 0$ to leży na niej co najwyżej skończenie wiele punktów wymiernych.

Uwaga. Do krzywych z mnożeniem zespolonym należą np. krzywe typu $y^2 = x^3 + B$ oraz typu $y^2 = x^3 + Ax$.

wyniki częściowe

Twierdzenie (J. Coates, A. Wiles, 1977). Jeśli krzywa eliptyczna E ma mnożenie zespolone oraz $L(1) \neq 0$ to leży na niej co najwyżej skończenie wiele punktów wymiernych.

Uwaga. Do krzywych z mnożeniem zespolonym należą np. krzywe typu $y^2 = x^3 + B$ oraz typu $y^2 = x^3 + Ax$.

Twierdzenie (B. Gross, D. Zagier, 1986). Jeśli krzywa E jest modularna oraz $s = 1$ jest zerem jednokrotnym funkcji $L(s)$ to na krzywej E leży nieskończenie wiele punktów wymiernych.

wyniki częściowe

Twierdzenie (J. Coates, A. Wiles, 1977). Jeśli krzywa eliptyczna E ma mnożenie zespolone oraz $L(1) \neq 0$ to leży na niej co najwyżej skończenie wiele punktów wymiernych.

Uwaga. Do krzywych z mnożeniem zespolonym należą np. krzywe typu $y^2 = x^3 + B$ oraz typu $y^2 = x^3 + Ax$.

Twierdzenie (B. Gross, D. Zagier, 1986). Jeśli krzywa E jest modularna oraz $s = 1$ jest zerem jednokrotnym funkcji $L(s)$ to na krzywej E leży nieskończenie wiele punktów wymiernych.

Uwaga. Każda krzywa eliptyczna o współczynnikach wymiernych jest modularna.

wyniki częściowe

Twierdzenie (J. Coates, A. Wiles, 1977). Jeśli krzywa eliptyczna E ma mnożenie zespolone oraz $L(1) \neq 0$ to leży na niej co najwyżej skończenie wiele punktów wymiernych.

Uwaga. Do krzywych z mnożeniem zespolonym należą np. krzywe typu $y^2 = x^3 + B$ oraz typu $y^2 = x^3 + Ax$.

Twierdzenie (B. Gross, D. Zagier, 1986). Jeśli krzywa E jest modularna oraz $s = 1$ jest zerem jednokrotnym funkcji $L(s)$ to na krzywej E leży nieskończenie wiele punktów wymiernych.

Uwaga. Każda krzywa eliptyczna o współczynnikach wymiernych jest modularna. (A. Wiles i inni).

zastosowanie BSD do problemu liczb kongruentnych

Liczbę naturalną n nazywamy **kongruentną** wtw (z definicji), gdy

zastosowanie BSD do problemu liczb kongruentnych

Liczbę naturalną n nazywamy **kongruentną** wtw (z definicji), gdy istnieją liczby wymierne dodatnie x, y, z takie, że

$$n = \frac{1}{2}xy$$

zastosowanie BSD do problemu liczb kongruentnych

Liczbę naturalną n nazywamy **kongruentną** wtw (z definicji), gdy istnieją liczby wymierne dodatnie x, y, z takie, że

$$n = \frac{1}{2}xy$$

tzn. n jest polem trójkąta prostokatnego o wymiernych bokach.

zastosowanie BSD do problemu liczb kongruentnych

Liczbę naturalną n nazywamy **kongruentną** wtw (z definicji), gdy istnieją liczby wymierne dodatnie x, y, z takie, że

$$n = \frac{1}{2}xy$$

tzn. n jest polem trójkąta prostokatnego o wymiernych bokach.
Liczba $n = 6$ jest kongruentna, gdyż $6 = (3 \cdot 4)/2$ oraz $3^2 + 4^2 = 5^2$.

zastosowanie BSD do problemu liczb kongruentnych

Liczbę naturalną n nazywamy **kongruentną** wtw (z definicji), gdy istnieją liczby wymierne dodatnie x, y, z takie, że

$$n = \frac{1}{2}xy$$

tzn. n jest polem trójkąta prostokatnego o wymiernych bokach.
Liczba $n = 6$ jest kongruentna, gdyż $6 = (3 \cdot 4)/2$ oraz $3^2 + 4^2 = 5^2$. A mniejsze liczby naturalne?

zastosowanie BSD do problemu liczb kongruentnych

Liczbę naturalną n nazywamy **kongruentną** wtw (z definicji), gdy istnieją liczby wymierne dodatnie x, y, z takie, że

$$n = \frac{1}{2}xy$$

tzn. n jest polem trójkąta prostokatnego o wymiernych bokach. Liczba $n = 6$ jest kongruentna, gdyż $6 = (3 \cdot 4)/2$ oraz $3^2 + 4^2 = 5^2$. A mniejsze liczby naturalne?To, że $n = 1$ nie jest kongruentna jest równoważne następującemu faktowi:

zastosowanie BSD do problemu liczb kongruentnych

Liczbę naturalną n nazywamy **kongruentną** wtw (z definicji), gdy istnieją liczby wymierne dodatnie x, y, z takie, że

$$n = \frac{1}{2}xy$$

tzn. n jest polem trójkąta prostokatnego o wymiernych bokach.
Liczba $n = 6$ jest kongruentna, gdyż $6 = (3 \cdot 4)/2$ oraz $3^2 + 4^2 = 5^2$. A mniejsze liczby naturalne?To, że $n = 1$ nie jest kongruentna jest równoważne następującemu faktowi:
P. Fermat

zastosowanie BSD do problemu liczb kongruentnych

Liczbę naturalną n nazywamy **kongruentną** wtw (z definicji), gdy istnieją liczby wymierne dodatnie x, y, z takie, że

$$n = \frac{1}{2}xy$$

tzn. n jest polem trójkąta prostokatnego o wymiernych bokach.
Liczba $n = 6$ jest kongruentna, gdyż $6 = (3 \cdot 4)/2$ oraz $3^2 + 4^2 = 5^2$. A mniejsze liczby naturalne?To, że $n = 1$ nie jest kongruentna jest równoważne następującemu faktowi:
P. Fermat *nie ma takich liczb naturalnych $a \neq b$, że zarówno $a^2 - b^2$ jak i $a^2 + b^2$ są kwadratami.*

problem liczb kongruentnych

Niech

$$x = \frac{411340519227716149383203}{21666555693714761309610}$$

problem liczb kongruentnych

Niech

$$x = \frac{411340519227716149383203}{21666555693714761309610}$$

$$y = \frac{6803298487826435051217540}{411340519227716149383203}$$

problem liczb kongruentnych

Niech

$$x = \frac{411340519227716149383203}{21666555693714761309610}$$

$$y = \frac{6803298487826435051217540}{411340519227716149383203}$$

$$z = \frac{224403517704336969924557513090674863160948472041}{8912332268928859588025535178967163570016480830}.$$

Łatwiej sprawdzić (niż wypisać powyższe), że

$$x^2 + y^2 = z^2$$

oraz

$$\frac{1}{2}xy = 157.$$

problem liczb kongruentnych

Niech

$$x = \frac{411340519227716149383203}{216665556937147613096 10}$$

$$y = \frac{6803298487826435051217540}{411340519227716149383203}$$

$$z = \frac{224403517704336969924557513090674863160948472041}{8912332268928859588025535178967163570016480830}.$$

Łatwiej sprawdzić (niż wypisać powyższe), że

$$x^2 + y^2 = z^2$$

oraz

$$\frac{1}{2}xy = 157.$$

Zatem liczba 157 jest kongruentna.

twierdzenie Tunnela

Niech n liczbą nieparzystą bezkwadratową. Rozważmy dwa warunki

twierdzenie Tunnela

Niech n liczbą nieparzystą bezkwadratową. Rozważmy dwa warunki

1. Liczba n jest kongruentna.
2. liczba trójek liczb całkowitych (x, y, z) spełniających równanie

twierdzenie Tunnela

Niech n liczbą nieparzystą bezkwadratową. Rozważmy dwa warunki

1. Liczba n jest kongruentna.
2. liczba trójek liczb całkowitych (x, y, z) spełniających równanie

$$2x^2 + y^2 + 8z^2 = n$$

twierdzenie Tunnela

Niech n liczbą nieparzystą bezkwadratową. Rozważmy dwa warunki

1. Liczba n jest kongruentna.
2. liczba trójek liczb całkowitych (x, y, z) spełniających równanie

$$2x^2 + y^2 + 8z^2 = n$$

równa się dwa razy liczba trójek spełniających równanie

twierdzenie Tunnela

Niech n liczbą nieparzystą bezkwadratową. Rozważmy dwa warunki

1. Liczba n jest kongruentna.
2. liczba trójek liczb całkowitych (x, y, z) spełniających równanie

$$2x^2 + y^2 + 8z^2 = n$$

równa się dwa razy liczba trójek spełniających równanie

$$2x^2 + y^2 + 32z^2 = n$$

twierdzenie Tunnela

Niech n liczbą nieparzystą bezkwadratową. Rozważmy dwa warunki

1. Liczba n jest kongruentna.
2. liczba trójek liczb całkowitych (x, y, z) spełniających równanie

$$2x^2 + y^2 + 8z^2 = n$$

równa się dwa razy liczba trójek spełniających równanie

$$2x^2 + y^2 + 32z^2 = n$$

Wówczas z (1) wynika (2).

twierdzenie Tunnela

Niech n liczbą nieparzystą bezkwadratową. Rozważmy dwa warunki

1. Liczba n jest kongruentna.
2. liczba trójek liczb całkowitych (x, y, z) spełniających równanie

$$2x^2 + y^2 + 8z^2 = n$$

równa się dwa razy liczba trójek spełniających równanie

$$2x^2 + y^2 + 32z^2 = n$$

Wówczas z (1) wynika (2).Ponadto, jeżeli zachodzi słaba wersja hipotezy Bircha-Swinnertona-Dyera to również z (2) wynika (1).

wniosek z twierdzenia Tunnela

Każda liczba bezkwadratowa n postaci $8k+5$ lub $8k+7$ jest kongruentna.

wniosek z twierdzenia Tunnela

Każda liczba bezkwadratowa n postaci $8k+5$ lub $8k+7$ jest kongruentna.
Dowód. Łatwo sprawdzić, że $n = 8k+5$ nie jest postaci $2x^2 + y^2 + 8z^2$

wniosek z twierdzenia Tunnela

Każda liczba bezkwadratowa n postaci $8k+5$ lub $8k+7$ jest kongruentna.
Dowód. Łatwo sprawdzić, że $n = 8k+5$ nie jest postaci $2x^2 + y^2 + 8z^2$ zatem $0 = 2 \cdot 0$ i warunek Tunella z poprzedniego slajdu jest spełniony.

wniosek z twierdzenia Tunnela

Każda liczba bezkwadratowa n postaci $8k+5$ lub $8k+7$ jest kongruentna.
Dowód. Łatwo sprawdzić, że $n = 8k+5$ nie jest postaci $2x^2 + y^2 + 8z^2$ zatem $0 = 2 \cdot 0$ i warunek Tunella z poprzedniego slajdu jest spełniony.
Uwaga. Gdy powyższe n jest liczbą pierwszą to jest kongruentna (bez żadnych hipotez).

Dziękuję.