§1. 素数(Prime Number)

定義　1と自分自身以外に正の約数をもたない2以上の整数を素数という。

注1)　整数 m, n に対し, $\frac{n}{m}$ が再び整数であるとき, つまり, $n = m \times$ (整数) の形に書けるとき, m は n の約数という。　記号 $m|n$

注2)　1は素数とは考えない。

例　2, 3, 5, 7, 11, 13, 17, 19 は素数.
4, 6, 8, 9, 10, 12, 14, 15, 16, 18, 20 は素数ではない。
$12 = 2 \times 6$　2は12でも1でもない12の約数　$2|12$

素数：0, 1について基本的な整数
整数における元素の役割

定理(Euclid)

2以上の整数はすべて有限個の素数の積に書ける。(素因数分解できる。)

しかも，(積の形にするプロセスによらず)書き表し方は，次の意味で一通り：

与えられた整数 $n \geqq 2$ に対し，n の素因数分解にあらわれる各素数 p の個数は n により一通りにきまる。

例

$$72 \overset{\text{順番}}{=} 2\cdot 36 = 2\cdot 2\cdot 18 = 2\cdot 2\cdot 2\cdot 9 = \overbrace{2\cdot 2\cdot 2}^{3\text{個}}\cdot\overbrace{3\cdot 3}^{2\text{個}}$$

$$= 2^3\cdot 3^2$$

$$72 \overset{\text{工夫}}{=} 8\cdot 9 = (2\cdot 2\cdot 2)\cdot(3\cdot 3) = 2^3\cdot 3^2$$

同じ

応用　約数，倍数の性質をはじめ多彩.

注) 定理の証明

前半: 定義から容易

後半: それなりに難しい。次の問を用いる。

問(既知) 次を示せ。

pを素数, m, nを整数とする。このとき,

$p \mid m \cdot n$ ならば, $p \mid m$ 又は $p \mid n$ である。

素数の見つけ方(Eratosthenesのふるい)

例 100以下の素数

	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

素数の見つけ方(Eratosthenesのふるい)

例　100以下の素数

	2	3	~~4~~	5	~~6~~	7	~~8~~	9	~~10~~
11	~~12~~	13	~~14~~	15	~~16~~	17	~~18~~	19	~~20~~
21	~~22~~	23	~~24~~	25	~~26~~	27	~~28~~	29	~~30~~
31	~~32~~	33	~~34~~	35	~~36~~	37	~~38~~	39	~~40~~
41	~~42~~	43	~~44~~	45	~~46~~	47	~~48~~	49	~~50~~
51	~~52~~	53	~~54~~	55	~~56~~	57	~~58~~	59	~~60~~
61	~~62~~	63	~~64~~	65	~~66~~	67	~~68~~	69	~~70~~
71	~~72~~	73	~~74~~	75	~~76~~	77	~~78~~	79	~~80~~
81	~~82~~	83	~~84~~	85	~~86~~	87	~~88~~	89	~~90~~
91	~~92~~	93	~~94~~	95	~~96~~	97	~~98~~	99	~~100~~

素数の見つけ方(Eratosthenesのふるい)

例　100以下の素数

	2	3	~~4~~	5	~~6~~	7	~~8~~	~~9~~	~~10~~
11	~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~
~~21~~	~~22~~	23	~~24~~	25	~~26~~	~~27~~	~~28~~	29	~~30~~
31	~~32~~	~~33~~	~~34~~	35	~~36~~	37	~~38~~	~~39~~	~~40~~
41	~~42~~	43	~~44~~	~~45~~	~~46~~	47	~~48~~	49	~~50~~
~~51~~	~~52~~	53	~~54~~	55	~~56~~	~~57~~	~~58~~	59	~~60~~
61	~~62~~	~~63~~	~~64~~	65	~~66~~	67	~~68~~	~~69~~	~~70~~
71	~~72~~	73	~~74~~	~~75~~	~~76~~	77	~~78~~	79	~~80~~
~~81~~	~~82~~	83	~~84~~	85	~~86~~	~~87~~	~~88~~	89	~~90~~
91	~~92~~	~~93~~	~~94~~	95	~~96~~	97	~~98~~	~~99~~	~~100~~

素数の見つけ方(Eratosthenesのふるい)

例　100以下の素数

2 3 ~~4~~ 5 ~~6~~ 7 ~~8~~ ~~9~~ ~~10~~

11 ~~12~~ 13 ~~14~~ ~~15~~ ~~16~~ 17 ~~18~~ 19 ~~20~~

~~21~~ ~~22~~ 23 ~~24~~ ~~25~~ ~~26~~ ~~27~~ ~~28~~ 29 ~~30~~

31 ~~32~~ ~~33~~ ~~34~~ ~~35~~ ~~36~~ 37 ~~38~~ ~~39~~ ~~40~~

41 ~~42~~ 43 44 ~~45~~ ~~46~~ 47 ~~48~~ 49 ~~50~~

~~51~~ ~~52~~ 53 ~~54~~ ~~55~~ ~~56~~ ~~57~~ ~~58~~ 59 ~~60~~

61 ~~62~~ ~~63~~ ~~64~~ ~~65~~ ~~66~~ 67 ~~68~~ ~~69~~ ~~70~~

71 ~~72~~ 73 ~~74~~ ~~75~~ ~~76~~ 77 ~~78~~ 79 ~~80~~

~~81~~ ~~82~~ 83 ~~84~~ ~~85~~ ~~86~~ ~~87~~ ~~88~~ 89 ~~90~~

91 ~~92~~ ~~93~~ ~~94~~ ~~95~~ ~~96~~ 97 ~~98~~ ~~99~~ ~~100~~

素数の見つけ方(Eratosthenesのふるい)

例 100以下の素数

	2	3	~~4~~	5	~~6~~	7	~~8~~	~~9~~	~~10~~
11	~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~
~~21~~	~~22~~	23	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	29	~~30~~
31	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	37	~~38~~	~~39~~	~~40~~
41	~~42~~	43	~~44~~	~~45~~	~~46~~	47	~~48~~	~~49~~	~~50~~
~~51~~	~~52~~	53	~~54~~	~~55~~	~~56~~	~~57~~	~~58~~	59	~~60~~
61	~~62~~	~~63~~	~~64~~	~~65~~	~~66~~	67	~~68~~	~~69~~	~~70~~
71	~~72~~	73	~~74~~	~~75~~	~~76~~	~~77~~	~~78~~	79	~~80~~
~~81~~	~~82~~	83	~~84~~	~~85~~	~~86~~	~~87~~	~~88~~	89	~~90~~
~~91~~	~~92~~	~~93~~	~~94~~	~~95~~	~~96~~	97	~~98~~	~~99~~	~~100~~

素数の見つけ方(Eratosthenesのふるい)

例 100以下の素数

$\sqrt{100}=10$より大

	2	3	~~4~~	5	~~6~~	7	~~8~~	~~9~~	~~10~~
11	~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~
~~21~~	~~22~~	23	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	29	~~30~~
31	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	37	~~38~~	~~39~~	~~40~~
41	~~42~~	43	~~44~~	~~45~~	~~46~~	47	~~48~~	~~49~~	~~50~~
~~51~~	~~52~~	53	~~54~~	~~55~~	~~56~~	~~57~~	~~58~~	59	~~60~~
61	~~62~~	~~63~~	~~64~~	~~65~~	~~66~~	67	~~68~~	~~69~~	~~70~~
71	~~72~~	73	~~74~~	~~75~~	~~76~~	~~77~~	~~78~~	79	~~80~~
~~81~~	~~82~~	83	~~84~~	~~85~~	~~86~~	~~87~~	~~88~~	89	~~90~~
~~91~~	~~92~~	~~93~~	~~94~~	~~95~~	~~96~~	97	~~98~~	~~99~~	~~100~~

行ったこと

1. 最初の数2を残し，2×(2以上の整数)を消す。

2. 次に残った最初の数3を残し，
3×(2以上の整数)を消す。

3. —————— 5 ———，
5×(2以上の整数)を消す。

4. —————— 7 ———，
7×(2以上の整数)を消す。

5. (観察) もう $\sqrt{100}=10$ 以下の数で新しく残っている数はない。消された数はすべて合成数。

結論 {残っている数} = {100以下の素数}

∵ 残っているある数 n が素数でなかったなら，
$n=p\cdot m$ (p は n をわる最小の素数，$m \geqq 2$)
の形。p の最小性から，
$p^2 \leqq p\cdot m = n \leqq 100$ ∴ $p \leqq \sqrt{100}=10$
従って，n は1〜4で消されているはず。矛盾！

・こうして，100以下の素数は

2，3，5，7，11，13，17，19

23，29，31，37，41，43，47，53

59，61，67，71，73，79，83，89，97

の25個.

・同じ考え方で，

10000（＝1万）以下の素数を全部

見い出すには，100以下の素数 p に対し，

$p\times$（2以上の整数）をすべて消せばよい。

・Gauß（Gauss）の時代（1777年～1855年）

すでに $\underbrace{400031}_{6ケタ}$ までの素数の表があった。

⇝ 素数定理の"発見"

（cf. 文献1-3 AppendixB，1849年12月24日の手紙）

現在：

・報告されている最大の素数

$2^{43112609}-1$ ← $2^{(素数)}-1$の形の素数

(12978189けた)　(メルセンヌ数)

・1億けた以上の素数の最初の発見者(団体)

には15万ドルの賞金

(cf. http://www.eff.org/awards/coop)

注) 数の1億＝100000000 (9けた)

注) 1億けたの素数をふつうに書くと：

2つの数字を1秒で書くとして

書くのに要する時間＝5000万秒

1日12時間頑張って書き続けても

$\frac{50000000}{60\times 60\times 12} \fallingdotseq 1157.4$日 (約3年2か月)

かかる。

素数はどの位あるか？

定理(Euclid) 素数は無限個ある。

証明(F. Saidak, 2006年)

注1) 無限個：自然数Bをどのように与えても，
必ずB個以上見い出せる。

注2) nと$n+1$をともにわる自然数は1のみ.

(∵ $m \mid n$ かつ $m \mid (n+1) \underset{\text{引算}}{\Rightarrow} m \mid 1 \Rightarrow m=1$.)

注3) 自然数$n\ (\geqq 2)$が異なる素因数をk個以上
もてば，$n(n+1)$は異なる素因数を$(k+1)$個以上
もつ。

(∵ 注2)により，$n+1$の素因数は，nのどの素因数
とも異なる。故に，最低1個はふえるから。)

注3)をくり返し用いることにより，数列

どんどん

$a_1=2,\ a_2=a_1(a_1+1),\ a_3=a_2(a_2+1),\ a_4=a_3(a_3+1), \cdots$

の第B項目a_Bは少くともB個異なる素因数をもつ。

特に，B個以上異なる素数がある。

証明2（Euler）

素数を小さい方からならべ，m番目の素数まで考える：

$p_1=2,\ p_2=3,\ \cdots,\ p_k,\ \cdots,\ p_m$

|公比|<1 の等比級数の和の公式

$$\frac{1}{1-\frac{1}{p_k^s}}=1+\frac{1}{p_k^s}+\frac{1}{p_k^{2s}}+\cdots+\frac{1}{p_k^{ls}}+\cdots\quad(s>1)$$

全部かけて

$$\prod_{k=1}^{m}\frac{1}{1-\frac{1}{p_k^s}}=\left(1+\frac{1}{p_1^s}+\frac{1}{p_1^{2s}}+\cdots\right)\left(1+\frac{1}{p_2^s}+\frac{1}{p_2^{2s}}+\cdots\right)\cdots\left(1+\frac{1}{p_m^s}+\frac{1}{p_m^{2s}}+\cdots\right)$$

右辺の展開：$\dfrac{1}{(p_1^{l_1}p_2^{l_2}\cdots p_m^{l_m})^s}$ $(l_1,l_2,\cdots,l_m\geqq 0)$

の形の項が1回ずつあらわれる。これより，

$$\prod_{k=1}^{m}\frac{1}{1-\frac{1}{p_k^s}}=\left(\text{すべての } l_1,\cdots,l_m\geqq 0 \text{ にわたる } \frac{1}{(p_1^{l_1}p_2^{l_2}\cdots p_m^{l_m})^s} \text{ の和}\right)$$

$$=\sum_{\substack{n\text{の素因数は}\\ p_1,p_2,\cdots,p_m\text{のみ}}}\frac{1}{n^s}\quad\text{—}(*)$$

↑

素因数分解の定理

以下，素数が有限個しかなかったと仮定する。

$p_1, p_2, \cdots, p_m$ が全部としてよい。すると：

(※)の右辺＝すべての自然数にわたる $\frac{1}{n^s}$ の和

$$\prod_{k=1}^{m} \frac{1}{1-\frac{1}{p_k^s}} = \sum_{n=1}^{\infty} \frac{1}{n^s} \quad (s>1)$$

（素因数分解定理）

特に，任意の自然数 N に対し

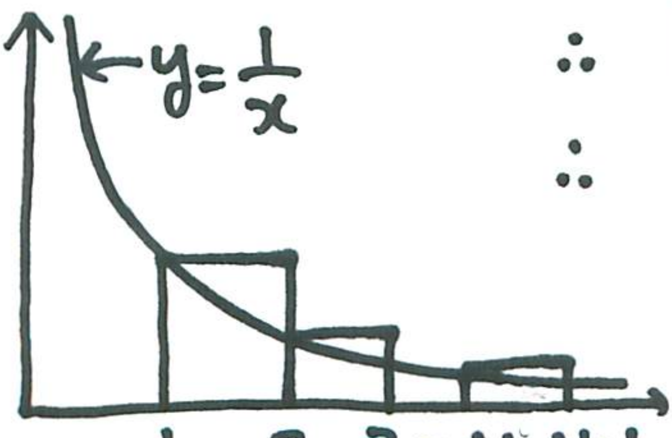
$$\prod_{k=1}^{m} \frac{1}{1-\frac{1}{p_k^s}} \geqq \sum_{n=1}^{N} \frac{1}{n^s}.$$

$s \to 1+0$ として

$$P = \prod_{k=1}^{m} \frac{1}{1-\frac{1}{p_k}} \geqq \sum_{n=1}^{N} \frac{1}{n}$$

（注：P は N によらない定数）

他方，$\displaystyle\sum_{n=1}^{N} \frac{1}{n} \geqq \int_1^{N+1} \frac{dx}{x} = \log(N+1)$



$\therefore\ P \geqq \log(N+1)$

$\therefore\ N \leqq e^P - 1$

N は任意の自然数にとれたことに矛盾！

・証明2の後半より

$$\sum_{n=1}^{\infty} \frac{1}{n} = +\infty$$

・収束に注意して，(*)で $m \to \infty$ として

定理（Euler）

$s > 1$ のとき

$$\zeta(s) \underset{\text{定義}}{=} \sum_{n=1}^{\infty} \frac{1}{n^s} = \frac{1}{\displaystyle\prod_{p:\text{素数}} \left(1 - \frac{1}{p^s}\right)}$$

（素数定理においても本質的）

こうして、素数を小さい方から順にならべた無限数列(素数列)

$$\begin{array}{cccccccc} p_1, & p_2, & p_3, & p_4, & \cdots, & p_n, & \cdots \\ \shortparallel & \shortparallel & \shortparallel & \shortparallel & & \shortparallel & \\ 2 & 3 & 5 & 7 & & \boxed{?} & \end{array}$$

ができる。

・n番目の素数p_nを明示的に与える公式は知られていない。

問(既知) 次を示せ。

(1) $p_n = f(n)$ (nはある自然数以上のすべての自然数)である整数を係数とする多項式$f(x)$はない。

(2) $p_n = \dfrac{G(n)}{F(n)}$ (nはある自然数以上のすべての自然数)である有理数を係数とする多項式$F(x)$, $G(x)$もない。

Gauß

$\pi(n)$ =（n 以下の素数の個数）

と

積分 $\displaystyle\int_2^n \frac{dx}{\log x}$ の比を比較し，

$n\to\infty$ で（比）$\longrightarrow 1$ と予測．

注）$\displaystyle\int_2^n \frac{dx}{\log x}$ との比を考えるかわりに

$\dfrac{n}{\log n}$ との比を考えても同じ．

☺ 問（既知）

$$\lim_{n\to\infty} \int_2^n \frac{dx}{\log x} \Big/ \frac{n}{\log n} = 1$$

を示せ。

素数定理(Prime Number Theorem, 1896年)

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

Euler, Gauß, Dirichlet, Chebychev, Riemann
らの本質的貢献を経て,
1896年に, Hadamard と de la Vallée Poussin
により独立に証明された。
$\zeta(s)$を複素数変数の関数に拡張して
考えること(複素関数論)が本質的.

1980年 D.J. Newman: 同路線だが非常に
簡単な証明を発見.

D.J. Newmanの証明:
D. Zagierによる2ページの自己完結的かつ
非常に明快な解説がある。
(大学2年生以上の人におすすめ。)

問(既知)

(1) 素数定理を用いて，次を示せ。

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

(2) 更に，Bakerの定理

$\log n$ (nは2以上の整数)は超越数

も既知として，次を示せ。

$$p_n=\frac{G(n,\log n)}{F(n,\log n)}\quad(n=1,2,3,\cdots)$$

である有理数を係数とする多項式

$F(x,y)$, $G(x,y)$はない。

(注) (2)で係数を実数や複素数に拡張した場合は，講演者には？)

§2. Green-Tao の定理

主定理 I (Green-Tao, Annals of Mathematics 167巻 481-547 (2008))

素数列

$p_1, p_2, p_3, \ldots, p_n, \ldots$

には，いくらでも長い 有限 等差数列

が含まれる。つまり，

与えられた自然数 k に対し，

素数列の中からうまく k 個の項をとり出して，

k 個の素数からなる等差数列

$p_{l_1}, p_{l_2}, \ldots, p_{l_k}$ $(l_1 < l_2 < \cdots < l_k)$

ができる。

Tao: この業績を主業績の1つとして，2006年 ICM (Madrid) で Fields賞を受賞.

等差数列

4, 7, 10, 13, … のように

$4 \xrightarrow{3} 7 \xrightarrow{3} 10 \xrightarrow{3} 13$

ある数から始めて、同じ数を次々と

たして得られる数列のこと。つまり、

$a,\ a+d,\ a+2d,\ \dots,\ a+(k-1)d,\ \dots$

$a \xrightarrow{d} a+d \xrightarrow{d} a+2d \xrightarrow{d} \cdots \xrightarrow{d}$ k番目

の形の数列。

- a：初項，d：公差 という。
- k個の項からなる等差数列

$$\underbrace{a,\ a+d,\ \dots,\ a+(k-1)d}_{k個}$$

のことを 長さkの等差数列 という。

Green : 1977年2月27日生 (31才)

2006年〜 ケンブリッジ大学
(28才?) Herchel Smith Professor

2005年 Salem賞
2006年 ICM招待講演
2008年 European Math. Soc. Prize

Tao : 1975年 7月17日生 (34才)

1986年 10才: 数学オリンピック 銅
1987年 11才: 〃 〃 銀
1988年 13才: 〃 〃 金
(すべて最年少記録)

1999年: 24才でカルフォルニア大学ロサンゼルス校の正教授
2000年: Salem賞
2003年: Clay Research賞
2006年: Fields賞 (31才)

(170個以上の論文, 979人以上から2344回以上引用)

例 主定理Iが意味をもつのは $k \geqq 3$ のとき.

$k=3$:　3, 5, 7　;　3, 7, 11

　　　2　2　　　　　4　4

(注: 2つ目の例: 5はとばされている。
このように, 途中はとばしてかまわない。)

$k=4$:　5, 11, 17, 23　;　43, 61, 79, 97

　　　6　6　6　　　　　18　18　18

$k=5$:　5, 11, 17, 23, 29

　　　6　6　6　6

ひょっとして簡単?

・5からはじまる長さ $6=5+1$ 以上の等差数列はダメ.
($\because$ 6項目 $= \underline{5} + (\text{公差}) \times \underline{5}$ は 5の倍数)

・同じ理由で, p からはじまる長さ $(p+1)$ 以上の等差数列もダメ.

・<u>帰結</u>
・無限に長い等差数列はない。
・長くするためには, 初項を大きくしていかないといけない。

2009年9月17日現在確認されている
素数列に含まれる等差数列の最長記録：

長さ　：25

初項：$a = 6171054912832631$

（≒6000兆）

公差：$d = 81737658082080$

（≒80兆）

数列：$\underbrace{a,\ a+d,\ a+2d,\ \cdots,\ a+24d}_{25項}$

注）$a-d = 31 \times 571 \times 344009787851$

$a+25d = 17471 \times 470178945961$

この数列はこれ以上伸せない。

```
PrimeQ[6 171 054 912 832 631]

True
366 384 × 223 092 870

True

81 737 658 082 080

PrimeQ[6 171 054 912 832 631]

True

PrimeQ[6 171 054 912 832 631 + 81 737 658 082 080]

True

PrimeQ[6 171 054 912 832 631 + 81 737 658 082 080 * 2]

True

81 737 658 082 080 * 2

163 475 316 164 160

PrimeQ[6 171 054 912 832 631 + 81 737 658 082 080 * 3]

True

PrimeQ[6 171 054 912 832 631 + 81 737 658 082 080 * 4]

True

PrimeQ[6 171 054 912 832 631 + 81 737 658 082 080 * 5]

True

PrimeQ[6 171 054 912 832 631 + 81 737 658 082 080 * 6]

True

PrimeQ[6 171 054 912 832 631 + 81 737 658 082 080 * 7]

True

PrimeQ[6 171 054 912 832 631 + 81 737 658 082 080 * 8]

True

PrimeQ[6 171 054 912 832 631 + 81 737 658 082 080 * 9]

True

PrimeQ[6 171 054 912 832 631 + 81 737 658 082 080 * 10]

True

PrimeQ[6 171 054 912 832 631 + 81 737 658 082 080 * 11]

True

PrimeQ[6 171 054 912 832 631 + 81 737 658 082 080 * 12]

True

PrimeQ[6 171 054 912 832 631 + 81 737 658 082 080 * 13]

True
```

```
PrimeQ[6171054912832631 + 81737658082080 * 14]
True
PrimeQ[6171054912832631 + 81737658082080 * 15]
True
PrimeQ[6171054912832631 + 81737658082080 * 16]
True
PrimeQ[6171054912832631 + 81737658082080 * 17]
True
PrimeQ[6171054912832631 + 81737658082080 * 18]
True
PrimeQ[6171054912832631 + 81737658082080 * 19]
True
PrimeQ[6171054912832631 + 81737658082080 * 20]
True
PrimeQ[6171054912832631 + 81737658082080 * 21]
True
PrimeQ[6171054912832631 + 81737658082080 * 22]
True
PrimeQ[6171054912832631 + 81737658082080 * 23]
True
PrimeQ[6171054912832631 + 81737658082080 * 24]
True
PrimeQ[6171054912832631 + 81737658082080 * 25]
False
FactorInteger[6171054912832631 + 81737658082080 * 25]
{{17471, 1}, {470178945961, 1}}
PrimeQ[6171054912832631 - 81737658082080]
False
FactorInteger[6171054912832631 - 81737658082080]
{{31, 1}, {571, 1}, {344009787851, 1}}
```

Green-Taoが定理を見つけた当時
(2004年頃)

Green-Taoの論文によると:

最長記録 23

初項 = 56211383760397 (≒56兆)
公差 = 44546738095860 (≒4兆)

"何故定理が正しいと確信できたのか?"

I) Heuristic ("発見的方法")

II) 他の有名な予想からの帰結

III) 既知の定理とその拡張可能性

(I) Heuristic

$k \geqq 3$ 固定　　N：(kに対し) 非常に大きな整数

↑長さ　　(6000兆をはるかに越える.)

$\left(\begin{array}{l}\text{N以下の自然数 } k \text{ 項からなる} \\ \text{等差数列 } \underbrace{a_1, a_2, \cdots, a_k}_{k\text{コ}} \text{ の個数}\end{array}\right)$ ― ㊀

$$a_k = a_1 + (k-1)d \leqq N$$

$$\therefore d \leqq \left[\frac{N-a_1}{k-1}\right]$$

$$= \sum_{a_1=1}^{N} \left[\frac{N-a_1}{k-1}\right]$$

$$\geqq \sum_{a_1=1}^{N} \left(\frac{N-a_1}{k-1} - 1\right) = \frac{N(N-1)}{2(k-1)} - N \geqq \frac{N^2}{3(k-1)}$$

素数定理：N以下の自然数 a を"無作為"に選んだとき，a が素数である"確率"

$$\fallingdotseq \frac{1}{\log N}$$

∴もし，素数が"十分に一様に分布"していれば"

$$\left(\begin{array}{l}\text{㊀のうち，全項が} \\ \text{素数である数列の個数}\end{array}\right) \geqq \frac{N^2}{3(k-1)} \cdot \frac{1}{(\log N)^k} > 0 \;!!$$

問題点：素数の分布は"一様"からはほど遠い

$$\begin{cases} 1, 3, 5, 7, 9, 11, \cdots & \text{無数の素数がある} \\ 2, 4, 6, 8, 10, 12, \cdots & \text{2だけ素数} \end{cases}$$

より一般に：

$$\left.\begin{array}{l} 1,\ 1+d,\ 1+2d,\ \cdots \\ 2,\ 2+d,\ 2+2d,\ \cdots \\ \qquad\vdots \\ (d-1),\ (d-1)+d,\ (d-1)+2d,\ \cdots \\ d,\ 2d,\ 3d,\ \cdots \end{array}\right\}$$

dで割った余りでd個のグループに分ける.

- 初項とdの最大公約数$\geqq 2$のグループ：素数はあっても初項だけ
- 初項とdの最大公約数$=1$のグループ：素数は無限個ある。(Dirichletの定理)

問（既知） 次を示せ。

与えられた正の整数 k に対して，

$$\underbrace{a+1,\ a+2,\ \ldots,\ a+(k-1),\ a+k}_{k\text{個の続いた自然数}}$$

がすべて合成数（＝素数でない2以上の整数）になってしまう自然数 a が必ず存在する。

（例えば，$k=6000$兆でもよい。）

cf. 今年度の阪大(情報)大学院の英語の入試問題

(II) 他の有名な予想からの帰結

予想(Erdős-Turán, 1936年) 未解決

$\displaystyle\sum_{n=1}^{\infty} \frac{1}{a_n} = \infty$ である正の整数からなる数列

$0 < a_1 < a_2 < \cdots < a_n < \cdots$

には，いくらでも長い有限等差数列が含まれる。

例

$\sum \frac{1}{n} = \infty$: $1, 2, 3, \cdots, n, \cdots$　いくらでも長い等差数列あり

$\sum \frac{1}{n^2} < \infty$: $1, 2^2, 3^2, \cdots, n^2, \cdots$　長さ3以上の等差数列はない。

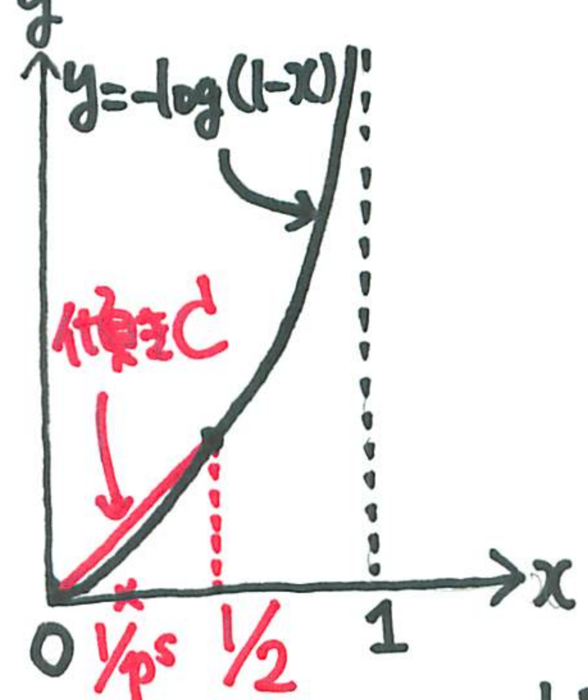
Erdős-Turán予想 ⇒ Green-Taoの定理I

∵ 命題 $\displaystyle\sum_{p:\text{素数}} \frac{1}{p} = \infty$

もし≠∞ ⇒ $\displaystyle\sum_{p:素数} \frac{1}{p} \leqq B$ (頭打ち)

$$\sum_{n=1}^{\infty} \frac{1}{n^s} = \frac{1}{\displaystyle\prod_{p:素数}\left(1-\frac{1}{p^s}\right)}$$ (s>1) Eulerの等式

$$\log\left(\sum_{n=1}^{\infty}\frac{1}{n^s}\right) = -\log\left(\prod_{p}\left(1-\frac{1}{p^s}\right)\right)$$



$$= \sum_{p} -\log\left(1-\frac{1}{p^s}\right)$$

$$\leqq \sum_{p} d\cdot\frac{1}{p^s}$$

$$\leqq \sum_{p} d\cdot\frac{1}{p} \leqq d\cdot B$$

$$\therefore \sum_{n=1}^{\infty}\frac{1}{n^s} \leqq e^{d\cdot B}$$

$$\therefore \sum_{n=1}^{N}\frac{1}{n^s} \leqq e^{\overbrace{d\cdot B}^{N,\,sによらない}}$$

← 任意 (N)

← s>1で任意 (s)

s→1+0 $\displaystyle\sum_{n=1}^{N}\frac{1}{n} \leqq e^{d\cdot B}$

N→∞ $\displaystyle\infty = \sum_{n=1}^{\infty}\frac{1}{n} \leqq e^{d\cdot B}$ 矛盾!!

予想（Hardy-Littleword, 1920年代）未解決

$a_i x + b_i$ $(i=1,2,\cdots,k)$ を $a_i>0$ である

k個の整数係数の1次式とする。

$$F(x) = \prod_{i=1}^{k} (a_i x + b_i)$$ 全部の積（k次式）

が，次の条件㊟ をみたすならば，

$$a_1 n + b_1, \underbrace{a_2 n + b_2, \cdots, a_k}_{k\text{コ}} n + b_k$$

が すべて素数になる ような自然数n

が無限個ある。

条件㊟　各素数pに対して，

$F(m)$ が pでわりきれないような

整数m が必ずある。

（各素数pに対して，$F(x)$は $\mathbb{Z}/p$上

$\mathbb{Z}/p$値関数として 0ではない。）

Hardy-Littlewood予想が正しかったとする：

$F(x) = x\cdot(x+2)$　　2つの1次式の積

$p \geqq 5$ 又は $p=2$：　$F(1)=3$ は p でわれない。
$p=3$　　　　　：　$F(2)=8$ は 3 でわれない。

条件㊟ をみたす。

帰結　$n, n+2$ がともに素数になる n は無限個。
⇒ 双子素数予想の解決が従う.

$F(x) = (x+1)(2x+1)\cdots(kx+1)$

$F(0)=1$ は どの素数 p でもわれない。

条件㊟ をみたす。

帰結　$\underbrace{n+1, 2n+1, \cdots, kn+1}_{\text{公差}\, n,\ \text{長さ}\, k\, \text{の等差数列}}$
がすべて素数である n が無限個。
⇒ Green-Taoの定理Ⅰが従う.

III) 既知の定理とその拡張可能性

Green-Taoの定理

(1) 素数を考える。
(2) 与えられた集合に等差数列を見い出す。

(2)：Van der Waerdenの定理を源とする一連の流れ

定理(Van der Waerden，1927年)

1からNまでのN個の自然数を
m色で色分けすることを考える。このとき：
与えられた自然数$m \geqq 1$，$k \geqq 3$に対し，
mとkで決まる自然数$N(m,k)$があり，
次をみたす：
$N \geqq N(m,k)$ならば，
同じ色からなる長さkの等差数列が
(N^m通りあるどの色付けにおいても)
必ず存在する。

問(既知)

自然数 $k \geqq 3$ と, $0 < a < a+\delta < 1$ である

実数 a, δ を固定して考える。

$A = \{-N \leqq n \leqq N \mid a < \{\sqrt{2}n\} < a+\delta\}$

$B = \{-N \leqq n \leqq N \mid a < \{1.41 \times n\} < a+\delta\}$

(ただし, $\{x\} = x - (x$ の整数部分$) = (x$ の小数部分$)$.)

(1) N を十分大きくとれば, A は長さ k の

等差数列を含むことを示せ。

(2) B についてはどうか?

(ヒント) Dirichlet の部屋割り論法:

任意の実数 α と任意の自然数 m に対し

$|\alpha x - y| < \frac{1}{m}$, $0 < x \leqq m$

である整数 x, y が必ずみつかる。

例　$k \geq 3$ 固定

N : kに比べ非常に大きな自然数

$1 \sim N$ ＜ 素数 : 緑 / それ以外 : 赤　2色で色付け

・Van der Waerden の定理

⇒ 赤, 緑の少くとも一方には
長さ k の等差数列がある。

・赤には

$4, 6, 8, \cdots, 2 \cdot \left[\frac{N}{2}\right]$

という長さ k をはるかに越える
等差数列がある。

帰結　残念ながら, 緑(素数)の方
については, まだ何とも言えない。

定理の弱点：どの色の中に等差数列が
見つかるか教えてくれない。

Erdős-Turán：
Van der Waerdenの定理を強化する形
の予想を提唱（1936年）
→ Szemerédiが最初に解決.

記号

$[N] = \{1, 2, 3, \cdots, N\}$

$[N]$の部分集合Aに対し

$|A| =$（Aに属する自然数の個数）

$\dfrac{|A|}{N} =$（Aの密度）

定理(Szemerédi, 1975年)

$0<\delta<1$ 任意に選んで固定(最初に与える)。
密度 $\geqq \delta$ である $[N]$ の部分集合について考える。
このとき, δ 及び与えられた自然数 $k \geqq 3$ に応じて定まる自然数 $N(k,\delta)$ があって, 次が成りたつ:

$N \geqq N(k,\delta)$ ならば, 密度 $\geqq \delta$ である $[N]$ の部分集合には, 長さ k の等差数列が必ず含まれる。

- Van der Waerden の定理よりよくなっている点: どの部分集合に含まれるかについて, よりくわしい情報を与えている点。

<u>例</u> A, B がともに $[N]$ の密度 $\geqq \delta$ の部分集合なら, A にも B にも長さ k の等差数列がみつかることになる。

1) Van der Waerden の定理の一般化

☺ $[N]$ を m 色で色分けするとき，
ある色からなる部分集合の密度 $\geq \frac{1}{m}$.
∴ 定理を $\delta = \frac{1}{m}$ と k に用いればよい。

2) Green-Tao の主定理Ⅰを"直接"
導くためにはまだ不十分

☺ $A = \{N$ 以下の素数$\} \subseteq [N]$
N についてのより詳しい情報なしに
いつでも $\frac{|A|}{N} \geq \delta$ である正の数 δ
は見つかるか？

$$\frac{|A|}{N} = \frac{\pi(N)}{N} = \frac{\pi(N)}{\frac{N}{\log N}} \cdot \frac{1}{\log N} \xrightarrow[\text{素数定理}]{N\to\infty} 1 \cdot 0 = 0$$

なので残念ながら見い出せない。

（あと２ステップの拡張が必要.）

Szemerédiの定理

分野を越えた多くの数学者に刺激を与えた。

- Furstenberg : エルゴード理論
- Gower : 関数解析, 組合せ論
(1998年ICMでFields賞)

- 集合と部分集合のみではなく,
その上の関数と期待値も考える。
  - 三則演算(±, ・)ができる。(環)
  - 全体はベクトル空間をなす。
  (性質に応じた近さを測るノルム
  が考察できる。)

⇒ 使える手法が格段に増す。
拡張の自由度も増す。

- Tao : Szemerédiの定理の異なる定式化
と別証明

記号

N：十分大きな素数

$[N] = \{1, 2, 3, \cdots, N-1, \overset{\overset{0}{\shortparallel}}{N}\}$

$= \mathbb{Z}_N$（Nでわった余りの集合，四則演算ができる）

同一視

$f(x)$：$[N] = \mathbb{Z}_N$ 上の実数値関数

期待値

・$\mathbb{E}(f(x) \mid x \in \mathbb{Z}_N) = \frac{1}{N} \sum_{x \in \mathbb{Z}_N} f(x)$

$f(x)$の値の期待値（平均値）

全部で N^2コ

・$\mathbb{E}(\underbrace{f(x) f(x+r) \cdots f(x+(k-1)r)}_{k\text{コの積}} \mid x \in \mathbb{Z}_N, r \in \mathbb{Z}_N)$

$= \frac{1}{N^2} \sum_{\substack{x \in \mathbb{Z}_N \\ r \in \mathbb{Z}_N}} f(x) f(x+r) \cdots f(x+(k-1)r)$

長さkの"等差数列" $x, x+r, \cdots, x+(k-1)r$

上の値の積の期待値（平均値）

注) 期待値と等差数列

問 次を示せ。

(既知)

$$\left|\mathbb{E}\left(f(x) \mid x \in \mathbb{Z}_N\right)\right|^2$$

$$= \mathbb{E}\left(f(x) f(x+r) \,\middle|\, \begin{array}{l} x \in \mathbb{Z}_N \\ r \in \mathbb{Z}_N \end{array}\right)$$

定理($\cdots$, Tao ; Szemerédiの定理の変形版)

実数 $0<\delta<1$ と自然数 $k\geqq 3$ を固定する。

$[N]=\mathbb{Z}_N$ 上

$$\begin{cases} (1)\ \text{すべての}\ x\ \text{に対し}\ 0\leqq f(x)\leqq 1 = \nu_{\mathrm{const}}(x) \\ (2)\ \mathbb{E}(f(x) \mid x\in\mathbb{Z}_N) > \delta \end{cases}$$

の2つをみたす関数 $f(x)$ について考える。

このとき，δ と k に依存してきまる

整数 $N(\delta, k)$ と正の数 $C(k,\delta)>0$

があり，次をみたす:

N が $N(\delta, k)$ 以上の素数ならば，

(1), (2) をみたすどの関数 $f(x)$ に対しても

$$\mathbb{E}\left(f(x)f(x+r)\cdots f(x+(k-1)r) \,\middle|\, \begin{matrix} x\in\mathbb{Z}_N \\ r\in\mathbb{Z}_N \end{matrix}\right) > C(k,\delta).$$

変形版 ⇒ 原型（Szemerédiの定理）

（概略）　$A \subseteq [N]$，（密度）$> \delta$ とする。

$$f(x) = \begin{cases} 1 & (x \in A \text{のとき}) \\ 0 & (x \notin A \text{のとき}) \end{cases}$$ とおくと

$\mathbb{E}(f(x) \mid x \in \mathbb{Z}_N) = (A\text{の密度})$

∴ (1), (2) が成立.

故に，素数 N を十分大きくとれば，

$$\mathbb{E}\left(f(x)f(x+r)\cdots f(x+(k-1)r) \,\middle|\, \begin{matrix} x \in \mathbb{Z}_N \\ r \in \mathbb{Z}_N \end{matrix}\right) > c(k,\delta).$$

（変形版の帰結）

∴ $f(x)f(x+r)\cdots f(x+(k-1)r) > 0$

である $x, x+r, \ldots, x+(k-1)r$ ―㊍

の組が $c(k,\delta)N^2$ コ以上ある

㊍の各項 $\in A$　（∵ $f(x), \ldots, f(x+(k-1)r) > 0$）

こうして㊍は A に含まれる長さ k の

"等差数列".

注1)

㊍の中で $r=0$ の列：N 個

無視できる。

注2)

・N を素数に限定している点

・(+は余りの世界 $\mathbb{Z}_N$ で考えているため)
$2+(N-1)=1$ のように，㊍の中には
途中で巡回してしまう列がある点

この2点：変型版を $\delta=\delta/2k$ と k

に適用し，

定理(Bertrandの公準，Chebychevの定理)
自然数 N に対し，$kN < N' < 2kN$
である素数 N' がある。

を用いることで同時に克服できる。

- 先と全く同じ理由(素数定理)により,

$A = \{N\text{以下の素数}\} \subseteq [N]$

に"直接"適用 $\left(f(x) = \begin{cases} a(x) & x \in A \\ 0 & x \notin A \end{cases} \text{に適用} \right)$

するにはやはり不十分.

- Green-Tao が至った最後の拡張:

変型版(1)における $1 = \nu_{const}(x)$ を

(期待値)≒1 である非負関数に

おきかえる。

例

・ $1 = \nu_{const}(x)$

$\mathbb{E}(1 \mid x \in \mathbb{Z}_N) = 1$　期待値1

・ von Mangoldt 関数

$$\Lambda(x) = \begin{cases} \log p & (x = p^m : \text{素数べきのとき}) \\ 0 & (\text{それ以外}) \end{cases}$$

$\boxed{\text{性質}}$ $\mathbb{E}(\Lambda(x) \mid x \in \mathbb{Z}_N)$

$$= \frac{\sum_{x \in \mathbb{Z}_N} \Lambda(x)}{N} \xrightarrow{N \to \infty} 1$$

このように、素数を反映した関数も使える可能性がでてくる。

問（既知）素数定理を用いて $\boxed{\text{性質}}$ を示せ。

§4. Green-Taoの Szemerédi 型定理

定義 $\nu(x)=\nu_N(x)$: $\mathbb{Z}_N=[N]$ 上の非負関数
(十分大きい素数 N 全部に対して与える。)
$\nu(x)$ が $\mathbb{Z}_N$ 上の測度
$\Leftrightarrow \mathbb{E}(\nu(x) \mid x\in\mathbb{Z}_N) \xrightarrow[N\to\infty]{} 1.$

主定理II (Green-Taoの Szemerédi 型定理)
実数 $0<\delta<1$ と自然数 $k\geqq 3$ を固定する。
$\nu(x)=\nu_N(x)$ を $\mathbb{Z}_N$ 上の k-準乱雑測度とする。

このとき,

$$\begin{cases} (1)\ \text{すべての } x\in\mathbb{Z}_N \text{ に対し, } 0\leqq f(x)\leqq \underbrace{\nu(x)}_{\text{ここが一般化されているところ}} \\ (2)\ \mathbb{E}(f(x) \mid x\in\mathbb{Z}_N)>\delta \end{cases}$$

をみたす $\mathbb{Z}_N$ 上のどの関数 $f(x)$ に対しても

$$\mathbb{E}\left(f(x)f(x+r)\cdots f(x+(k-1)r) \,\middle|\, \begin{matrix} x\in\mathbb{Z}_N \\ r\in\mathbb{Z}_N \end{matrix}\right)$$

$$> \underbrace{C(k,\delta)}_{\substack{\text{正の実数} \\ \text{(変型版と同じ)}}} - \underbrace{\varepsilon(k,\delta,N)}_{\substack{N\to\infty\text{で}0\text{に収束} \\ (\nu(x),\ f(x)\text{によらない})}}$$

が成りたつ。

- k-準乱雑な測度(族) $\nu(x)=\nu_N(x)$
  - 変数のアフィン変換に関し
    十分に一様なふるまいをする測度
  - 正確には，2つの条件

$$\begin{cases} (k\cdot 2^{k-1}, 3k-4, k) & \text{- 線形条件} \\ 2^{k-1} & \text{- 相関条件} \end{cases}$$

をみたす測度族.

- Green-Taoは主定理IIを証明
  (ここまでは主定理Iとは完全に独立)
  した後，
  主定理IIを主定理Iに応用する
  ことを考えた。

◎ $(\underbrace{k\cdot 2^{k-1}}_{\text{1次式}},\ \underbrace{3k-4}_{\text{変数}},\ \underbrace{k}_{\text{値}})$ − 線形条件

- $m \leqq k\cdot 2^{k-1}$, $t \leqq 3k-4$ をみたすすべての自然数 m, t
- $$(L_{ij}) = \underbrace{\begin{pmatrix} \boxed{\qquad\qquad} \\ \boxed{\qquad\qquad} \\ \vdots \\ \boxed{\qquad\qquad} \end{pmatrix}}_{t\text{列}} \left.\vphantom{\begin{pmatrix} a \\ a \\ \vdots \\ a \end{pmatrix}}\right\} m\text{行}$$
  - すべての成分は $|\text{分子}|$, $|\text{分母}| \leqq k$ である有理数
  - どの2行も平行でない

  をみたすすべての $m\times t$ 行列
- すべての $b_1, b_2, \cdots, b_m \in \mathbb{Z}_N$

に対し, $\psi_i(\mathbf{x}) = \sum_{j=1}^{t} L_{ij}x_j + b_i \quad (i=1,2,\cdots,m)$

とおくとき

$$\underbrace{\mathbb{E}\left(\nu(\psi_1(\mathbf{x}))\nu(\psi_2(\mathbf{x}))\cdots\nu(\psi_m(\mathbf{x})) \mid \mathbf{x}\in\mathbb{Z}_N^t\right)}_{N^t\text{個の値の平均値}} \xrightarrow{N\to\infty} 1$$

◎ $\underbrace{2^{k-1}}_{\text{1次式}}$ − 相関条件

N, m, q に依存しない

$m \leqq 2^{k-1}$ をみたすすべての自然数 m に対し,

すべての自然数 q に対して $\mathbb{E}((\tau_m(x))^q \mid x\in\mathbb{Z}_N) < B$

をみたす $\mathbb{Z}_N$ 上の非負関数 $\tau_m(x)$ $(m=1,2,\cdots,2^{k-1})$

があって, すべての $h_1, h_2, \cdots, h_m \in \mathbb{Z}_N$ に対し,

$$\mathbb{E}(\nu(x+h_1)\nu(x+h_2)\cdots\nu(x+h_m) \mid x\in\mathbb{Z}_N)$$

$$\leqq \sum_{1\leqq i<j\leqq m} \tau_m(h_i-h_j)$$ が成りたつ。

主定理IIを主定理Iに応用するには，
（安直に考えると）：

主定理IIの条件(1),(2)をみたす

※ (a) $\mathbb{Z}_N$上のk-準乱雑測度 $\nu(x)=\nu_N(x)$

(b) $\mathbb{Z}_N=[N]$に属する素数以外では値が0である$\mathbb{Z}_N$上の関数$f(x)=f_N(x)$

を十分大きなすべての素数Nについて作ればよい。（再び素数の問題）

先と同じ考え方で，主定理IIから，

$f(x)f(x+r)\cdots f(x+(k-1)r)>0$ — ①

であるk項からなる本当の等差数列

$x, x+r, \ldots, x+(k-1)r$ $(\in[N])$

が“N^2個のオーダー”であることになる。

$f(x)$は素数においてのみ$\neq 0$なので

$x, x+r, \ldots, x+(k-1)r$は，①より

すべて素数．主定理I.

Green-Tao：

㊋(b)を絶妙に修正した形の条件

をみたす組 $(\nu_N(x), f_N(x))$ を作った。

__構成法__ W-技巧

N：非常に大きな素数 （$N \fallingdotseq 6000$兆）

$\downarrow$

$w = w(N) = \log(\log N)$ （$w(N) \fallingdotseq 3.5$）

非常にゆっくり∞に増大.

$$W = W(N) = \prod_{p < w(N)} p$$

修正されたvon Mangoldt関数

$$\tilde{\Lambda}_N(n) = \begin{cases} \dfrac{\phi(W)}{W} \log(Wn+1) & \text{（}Wn+1\text{が素数のとき）} \\ 0 & \text{（それ以外）} \end{cases}$$

__性質__

$$\frac{\sum_{n=1}^{N} \tilde{\Lambda}_N(n)}{N} \xrightarrow{N \to \infty} 1$$

測度の条件をみたす。

（∵ Dirichletの定理の素数定理型版）

主補題（Green-Tao）

自然数 $k \geqq 3$ を固定

$$\varepsilon_k = \frac{1}{2^k \cdot (k+4)!}$$

（Nによらない
分母は大きいが
Nにくらべて微小）

N：（kにくらべ）非常に大きな素数

このとき，

$$\varepsilon_k N \leqq n \leqq 2\varepsilon_k N$$

をみたすすべての整数 n に対し，

$$\nu_N(n) \geqq \frac{1}{k \cdot 2^{k+5}} \widetilde{\Lambda}_N(n)$$

である $\mathbb{Z}_N$ の k-準乱雑測度

$\nu(x) = \nu_N(x)$ がある。

・主定理Ⅰへの応用に必要な素数の性質はすべてこの主補題に内包されている．

主補題＋主定理II ⇒ 主定理I

主補題の $\nu_N(x)$ と $[N]=\mathbb{Z}_N$ 上の関数

$$f_N(x) = \begin{cases} \dfrac{1}{k\cdot 2^{k+5}}\tilde{\Lambda}_N(x) & \left(\varepsilon_k N \leqq x \leqq 2\varepsilon_k N \text{ のとき}\right) \\ 0 & (\text{それ以外}) \end{cases}$$

について考える。

- $0 \leqq f_N(x) \leqq \nu_N(x)$
- $f_N(x)$ は $\underline{\varepsilon_k N \leqq x \leqq 2\varepsilon_k N}$ かつ $\underline{Wx+1 \text{ が素数}}$ のときのみ $\neq 0$

$$\mathbb{E}(f_N(x) \mid x \in \mathbb{Z}_N)$$

$$= \frac{1}{k\cdot 2^{k+5}\cdot N} \sum_{\varepsilon_k N \leqq x \leqq 2\varepsilon_k N} \tilde{\Lambda}_N(x)$$

$$\underset{\text{性質}}{=} \frac{1}{k\cdot 2^{k+5}\cdot N} (2\varepsilon_k N - \varepsilon_k N)(1+\overbrace{o(1)}^{N\to\infty \text{ で } 0 \text{ に収束}})$$

$$> \varepsilon_k / k\cdot 2^{k+6} > 0$$

N: 十分大

($N, \nu_N(x), f_N(x)$ によらない)

$\therefore \delta = \varepsilon_k / k\cdot 2^{k+6}$ に対し、主定理IIの要請がみたされる。

従って，主定理IIにより，

十分大きな素数 N に対し

$$\mathbb{E}\left(f_N(x)f_N(x+r)\cdots f_N(x+(k-1)r)\,\middle|\,\begin{matrix}x\in\mathbb{Z}_N\\ r\in\mathbb{Z}_N\end{matrix}\right)>\frac{C(k,\delta)}{2}$$

左辺への $r=0$ の項の寄与：

高々 $(\log N)^k \cdot N/N^2 = \dfrac{(\log N)^k}{N} \xrightarrow[N\to\infty]{} 0$ のオーダー

$\therefore f_N(x)f_N(x+r)\cdots f_N(x+(k-1)r)>0$ —(*)

である本当の等差数列（k項）

$x,\ x+r,\ \cdots,\ x+(k-1)r \in [N]$ —(**)

が $N^2/(\log N)^k$ のオーダーである。

$f_N(x)$ の定義より

$f_N(x)\neq 0 \Rightarrow Wx+1$ は素数

$\therefore$ 数列(**)に対し，(*)により

$Wx+1,\ W(x+r)+1,\ \cdots,\ W(x+(k-1)r)+1$

は k個の素数からなる（公差 Wr の）等差数列!!

$\therefore$ 主定理I

主補題における $\nu_N(x)$ の構成

$$\Lambda_R(n) = \sum_{\substack{d \mid n \\ d \leq R}} \mu(d) \log(n/d)$$

ただし, $R = \sqrt[k\cdot 2^{k+4}]{N}$

$$\mu(d) = \begin{cases} 1 & (d=1) \\ 0 & (d:\text{平方因子をもつ}) \\ (-1)^r & \left(\begin{array}{l} d:\text{それ以外},\ r\text{は} \\ d\text{の素因数の個数} \end{array}\right) \end{cases}$$

(メビウス関数)

$$\nu_N(n) = \begin{cases} \dfrac{\phi(W)}{W} \dfrac{\{\Lambda_R(Wn+1)\}^2}{\log R} & \left(\begin{array}{l} \varepsilon_k N \leq n \leq 2\varepsilon_k N \\ \text{のとき} \end{array}\right) \\ 1 & (\text{それ以外}) \end{cases}$$

と定める。この $\nu_N(x)$ は主補題の条件をみたす。

確かめるべきこと

① $\nu_N(n) \geqq \dfrac{\widehat{\Lambda}_N(n)}{k\cdot 2^{k+5}}$ ：容易

② $\nu_N(x)$ は測度

③ $\nu_N(x)$ は k-準乱雑

Goldston-Yildirim の結果

($\Lambda_R(W\psi_i+1)$ の期待値に関する結果)

文献

平成 21 年 9 月 21 日

1 前半の内容に関する文献

1. 河田敬義: "数論 I, II, III", 岩波講座　基礎数学. (全般に対して. 後半に述べる Chebychev の定理の証明もある.)

2. 杉浦光夫: "解析入門 I", 東大出版会 (391–393 ページに, Euler の積公式の厳密な証明がある.)

3. L. J. Goldstein: "A history of the prime number theorem", American Math. Monthly **80** (1973) 599–615.Amer. Math. Monthly 104 (1997), no. 8, 705–708. (素数定理に向けた試みを書いた Gauss の手紙の英訳がある.)

4. D. Zagier: "Newman's short proof of the prime number theorem - dedicated to the Prime Number Theorem on the occasion of the 100th birthday", American Math. Monthly **104** (1997) 705–708. (素数定理の短く明快な証明. 大学 2 年生程度の人には予備知識 0 で読める.)

5. I. Soprounov: "A short proof of the prime number theorem for arithmetic progressions", (Dirichlet の定理の素数定理版の [4] にそった短い証明.)

6. F. Saidak, "A. New Proof of Euclid's Theorem", American Math. Monthly **113** (2006) 937–938. (素数が無限個あることに対する新証明.)

2 後半の内容に関する文献

1. , B. Green, T. Tao: "The primes contain arbitrarily long arithmetic progressions", Annals of mathematics **167** (2008) 481–547. (ArXiv:math/0404188) (主定理 I, II.)

2. T. Tao: "A quantitative ergodic theory proof of Szemerédi's theorem", The electronic Journal of Combinatorics **13** (2006), Research paper 99, 49 pages, (arXiv:math/0405251) (Szemerédi の定理に対する新しい証明.)

3. T. Tao: "What is good mathematics?", Bulletin of the American Mathermatical Society **44** (2007) 623–634. (arXiv:math/0702396) (Essey: Tao の数学観が断定的な形ではなく綴られている. Szemerédi の定理の発見や拡張の歴史も経験とともに語られている.)

4. B. Kra: "The Green-Tao theorem on arithmetic progressions in the primes: an ergodic point of view", Bulletin of the American Mathermatical Society 43 (2006) 3–23. (survey: Frusteinberg や Gower の仕事との関係もわかりやすく解説されている.)

5. I.D. Shkredov: "Szemerédi's theorem and problems on arithmetic progressions", Russian Math. Surveys 61 (2006), no. 6, 1101–1166. (survey: Van der Waerden の定理の証明も解説されている.)