高校生のための現代数学講座　　　　　　　　　　　　　　　東京大学
「数論と暗号」　　　　　　　　　　　　　　　　　玉原国際セミナーハウス
講義 (2)　寺杣　友秀　　　　　　　　　　　　　　　2005 年 9 月 10 日

「素数の分布」（メモ）

1. 与えられた素数の有限集合と素になる確率

1. 連続する自然数の集合 $S = \{a+1, a+2, \ldots, b-1, b\}$ からひとつ数 x を選んだときにそれが偶数である確率は $b-a$ が十分大きいと $\frac{1}{2}$ といえる。
2. 同じく 3 で割れる確率は $\frac{1}{3}$ といえる。
3. ベン図を描いてみればわかるように、2 でも 3 でも割り切れない確率は
$$1 - \frac{1}{2} - \frac{1}{3} + \frac{1}{6}$$
となる。重なる部分が 6 の倍数となっていることに注意。
4. 2 でも 3 でも、そして 5 でも割り切れない確率は同様に
$$1 - \frac{1}{2} - \frac{1}{3} - \frac{1}{5} + \frac{1}{2\cdot 3} + \frac{1}{2\cdot 5} + \frac{1}{3\cdot 5} - \frac{1}{2\cdot 3\cdot 5}$$
と計算されるが、これは幸運にも因数分解できてしまう。
$$= (1 - \frac{1}{2})(1 - \frac{1}{3})(1 - \frac{1}{5})$$
5. （作業仮定）ある数 $n+1$ が素数になるためには n 以下の素数と素となることが必要十分なので（もう少し節約して $\sqrt{n}$ 以下の素数で確かめればよいが...）n 以下の素数を $p_1, \ldots, p_m$ とおくと、が素数になる確率は
$$(1 - \frac{1}{p_1})(1 - \frac{1}{p_2})\cdots(1 - \frac{1}{p_m}) \tag{1.1}$$
と考えてよいのではないか。

2. 無限等比級数、素因数分解の一意性

1. 等比級数の和の公式
$$1 + x + x^2 + \cdots x^n = \frac{1 - x^{n+1}}{1 - x}$$
$0 < x < 1$ の時は無限和を考えることができる。つまり上の極限をとる。
$$\sum_{i=0}^{\infty} x^i = 1 + x + x^2 + \cdots = \frac{1}{1 - x}$$

2. 上の x として $0 < \frac{1}{p_1} < 1$ をとれば

$$\frac{1}{1-\frac{1}{p_1}} = 1 + \frac{1}{p_1} + \frac{1}{p_1^2} + \frac{1}{p_1^3} + \cdots = \sum_{i=0}^{\infty} \frac{1}{p_1^n}$$

3. 1 から n までの数はただ一通りに素因数分解され、かつその因数は $\{p_1, \ldots, p_m\}$ の元なので、

$$(\frac{1}{1-\frac{1}{p_1}})(\frac{1}{1-\frac{1}{p_2}})\cdots(\frac{1}{1-\frac{1}{p_m}})$$

の展開には $\frac{1}{1}, \frac{1}{2}, \frac{1}{3}, \ldots, \frac{1}{n}$ が一度づつでてきて、さらに出てくる項はすべて正の数。

4. 従って下の不等式をえる。

$$\frac{1}{1} + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n} \le (\frac{1}{1-\frac{1}{p_1}})(\frac{1}{1-\frac{1}{p_2}})\cdots(\frac{1}{1-\frac{1}{p_m}}) \tag{2.1}$$

この式の右辺と式 (1.1) は逆数になっている。

3. 調和級数と対数

1.

$$1 + \frac{1}{2} + \underbrace{(\frac{1}{3} + \frac{1}{4})}_{\ge 2\times\frac{1}{4}} + \underbrace{(\frac{1}{5} + \frac{1}{6} + \frac{1}{7} + \frac{1}{8})}_{\ge 4\times\frac{1}{8}} \cdots + \underbrace{(\frac{1}{2^k} + \frac{1}{2^k+1} + \cdots + \frac{1}{2^{k+1}})}_{\ge 2^k\times\frac{1}{2^{k+1}}}$$
$$\ge 1 + \frac{k+1}{2}$$

2. 従って

$$\sum_{i=1}^{2^k} \frac{1}{i} \ge 1 + \frac{k}{2}$$

3. 一般に実数 x に対して $x = 2^y$ なる y が定まる。この y のことを x の y を底とする対数という。そして $y = \log_2 x$ とあらわす。このとき任意の自然数 n に対して

$$\sum_{i=1}^{n} \frac{1}{i} \ge 1 + \frac{\log_2 n}{2} \tag{3.1}$$

が成立する。

4. 結論。不等式 (2.1) と不等式 (3.1) より $n+1$ が素数である確率 (1.1) は

$$(1-\frac{1}{p_1})(1-\frac{1}{p_2})\cdots(1-\frac{1}{p_m}) \le \frac{2}{2+\log_2 n}$$

という不等式を満たす。この不等式の右辺は大変ゆっくりではあるが 0 に近づいていくことがわかる。

5. 実は

$$\lim_{X\to\infty} \frac{(\{p : 素数 \mid p < X\} の個数) \cdot \log X}{X} = 1$$

がルジャンドル（とガウス）により予想され、アダマール-ドゥラバレ-プサンにより証明された。ここで $\log$ の底としては自然対数の底

$$e = \lim_{n\to\infty}(1+\frac{1}{n})^n$$

をとる。これは素数の分布がランダムであることを表している定理である。証明には複素関数論（複素数を使った微積分学）が不可欠。

6. さらに良い評価

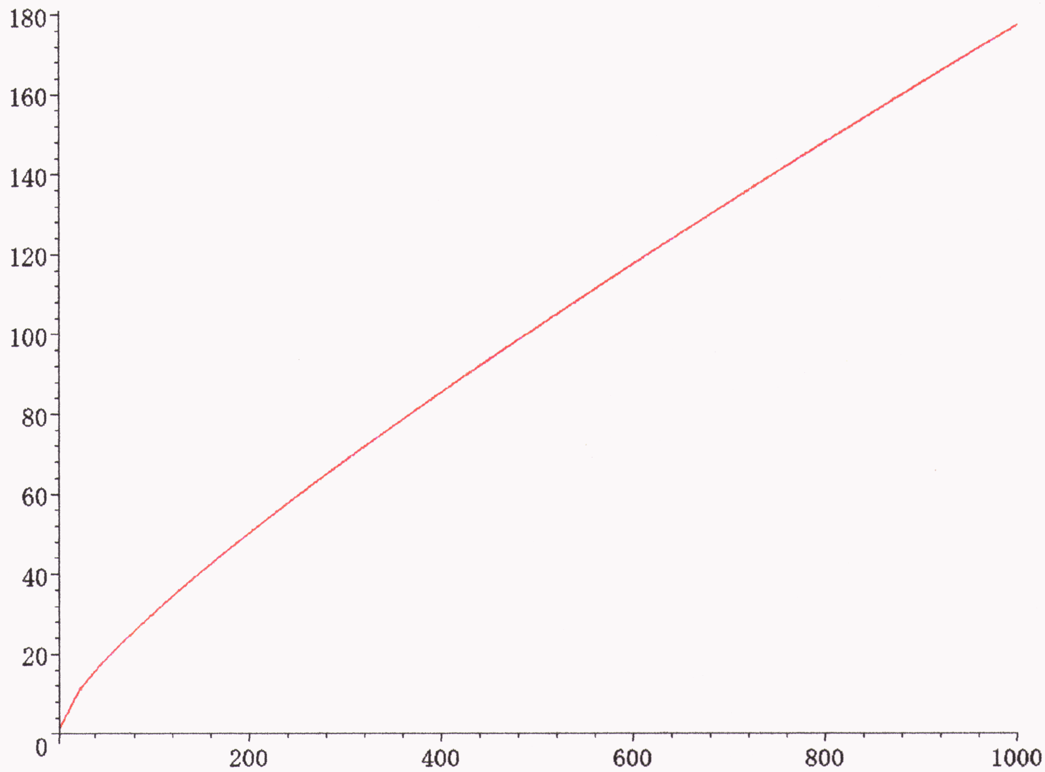
$$\frac{\#\{p : 素数 \mid p < X\} - \int_2^X \frac{dt}{\log(t)}}{\sqrt{X}\log X}$$

が X について有界関数となるという予想があり、ゼータ関数という複素数関数がどこで値が 0 になるかという、有名なリーマン予想と同値。

表. 近似の様子(Wikipediaより引用)

x	$\pi(x)$	$\mathrm{Li}(x)$	$x / \log x$	$\pi(x) / \mathrm{Li}(x)$	$\dfrac{\pi(x)}{x / \log x}$
10	4	5.12...	4.34...	0.78118...	0.92103...
100	25	29.08...	21.71...	0.85966...	1.1513...
1000	168	176.56...	144.76...	0.95149...	1.1605...
10000	1229	1245.09...	1085.73...	0.98708...	1.1320...
100000	9592	9628.76...	8685.89...	0.99618...	1.1043...
1000000	78498	78626.50...	72382.41...	0.99837...	1.0845...
10000000	664579	664917.35...	620420.69...	0.99949...	1.0712...
100000000	5761455	5762208.33...	5428681.02...	0.99987...	1.0613...

```
>
> plot(Li(x),x=2..1000);
```




```
>
```