

素数を調べる

— その多様な姿 —

広島大学大学院理学研究科

数学専攻 高橋浩樹

1. 1 素数の定義

1とそれ自身以外に約数を持たない
1より大きな自然数.

自然数 1, ②, ③, ~~4~~, ⑤, ~~6~~, ⑦, ...
○素数 ×合成数

$$(2の約数) = \{1, 2\} \quad (3の約数) = \{1, 3\}$$

$$(4の約数) = \{1, 2, 4\} \quad (5の約数) = \{1, 5\}$$

$$(6の約数) = \{1, 2, 3, 6\} \quad (7の約数) = \{1, 7\}$$

小さな素数たち

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, ...

定義は簡単であるが、
その多様な性質を解き明かそうとすると
しばしば困難を極める。

ゴールドバッハの予想

(4以上の偶数)=素数+素数.

$4=2+2, 6=3+3, 8=3+5, 10=3+7, 12=5+7, \dots$

代数, 幾何, 解析的手法
が多面的に利用される。

色々な数学に感謝!

表が単純なパターンになる理由

×印の周期を m とする.

1行の文字数 a を m で割った余りを r とすると、
次の行では、×印は **左に r ずれ**、
右に $m-r$ ずれる.

$a=14$, $m=2,3,5,7$ の場合、ずれが小さい.

$a=14$

$m=2$, $14 \div 2 = 7$ 余り $r=0$ ずれない.

$m=3$, $14 \div 3 = 4$ 余り $r=2=m-1$ **右に1ずれる.**

$m=5$, $14 \div 5 = 2$ 余り $r=4=m-1$ **右に1ずれる.**

$m=7$, $14 \div 7 = 2$ 余り $r=0$ ずれない.

ずれが小さいので単純なパターンになる.

1. 3 整数をmで割った余りの集合

$$\mathbb{Z}/m\mathbb{Z}=\{0,1,2,3,\dots,m-2,m-1\}$$

この集合内での足し算, 引き算, 掛け算, 割り算の構造

→ 代数学 群論, 環論, 体論

- mが素数である時と合成数である時の違いを表で探してみよう!
- 1 ~ m-1の全ての数字が現れる行や列は?

1. 4 素数の無限性(ユークリッド)

$p_1, p_2, p_3, \dots, p_{r-1}$: 素数とする.

$p_r = (p_1 p_2 p_3 \dots p_{r-1} + 1)$ の素因数) とすると,

p_r は p_1, p_2, \dots, p_{r-1} とは異なる新たな素数である.

大きな数の素因数分解は難しい.

この難しさが公開鍵暗号の代表である
RSA暗号に用いられている.

1. 5 有名な素数たち

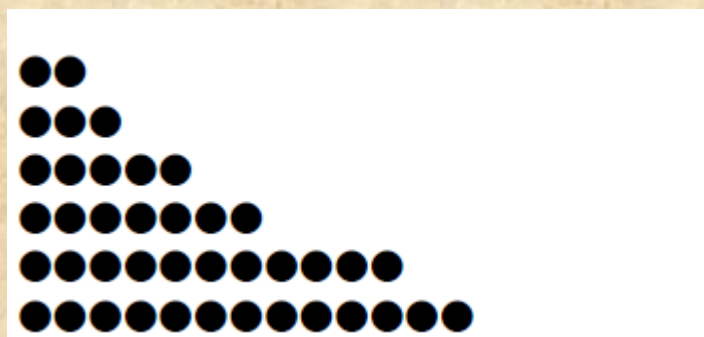
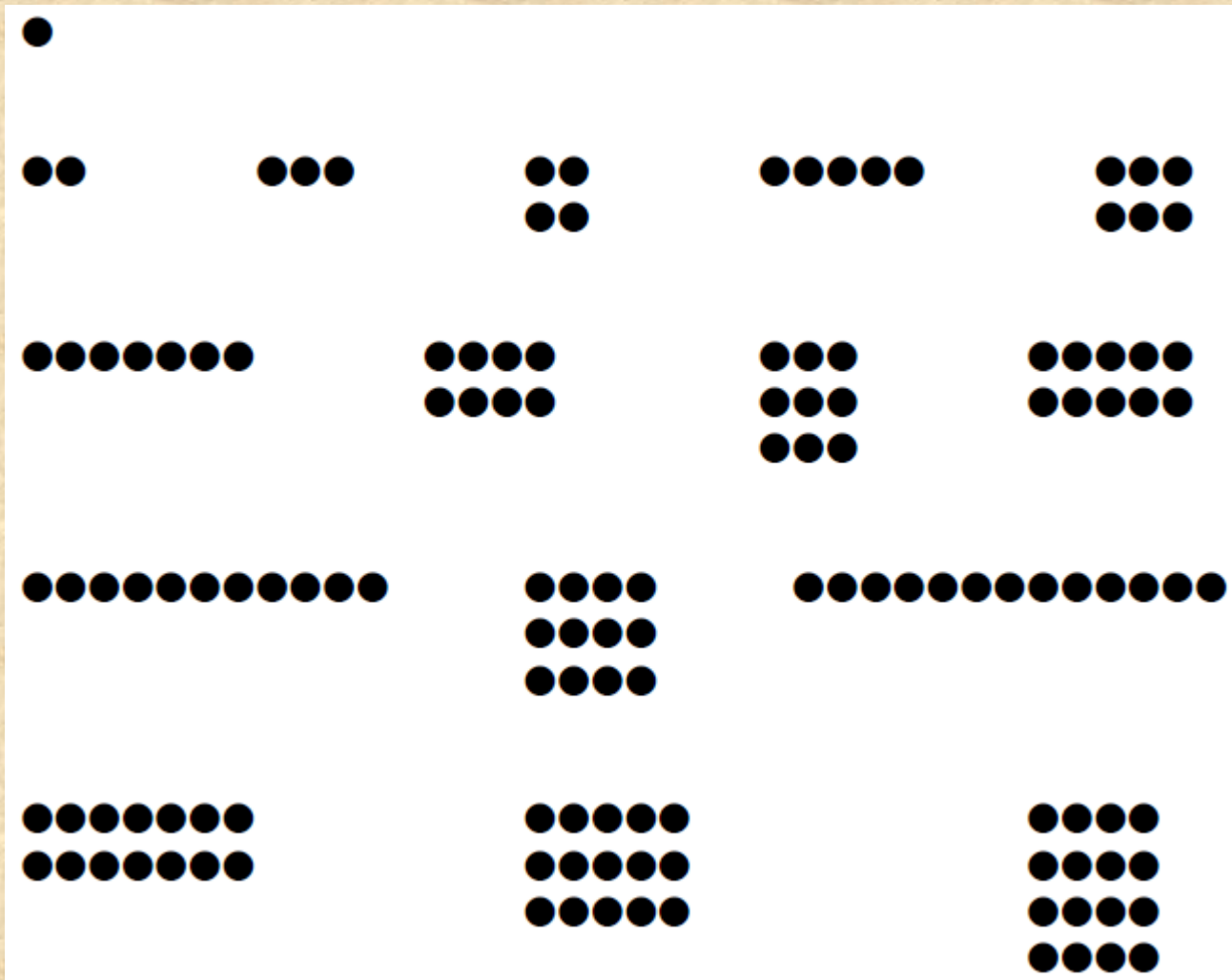
- ・フェルマー素数: $2^m + 1$ 型の素数
 $m = 2^n$ 5個知られている.
正多角形の作図問題(2. 3)
- ・メルセンヌ素数: $2^m - 1$ 型の素数
 $m = p$ 47個知られている.
完全数の構成
 $M_{43112609}$ は約1300万桁の素数!
・・・巨大素数探し: GIMPS
- ・双子素数, 三つ子素数, ...

2.1 素数の表現

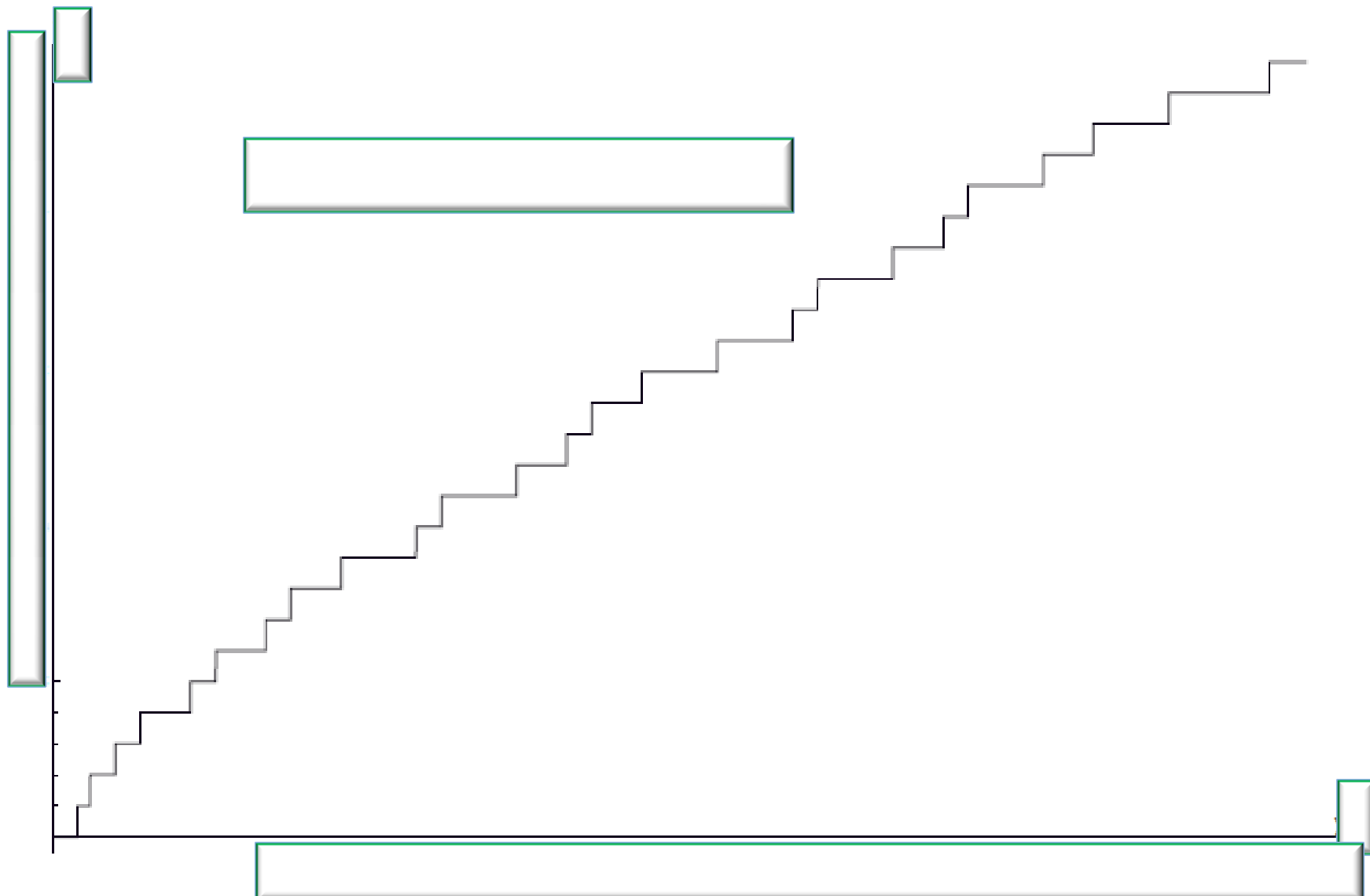


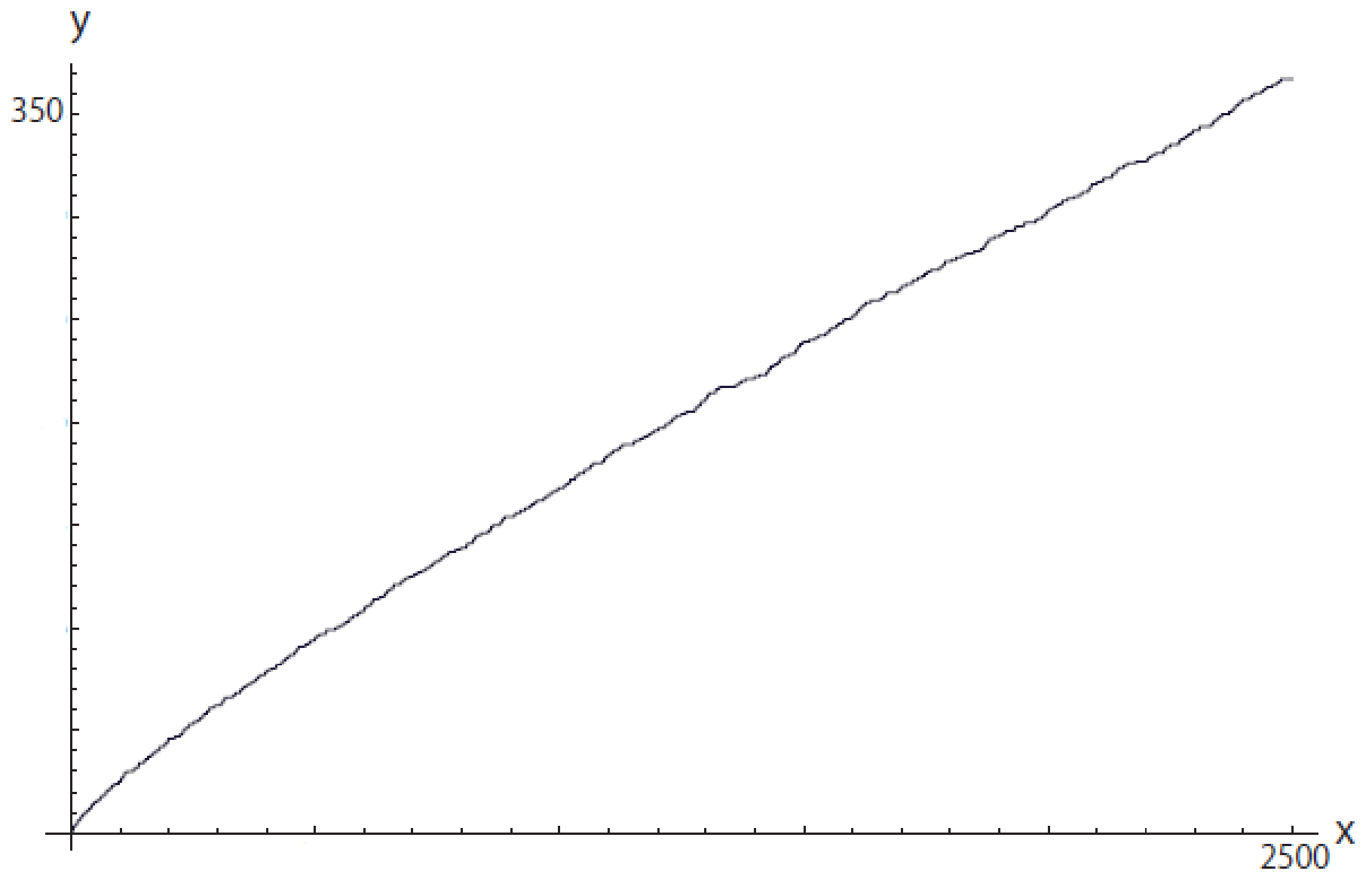
紀元前2万年頃のイシャンゴ骨（ナイル川源流）

Science Museum of Brussels提供. (Wikipedia)

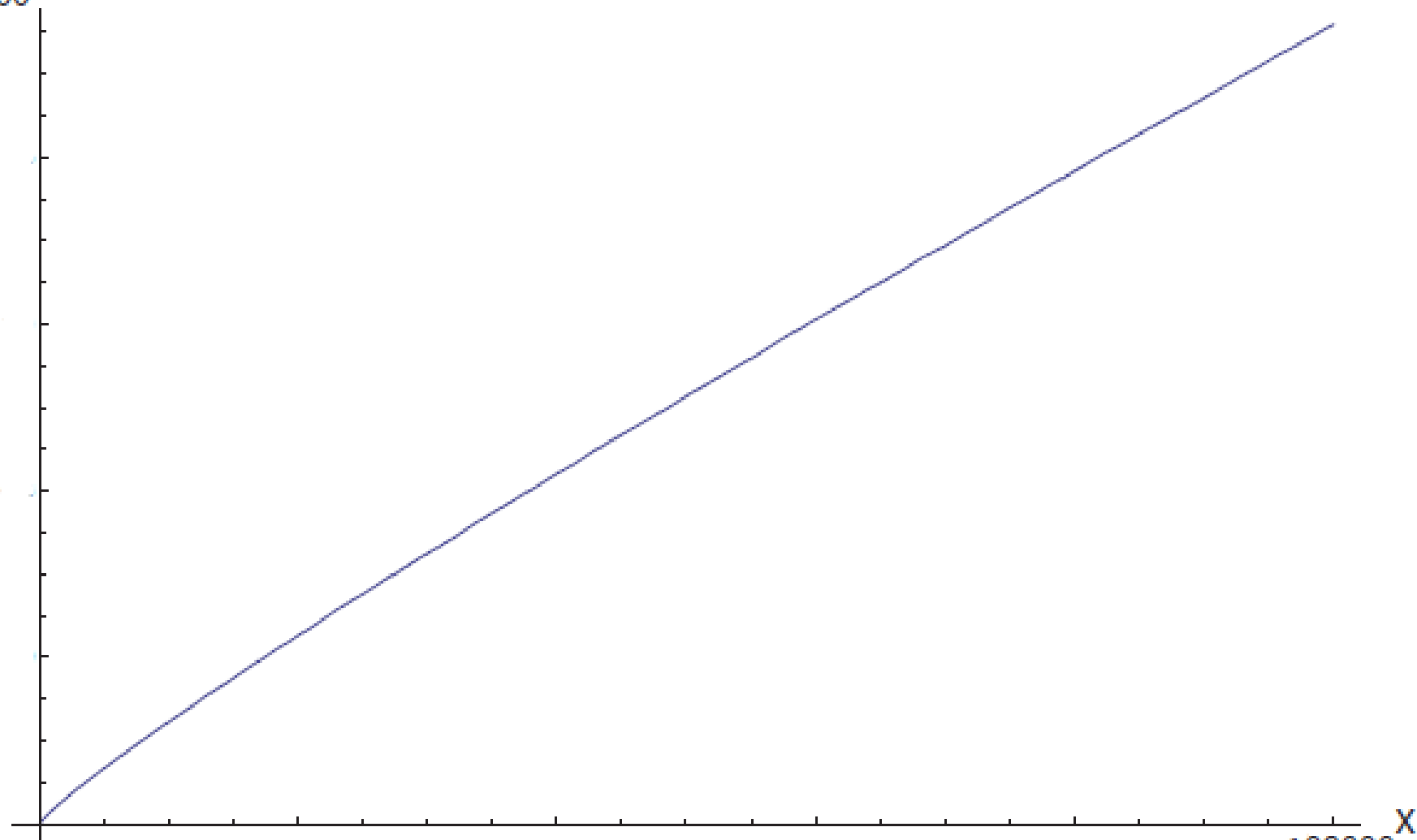


2.2 素数のグラフ





10000^y

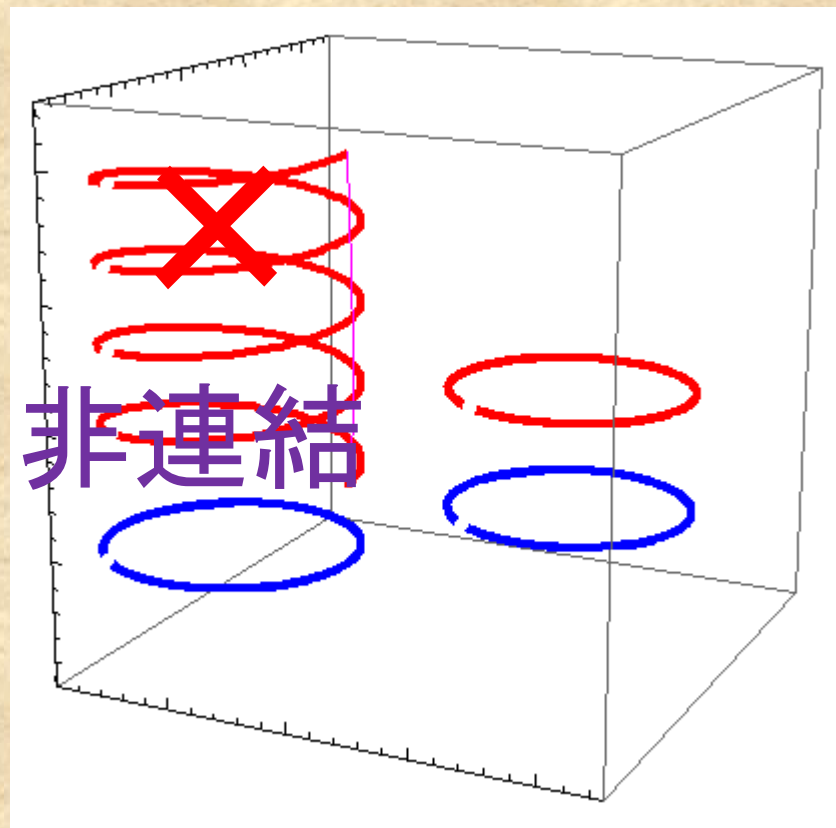
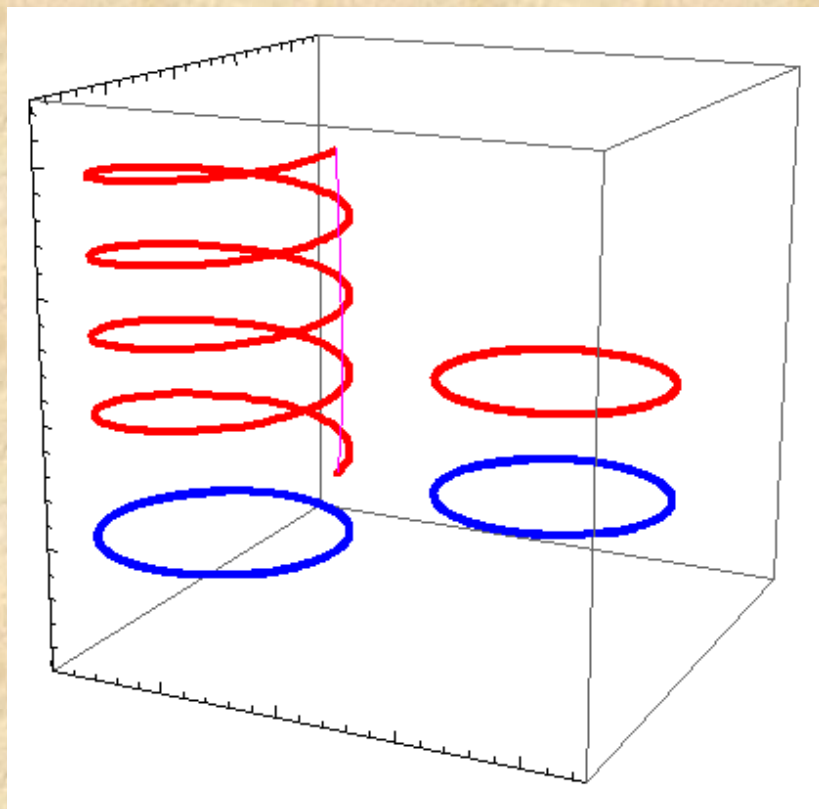


10000^x

☆素数をまとめて考える

→ **素数空間** (1次元～3次元)

☆**空間**の「形」を調べるために、その**被覆空間**たちを調べる方法がある。



▪ **Zの素数空間**

$$P = \{2, 3, 5, 7, 11, 13, 17, 19, 23, 29, \dots\}$$

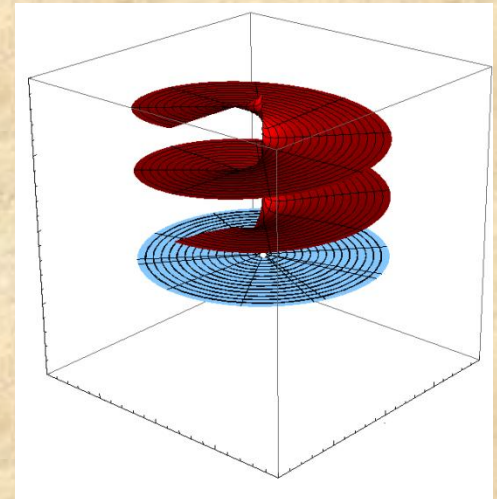
▪ **Zの素数空間の被覆空間の例**

$Z[i] = \{a + bi \mid a, b: \text{整数}\}$ の全ての素元 ($i^2 = -1$)

$$P' = \{1+i, 3, 1+2i, 1-2i, 7, 11, 3+2i, 3-2i, \dots\}$$

$$P' - \{1+i\} \quad \square \quad \vdots \quad \square \quad \square \quad \vdots$$

$$P - \{2\} \quad \square \quad \square \quad \square \quad \square \quad \square$$



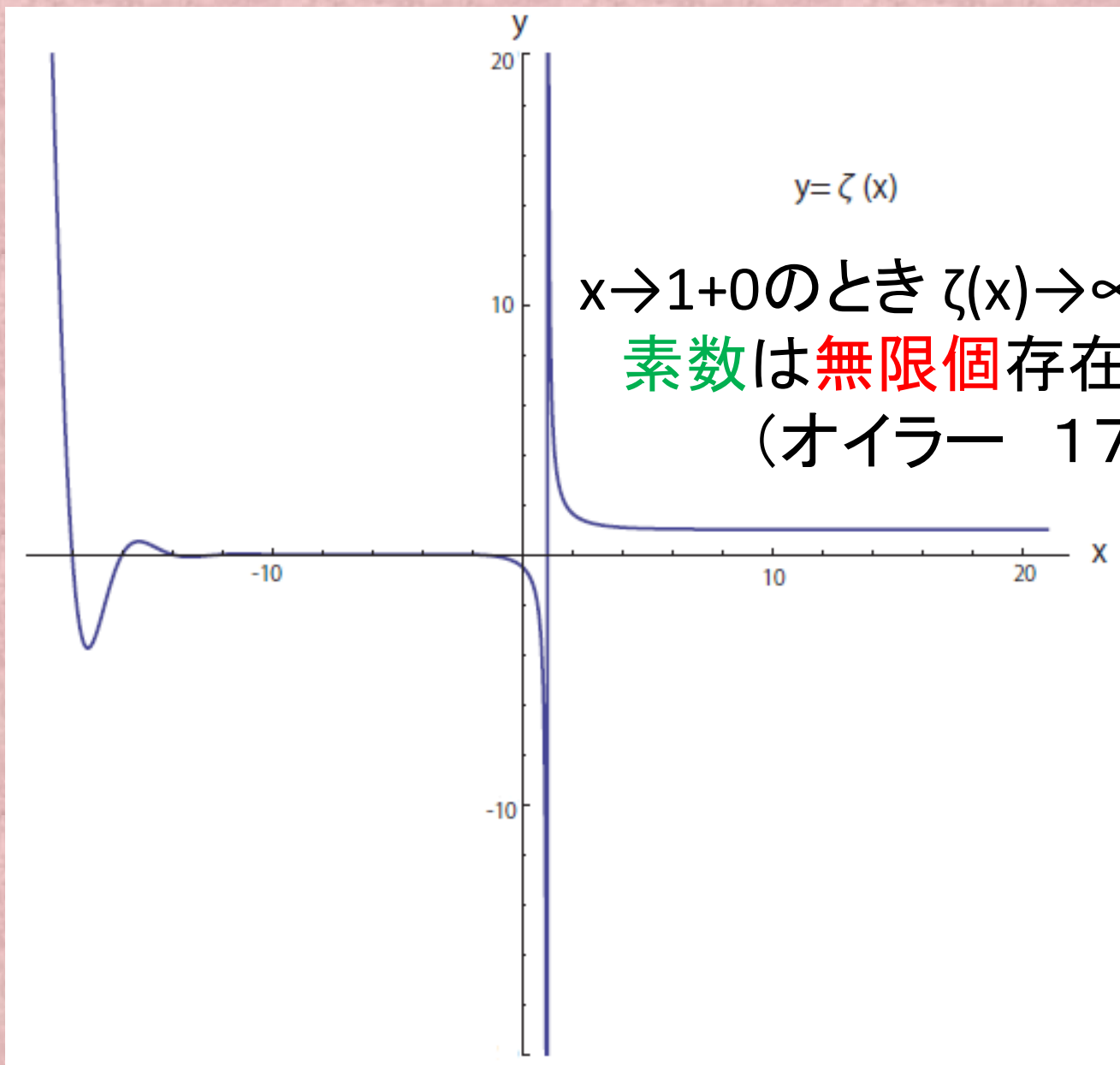
素数の個数 $\pi(x)$ は？
素数空間 P の被覆空間は？

いずれの問題もゼータ関数
と呼ばれる特殊関数が
解答の鍵を握っている！

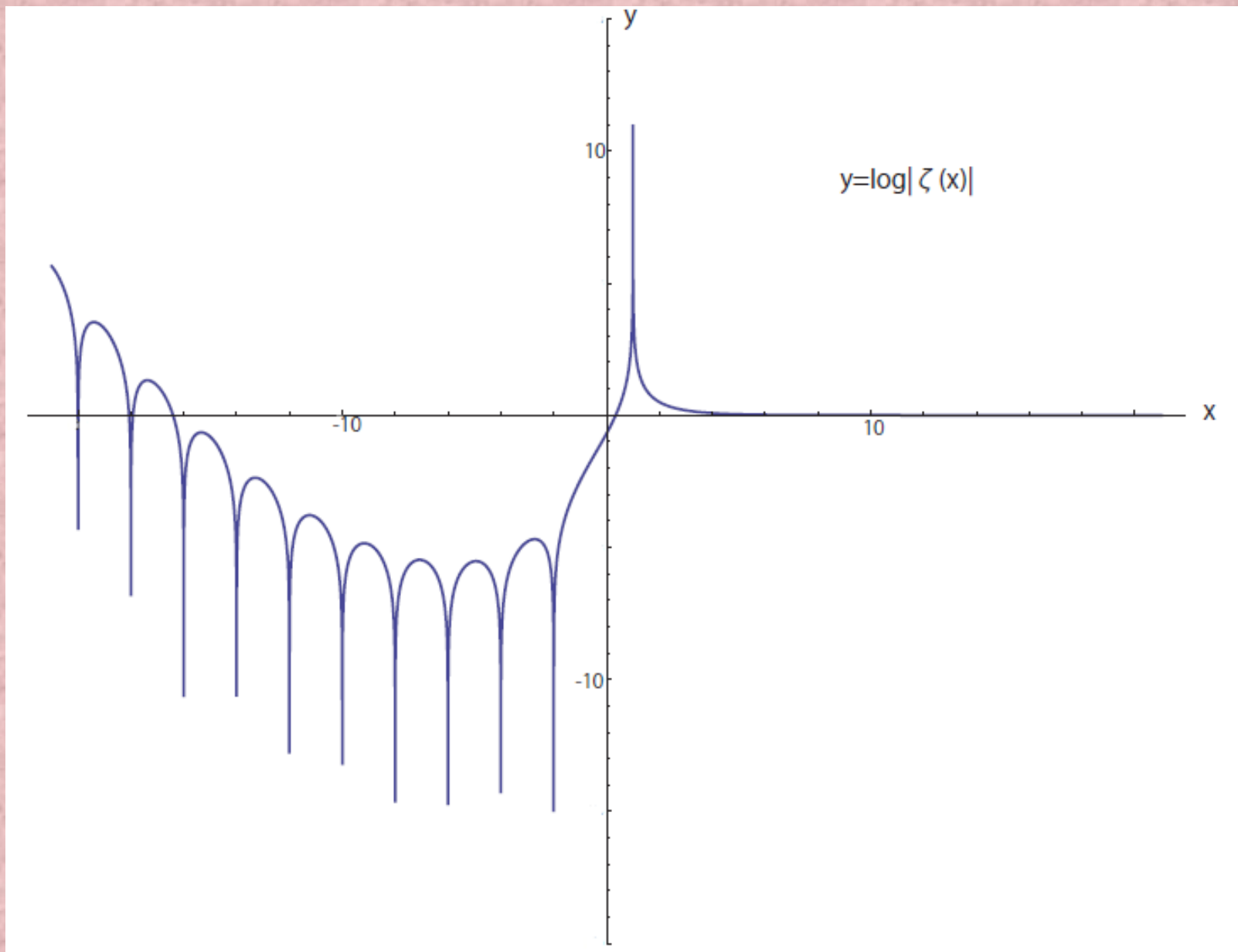
3. 1 – 3. 2 リーマンゼータ関数

$$\zeta(x) = \frac{1}{1^x} + \frac{1}{2^x} + \frac{1}{3^x} + \frac{1}{4^x} + \frac{1}{5^x} + \cdots + \frac{1}{n^x} + \cdots$$

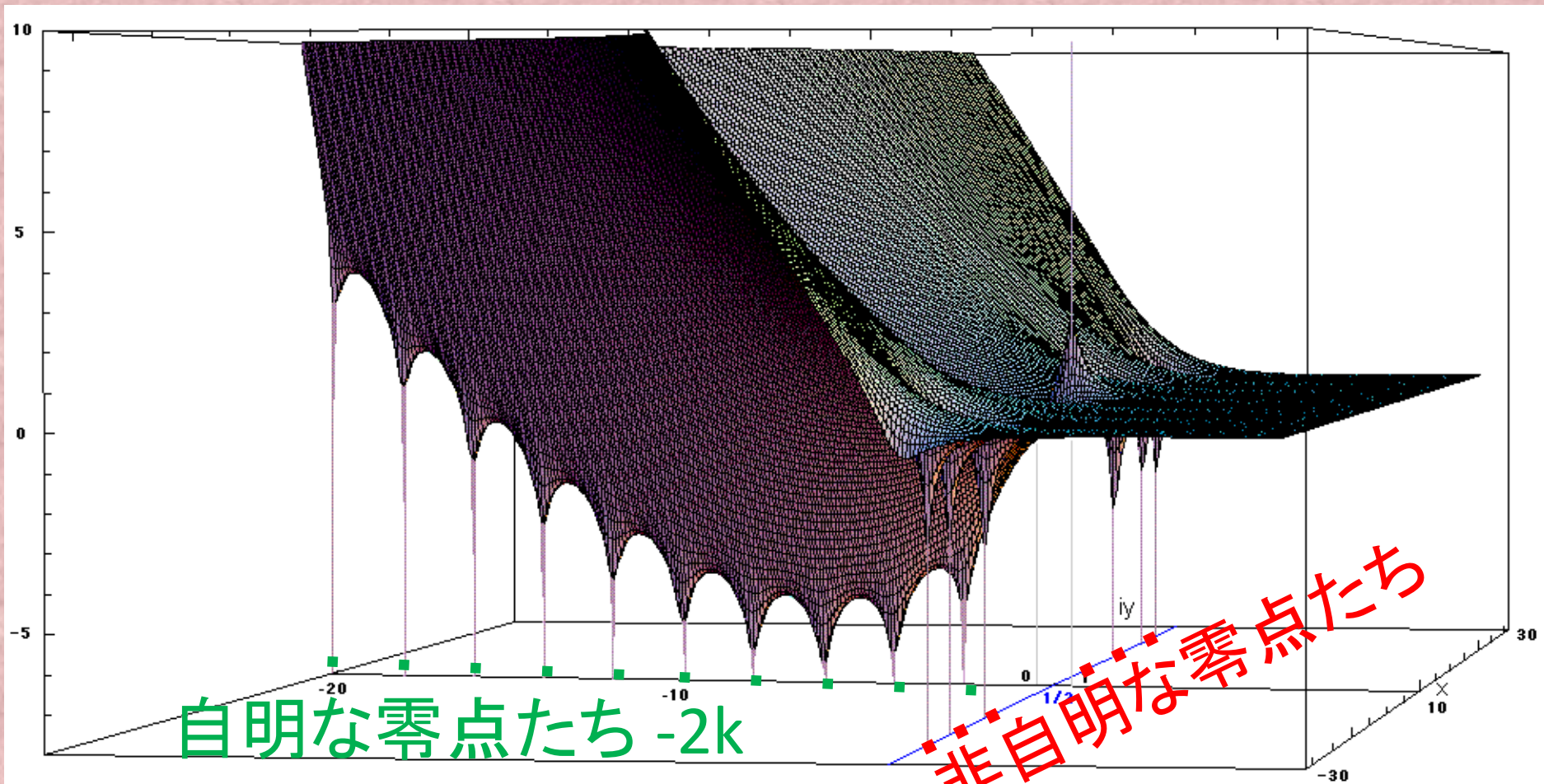
- $x > 1$ のとき収束する.
- 複素変数 $s = x + iy$ の複素関数 $\zeta(s)$ に滑らかに拡張できる.
(滑らかさ \Leftrightarrow 高次の微分可能性)



実関数 $\zeta(x)$



実関数 $\log|\zeta(x)|$



複素関数 $\log |\zeta(s)| = \log |\zeta(x+iy)|$

$\zeta(s_0)=0$ となる s_0 を $\zeta(s)$ の零点という.

$\Leftrightarrow s \rightarrow s_0$ のとき $\log |\zeta(s)| \rightarrow -\infty$ となる.

3.3 リーマン予想

$\zeta(s)$ の全ての非自明な零点は、
直線 $x=1/2$ 上にある。



同値な予想

素数の個数 $\pi(x)$ の予想

$$\pi(x) = \int_2^x \frac{dt}{\log t} + O(\sqrt{x} \log x)$$

解決すればクレイ数学研究所から100万ドル！

(× クレイ社 p.13,-1.4)

3. 4 リーマンゼータ値

$$1 + \frac{1}{2^2} + \frac{1}{3^2} + \frac{1}{4^2} + \frac{1}{5^2} \text{ etc.} = \frac{p^2}{6} = P$$

$$1 + \frac{1}{2^4} + \frac{1}{3^4} + \frac{1}{4^4} + \frac{1}{5^4} \text{ etc.} = \frac{p^4}{90} = Q$$

$$1 + \frac{1}{2^6} + \frac{1}{3^6} + \frac{1}{4^6} + \frac{1}{5^6} \text{ etc.} = \frac{p^6}{945} = R$$

$$1 + \frac{1}{2^8} + \frac{1}{3^8} + \frac{1}{4^8} + \frac{1}{5^8} \text{ etc.} = \frac{p^8}{9450} = S$$

$$1 + \frac{1}{2^{10}} + \frac{1}{3^{10}} + \frac{1}{4^{10}} + \frac{1}{5^{10}} \text{ etc.} = \frac{p^{10}}{93555} = T$$

$$1 + \frac{1}{2^{12}} + \frac{1}{3^{12}} + \frac{1}{4^{12}} + \frac{1}{5^{12}} \text{ etc.} = \frac{691 p^{12}}{6425 \cdot 93555} = V.$$

オイラーの数値リスト(1735)

$\zeta(1-k)$ は有理数.

分母の予測は可能 *
分子の予測は困難 *

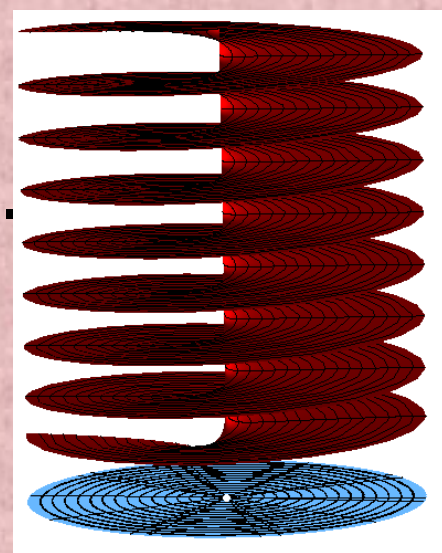
素数 p の出現が周期 $p-1$
となるのは同じ.

岩澤主予想 (メイザー & ワイルズ, 1984)

$\zeta(1-k)$ の分子に素数 p が出現する.

\Leftrightarrow 素数空間 $P - \{p\}$ に k 方向の p 巾無限次被覆空間 P' が存在.

$\Leftrightarrow p^\infty$ 円分体の k 方向の p 巾イデアル類群の位数は無限.



どの程度の無限であるかを精密に証明している.
保型形式という特殊関数を用いて被覆空間を構成する.

フェルマーの最終定理(ワイルズ,1994)

$$x^n + y^n = z^n, x, y, z, n : \text{整数}, n > 2$$

ならば, $x y z = 0$.

- ・フライは最終定理の反例から異常な楕円曲線(谷山-志村予想の反例)が構成されると主張し、リベットがその主張を証明した。
- ・ワイルズは、岩澤主予想の証明で用いた手法を発展させて谷山-志村予想(楕円曲線と保型形式の対応)を証明し、最終解決に至った。

素数空間, ゼータ関数はまだまだ未解明.

- ・高次表現での対応(ラングランズ予想)
- ・ゼータ関数の零点の位置の解釈.
- ・特殊な素数の革命的な探索方法.

無限の素数空間たちの探検は刺激的！