Ch2. 素数と円周率

2003年度 夏合宿

堀田 敬介

Contents

- 素数
  - 定義：素数とは？
  - 全ての素数を！
  - 素数生成Ⅰ～Ⅲ
  - 素数の分布・素数定理
  - 不思議な素数Ⅰ，Ⅱ
  - 素数判定
- 円周率
  - 定義：円周率とは？
  - 記憶術Ⅰ，Ⅱ
  - 円周率生成：近似Ⅰ，Ⅱ
  - 円周率生成：公式Ⅰ，Ⅱ
  - πを求める
  - πをシミュレーションで求める

Ch2. 素数と円周率

素数

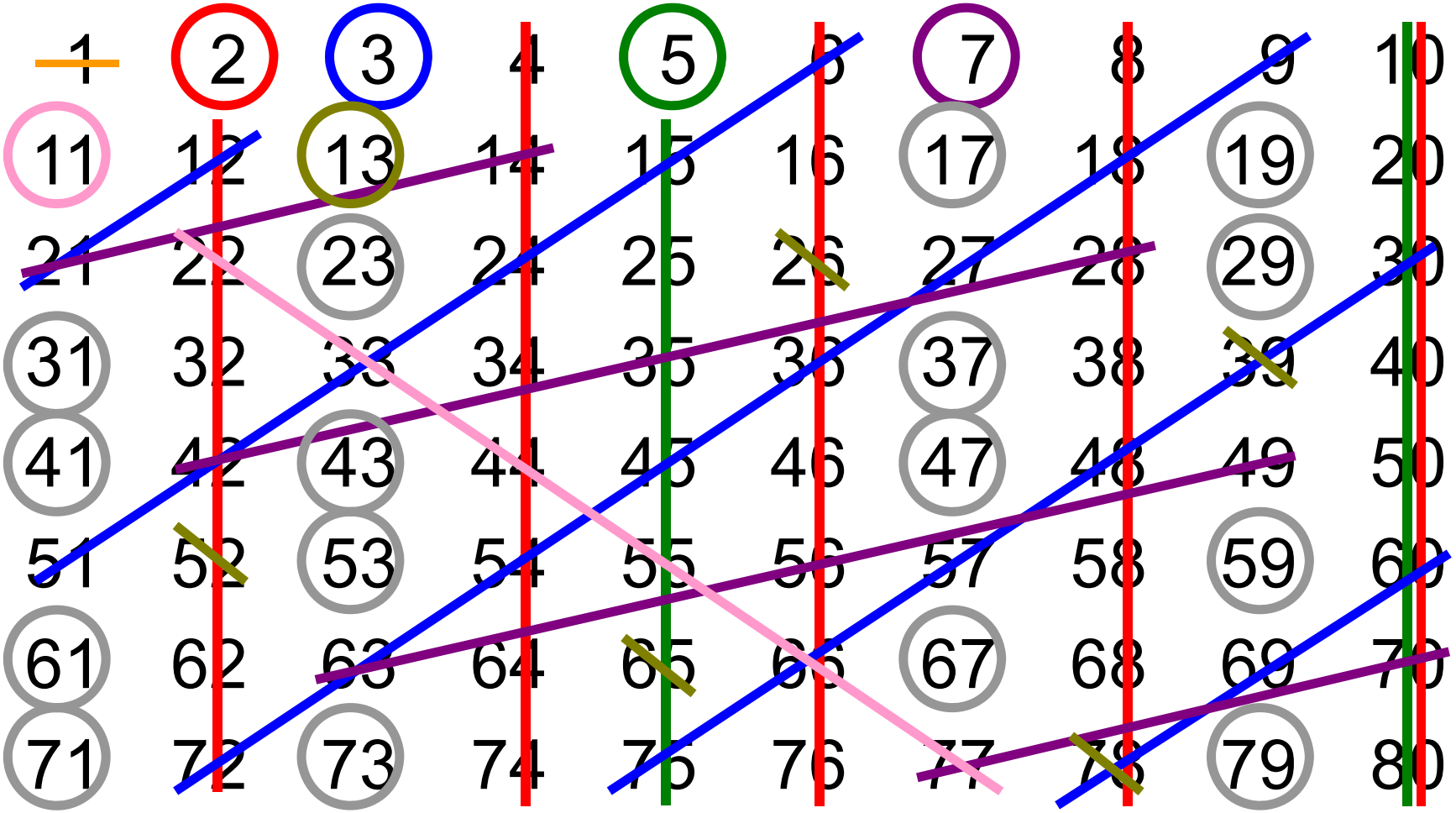
素数: 定義

- 素数
  - 「1とその数以外に約数を持たない数（1を除く）」
    - 2, 3, 5, 7, …
    - 100番目の素数: 541
    - 200番目の素数: 1223
    - 300番目の素数: 1987　　←逆！？
    - 400番目の素数: 1741　　←逆！？
    - 500番目の素数: 3559
    - 600番目の素数: 4409
    - 700番目の素数: 5279

……

素数: 全ての素数を！

- Eratosthenesの篩い (B.C.240頃)



素数：Coffee Break!

Eratosthenesの篩いはいつまでやるの？

$\sqrt{n}$ まで！

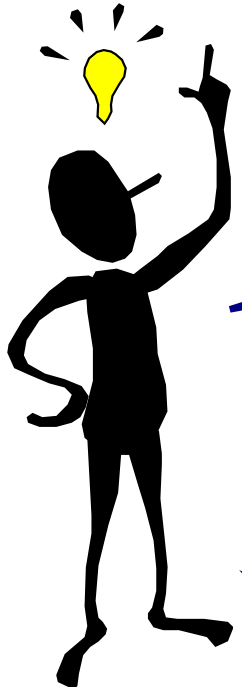
$\sqrt{80} \approx 8.94$

なんで？

素数は無限個あるの？

どうしてわかるの？

無限個ある！
by ユークリッド
B.C.330頃『原論』



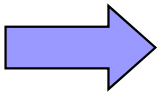
素数: 素数生成 I

- 素数生成多項式

$$4n^2+4n-1 \quad (n=1,\cdots,4)$$
$$n^2+n+17 \quad (n=1,\cdots,15)$$ byオイラー?
$$n^2+n+41 \quad (n=1,\cdots,39)$$ byオイラー?
$$n^2-n+41 \quad (n=1,\cdots,40)$$ byオイラー(1707-83)
$$n^2-5n+79 \quad (n=1,\cdots,78)$$

- 多項式による素数生成の限界

$$a_m n^m + a_{m-1} n^{m-1} + \cdots + a_0$$



$n=a_0$ のとき a_0 で割り切れる！

素数：素数生成 II

- フェルマ数： $F_n \equiv 2^{2^n}+1$

byフェルマー(1601-65)

$$F_1 = 2^{2^1}+1 = 5$$
$$F_2 = 2^{2^2}+1 = 17,$$
$$F_3 = 2^{2^3}+1 = 257,$$
$$F_4 = 2^{2^4}+1 = 513,$$
$$\vdots$$
$$F_5 = 2^{2^5}+1 = 4294967297 = 641\times 6700417$$

by オイラー(1707-83)

フェルマ予想
「全てのフェルマ数は素数」

新予想
「$n \geq$ のフェルマ数は合成数」

コンピュータの計算で，確認できたところまでは，nが5以上は全て合成数だった！

素数：素数生成Ⅲ

- メルセンヌ数：$M_n \equiv 2^n - 1$

byメルセンヌ(1588-1647)

$$M_1 = 2^1 - 1 = 1,$$
$$M_2 = 2^2 - 1 = 3,$$
$$M_3 = 2^3 - 1 = 7,$$
$$M_4 = 2^4 - 1 = 31,$$
$$M_5 = 2^5 - 1 = 127$$
$$\vdots$$
$$M_{11} = 2^{11} - 1 = 2047 = 23 \times 89$$

フランク・N・コール(コロンビア大,1903)

$$M_{67} = 147573952589676412927$$
$$= 193707721 \times 761838257287$$

- メルセンヌ素数：「$\exists n, M_n$と書ける素数」

素数：Coffee Break!

メルセンヌ素数探索の歴史

n	桁	発見者	発見年
8	2^{31}		1750
12	2^{127}		1876
13	2^{521}		1952
14	2^{607}		1952
15	2^{1279}		1952
16	2^{2203}		1952
17	2^{2281}		1952
…	⋮		…
34	2^{125778}		1996
35	$2^{1398269}$		1996.11.13
36	2^{297622}		1997.8.24
37	2^{302137}		1998.1.27
38	2^{697259}		1999.6.1
39	2^{134669}		2001.11.14

人間の時代
(B.C.～1876 [n=2～127])

人間＋コンピュータの時代
(1952～85 [n=521～216091])

スパコンの時代
(1992～96 [n=756839～1257787])

GIMPSの時代?
(1996～?? [n=1398269～13466917])

GIMPS (The Great Internet Mersenne Prime Search)
http://www.mersenne.org/prime.htm

素数：奇数素数に分解

- ゴルドバッハ分解：

$$20 = 7 + 13, \quad 30 = 13 + 17,$$
$$22 = 11 + 11, \quad 32 = 13 + 19$$
$$24 = 7 + 17, \quad 34 = 11 + 23,$$
$$26 = 13 + 13, \quad 36 = 7 + 29,$$
$$28 = 11 + 17, \quad 38 = 19 + 19,$$

ゴルドバッハ予想
「$n \geq 6$の任意の偶数は2つの奇素数の和で表せる」

4×10^{14}までの全ての偶数について成り立つことがコンピュータにより確かめられている.『Wikipedia』

素数：素数の分布

- ユークリッド(Eukleides,BC330頃)：『原論』
  - 「素数は無限にある」
- チェビシェフの定理(P.L. Chebyshev,1821-94)
  - 「$n>1$ のとき $(n,2n)$ に必ず素数が存在」
- 素数の分布
  - 「$\lim_{n\to\infty}\dfrac{\pi(n)\cdot\log n}{n}=1$」

1792年 15歳!
ルジャンドルも予想

ガウス(K.F. Gauss,1777-1855)
の予想

【注】$\pi(n)$：自然数 n 以下の素数の個数

素数: 素数の分布

n	$\pi(n)$	$n/\log n$	$\pi(n)\cdot\log n/n$
10^2	25	22	1.1513
10^3	168	145	1.1605
10^4	1232	1086	1.1347
10^5	9618	8686	1.1073
10^6	78498	72382	1.0845
10^7	664579	620421	1.0712
10^8	5761455	5428681	1.0613
10^9	50847534	48254942	1.0537
10^{10}	455052511	434294482	1.0478

【注】小数点以下四捨五入

素数：素数の分布

- ユークリッド(Eukleides,BC330頃) :『原論』
  - 「素数は無限にある」
- チェビシェフの定理(P.L. Chebyshev,1821-94)
  - 「$n>1$ のとき $(n,2n)$ に必ず素数が存在」
- 素数の分布
  - 「$\lim_{n\to\infty} \frac{\pi(n)\cdot\log n}{n} = 1$」

1792年 15歳!
ルジャンドルも予想

ガウス(K.F. Gauss,1777-1855)
の予想

素数定理

1896 アダマール(J.S. Hadamard,1865-1963),
プーサン(C.V. Poussin,1866-1962)
[リーマンのゼータ関数，一変数関数解析論で証明]
1949 セルバーグ (Serberg,1917-) [初等的証明]

（ガウスの）素数定理

$$\lim_{n\to\infty} \frac{\pi(n)}{\int_2^n \frac{dt}{\log_e t}} = 1$$

リーマンのゼータ関数

$$\zeta(s) = \sum_{n=1}^{\infty} n^{-s}$$

素数：不思議な素数Ⅰ

- 双子素数＝「差が2の素数の組」

$(3,5),(11,13),(17,19),(29,31),$
$(41,43),(71,73),\cdots$

双子素数予想
「双子素数は無限にある」

- 三つ子素数＝「差が2の3つの素数の組」

$(3,5,7)$

三つ子素数はこれだけ

【証】
$(3k,3k+2,3k+4)$
$(3k+1,3k+3,3k+5)$
$(3k+2,3k+4,3k+6)$

四つ子以上の素数はない！

素数：不思議な素数 Ⅱ

- 回文素数

  151,727,…

- エマープ　(emirp)　prime

  (13,31), (17,71), (37,73), (79,97),…

全部で
27個だけ

- 素な素数=「右から桁を落としていっても全て素数」

  53,317,599,797,2393,3793,3797,7331,
  23333,23339,31193,31379,…,73939133

- 素な素数=「左から桁を落としていっても全て素数」

  357686312646216567629137

これが最大

素数: 素数判定

- Sieve of Eratosthenes (B.C.240頃) $\Omega(\sqrt{n})$ steps
- Fermat's Little Theorem (1600代)
- E.A. Lucas (1876)
- 素数判定 $\in NP \cap coNP$ (V.Pratt,1975)
- Miller's Algorithm (G.L. Miller,1976, imp. by M.O.Rabin,1980)
  - (確率的に)多項式時間で判定
- $(\log n)^{O(\log\log\log n)}$ time (Adleman, Pomerance & Rumely, 1983)

……

- AKS Algorithm $\tilde{O}(\log^{7.5} n)$ time
  - (決定的に)多項式時間で判定

M.Agrawal, N.Kayal & N.Saxena ``PRIMES is in P'' 2002.8 (revised 2003?)

フェルマーの小定理

pを素数とすると,

$\forall a \in Z, a^p \equiv a \bmod p$

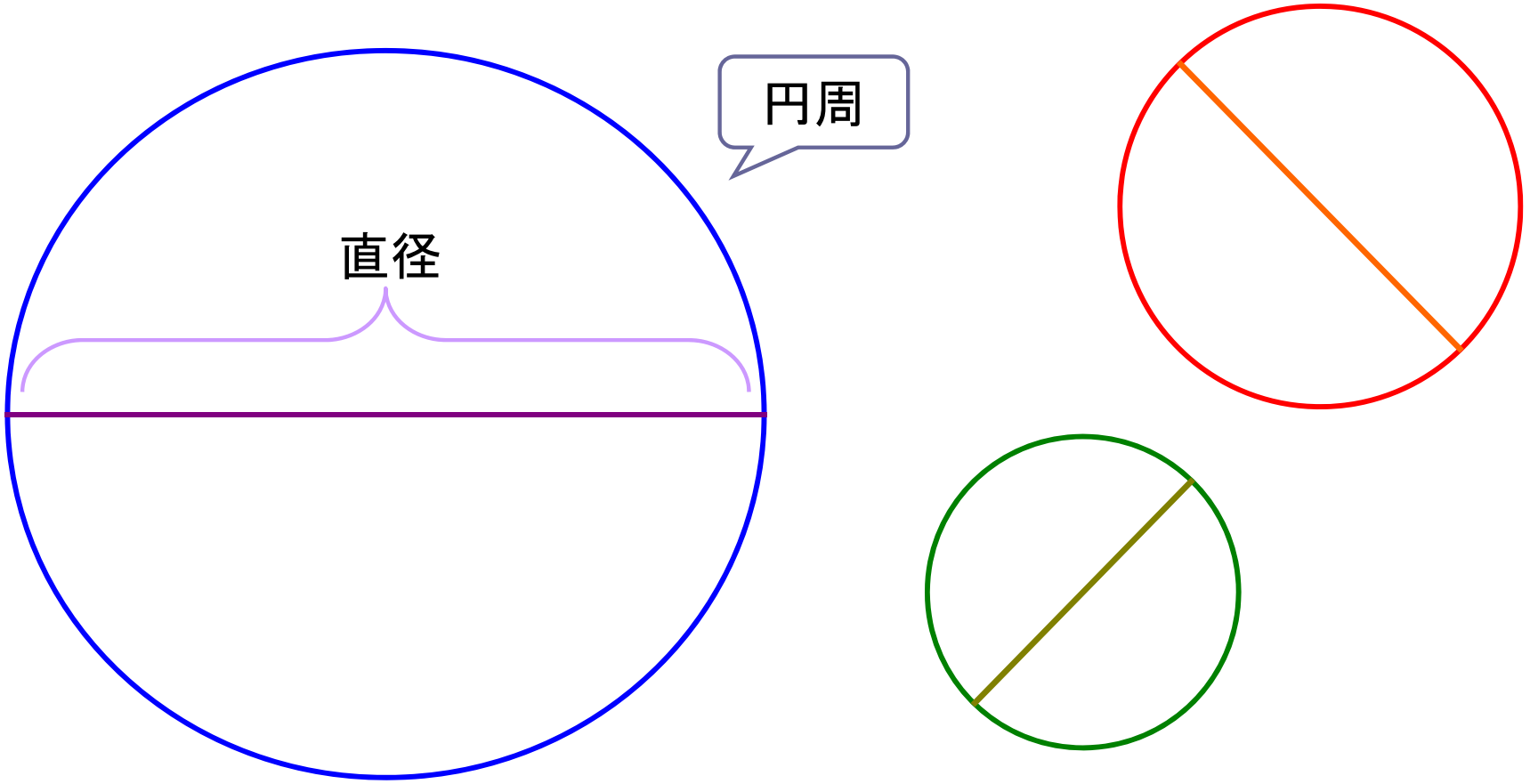
Ch2. 素数と円周率

円周率

円周率：定義

どんな大きさの円でも
この比率は等しい！

- 円周率:περιφερεια
  - 「直径に対する円周の比率（=円周/直径）」



円周率: 記憶術 I

- [日本語:40桁]

  3.1 4 159 2 6 5 35 8979 32 38462

  産医師異国に向こう 産後薬なく 産児御社に

  64 33 832 79 50 28 84 197

  虫散々闇に鳴く 御礼には早よ行くな

- [英語:31桁]

  3. 1 4 1 5 9 2 6 5 3 5 8 …

  Now I know a spell unfailing, an artful charm for tasks availing,…

- [英語:32桁]

  3. 1 4 1 5 9 2 6 5 3 5 8 …

  May I tell a story purposing to render clear the ratio circular …

円周率: 記憶術 II

- [英語:8桁]

  May I have a large container of coffee?

- [英語:15桁]

  How I want a drink, alcoholic of course, after the heavy lectures involving quantum mechanics.

- [英語:31桁] (A.C.オーのアルキメデスに対する詩)

  Now I, even I, would celebrate
  In rhymes, unapt, the great
  Immportal Syracusan, rivalend nevermore,
  Who in his wondrous lore,
  Passed on before, Left men his guidance
  How to circles mensurate.

円周率: 円周率 近似 I

- エジプトの公式:〔2桁〕(リンド・パピルス(B.C.1650頃))

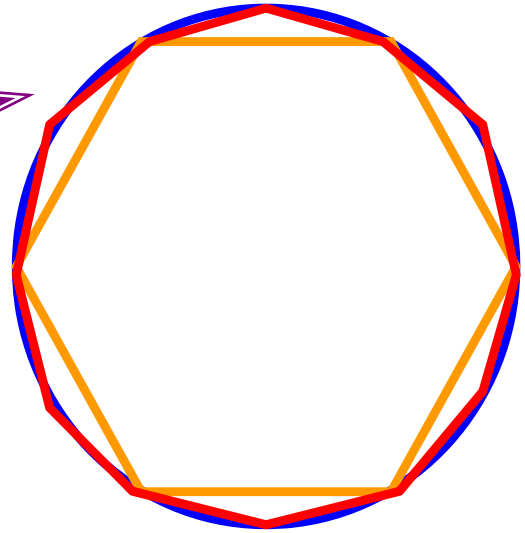
$$\pi \approx 4 \times \left(\frac{8}{9}\right)^2 = 3.1604\cdots$$

- アルキメデス (B.C.250頃):〔3桁〕 [正96角形]

$$3.1408\ldots = \frac{223}{71} < \pi < \frac{22}{7} = 3.1428\cdots$$

内接正多角形を利用した極限

内接正6角形	周	6
内接正12角形	周	約6.21
内接正24角形	周	…
内接正48角形	周	…
内接正96角形	周	…
円	周	2π



円周率: 円周率 近似 II

- 祖沖之（そちゅうし）(429-500) :〔7桁〕[正24576角形]

$$\pi \approx \frac{355}{113} = 3.1415929\cdots$$

- 関孝和(1642?-1708) :〔10桁〕[正131072角形]

$$\pi > 3.14159265328899277759弱$$

- ルドルフ(1539-1610) :〔35桁〕[正 60×2^{29} 角形]

- J.H.ランベルト (1767年):
  πが無理数と証明

近似では
これが限界!?

円周率：円周率 公式 I

- 1598年『数学の諸問題 第8巻』ヴィエート(1540-1603)

$$\frac{2}{\pi}=\sqrt{\frac{1}{2}}\times\sqrt{\frac{1}{2}+\frac{1}{2}\sqrt{\frac{1}{2}}}\times\sqrt{\frac{1}{2}+\frac{1}{2}\sqrt{\frac{1}{2}+\frac{1}{2}\sqrt{\frac{1}{2}}}}\times\cdots$$

計算には役に立たない

- 1655年 ウォリス(1616-1703)

$$\frac{\pi}{2}=\frac{2}{1}\cdot\frac{2}{3}\times\frac{4}{3}\cdot\frac{4}{5}\times\frac{6}{5}\cdot\frac{6}{7}\times\frac{8}{7}\cdots\left(=\prod_n\frac{2n\cdot 2n}{(2n-1)(2n+1)}\right)$$

πへの収束が遅い

- 1670年代 グレゴリー(1638-75)，ライプニッツ(1646-1716)

$$\frac{\pi}{4}=1-\frac{1}{3}+\frac{1}{5}-\frac{1}{7}+\frac{1}{9}-\frac{1}{11}+\frac{1}{13}-\cdots\left(=\sum_n\frac{(-1)^{n-1}}{2n-1}\right)$$

πへの収束はもっと遅い

- 1700年代 オイラー(1707-83)

$$\frac{\pi^2}{12}=\frac{1}{1^2}-\frac{1}{2^2}+\frac{1}{3^2}-\frac{1}{4^2}+\frac{1}{5^2}-\cdots\left(=\sum_n\frac{(-1)^{n-1}}{n^2}\right)$$

円周率: 円周率 公式 Ⅱ

- I.Newton(1642-1727)

$$\frac{\pi}{6}=\frac{1}{2}+\frac{1}{2\cdot 3\cdot 2^3}+\frac{1\cdot 3}{2\cdot 4\cdot 5\cdot 2^5}+\frac{1\cdot 3\cdot 5}{2\cdot 4\cdot 6\cdot 7\cdot 2^7}+\cdots$$

- J.Machin (1680-1751)

$$\frac{\pi}{4}=4\arctan\left(\frac{1}{5}\right)-\arctan\left(\frac{1}{239}\right)$$

- C.F.Gauss (1777-1855)

$$\pi=48\arctan\left(\frac{1}{18}\right)+32\arctan\left(\frac{1}{57}\right)-20\arctan\left(\frac{1}{239}\right)$$

- F.C.M.Stormer (18?-?)

$$\pi=24\arctan\left(\frac{1}{8}\right)+8\arctan\left(\frac{1}{57}\right)+4\arctan\left(\frac{1}{239}\right)$$

円周率の公式集 http://www.pluto.ai.kyutech.ac.jp/plt/matumoto/pi_small/

円周率：πを求める

- 1610 ルドルフ　35桁
- 1706 マチン　100桁
- 1719 ド・ラグニー　129桁
- 1794 ウェガ　140桁
- 1824 ラザフォード　152桁
- 1855 リヒテル　500桁
- 1947 ファガーソン　808桁

- 1949 ENIAC　2037桁
- 1957 PEGASUS　10021桁
- 1961 IBM7090　100265桁
- 1973 CDC7600　100万桁
- 1983 HITACM-280H　1600万桁　（金田・吉野・田村）
- 1989 CRAY-2　4億8千万桁　（チュドノフスキー兄弟）
- 1996 Homebrew　80億桁　（チュドノフスキー兄弟）
- 1997 HITAC SR2201　171億桁　（高橋・金田）
- 1998 HITAC SR8000　2061億桁　（高橋・金田）
- 2002 HITAC SR8000/MPP　1兆2411億桁　（金田）

InterNetで計算！　PiHex　http://www.cecm.sfu.ca/projects/pihex/pihex.html

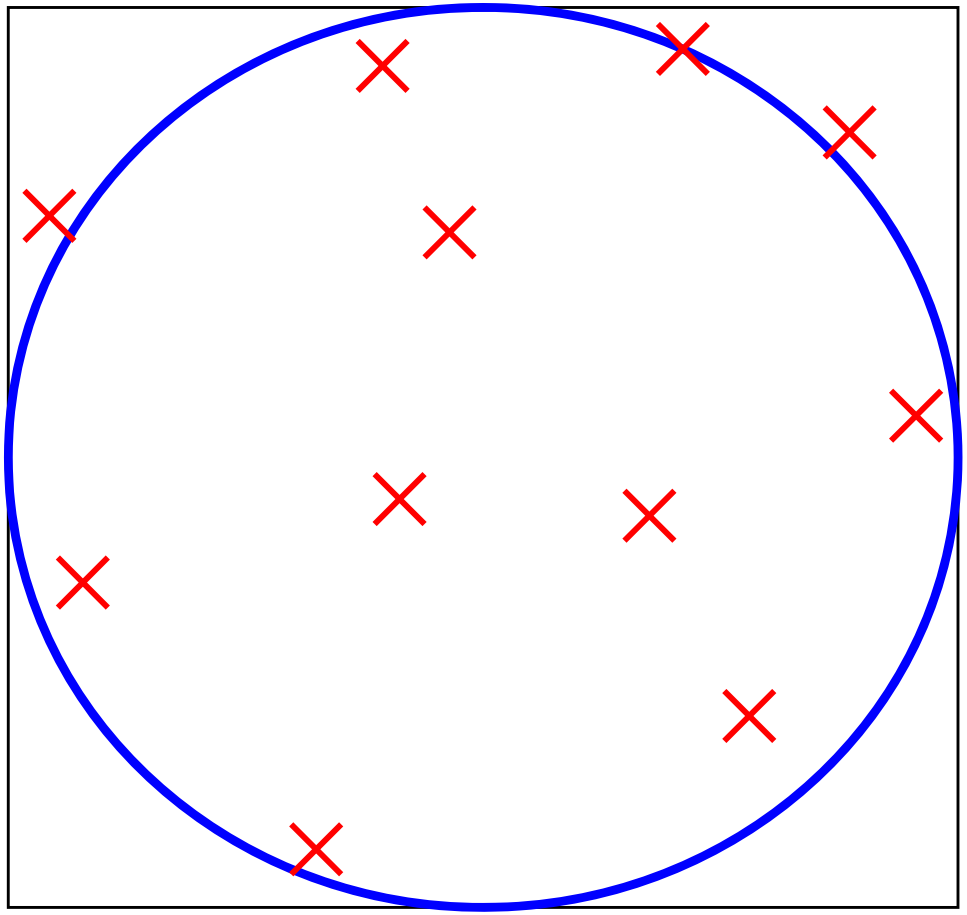
円周率：数値シミュレーション

- モンテカルロ法
  - 正方形（と内接円）の中に点をランダムに打つ．
  - 等間隔の平行線に対し，ランダムに針を落とす．

  など

円周率：数値シミュレーション

- モンテカルロ法：正方形と内接円



$$\pi r^2 : 4r^2 \approx m : n$$
$$\Leftrightarrow \pi \approx \frac{4m}{n}$$

m ：円内の点の数

n ：正方形内の点の数

円周率：数値シミュレーション

- モンテカルロ法：平行線に針を落とす(Buffon)

$$p = \frac{2l}{a\pi} \Leftrightarrow \pi = \frac{2l}{ap}$$

a ：平行線の間隔

l ：針の長さ（平行線間隔より短い）

p ：針が平行線と交わる確率

円周率：雑学

- πに現れる数字の頻度

100億桁までに，0～9が10億回ずつ出現するか？

- 1988：πの936万桁までの統計解析

  最も現れる数　：4 … 2,938,787回

  最も現れない数：7 … 2,934,083回

  最大連続数：　7が9個連続する

2936万桁のランダム数列で，9回連続で同じ数がでる確率は29%

結論

2936万桁の真にランダムな数列との差は統計的に認められない！

参考文献

- 堀場芳数「素数の不思議」講談社(1994.8)
- D.M. Davis, 好田順治 訳「美しい数学」青土社(1996.1)
- 今野紀雄「図解雑学 数の不思議」ナツメ社(2001.3)
- 有澤誠「パターンの発見」朝倉書店(2001.5)
- 涌井良幸・涌井貞美「パソコンで遊ぶ数学実験」講談社(2003.2)
- GIMPS : http://www.mersenne.org/prime.htm
- The Free Encyclopedia WIKIPEDIA : http://ja.wikipedia.org/wiki/
- 他…