International Statistical Review (3), 1966, 64, 329–344, Printed in Mexico

A Natural Random Number Generator

Yadolah Dodge

Statistics Group, University of Neuchâtel, Switzerland

Summary

Since the introduction of "middle square" method by John von Neumann for the production of "pseudo-random" numbers in about 1949, hundreds of other methods have been introduced. While each may have some virtue a single uniformly superior method has not emerged. The problems of cyclical repetition and the need to pass statistical tests for randomness still leave the issue unresolved. The aim of this article is to suggest the most natural random number generator of all, the decimals of π, as a unique source of random numbers. There is no cyclic behaviour, all finite dimensional distributions of the sequence are uniform, so that it satisfies all the properties of today's generation of statistical tests; because of the manner in which the numbers are generated it is conjectured that it will satisfy any further test with probability one. In addition, the history of π, its discovery and elucidation, is co-extensive with the entire history of mankind.

Key words: π; Random number generator; Simulation; Statistical tests; Pseudo-random numbers.

1 Introduction

... going only part of the way is not the same as going the wrong way.

Jostein Gaarder: Sophie's world

Random numbers are used in simulation, Monte Carlo methods, survey sampling, numerical analysis, computer programming, experimental physics and many other fields of applied sciences where random events play a major role. There are many ways to produce random numbers or a sequence of independent numbers with a specified distribution.

At the beginning, these numbers were obtained by mechanical devices such as well-stirred urns, roulette machines, or other instruments and the results were recorded either in tables, called tables of random numbers or used instantly for solution to a given problem. Random numbers collected in this fashion are sometimes called, *truly* random numbers.

The work of Tippett (1927), Fisher & Yates (1938), Kendall & Babington-Smith (1939b), Peatmann & Shafer (1942), Royo & Ferrer (1954a,b), and Steinhaus (1954) are major contributions prior to 1955. The total digits of random numbers found in these tables range between 1600 to 250,000. In 1955, RAND Corporation published a book containing one million random digits. The book also contains introductory material describing the production of the digits, tests of the digits and the use of the tables. The digits were prepared by driving electronic counters by electronically generated noises. Tables of random numbers are still used in experimental sciences such as design of experiments in agriculture, medicine or sampling surveys for randomization purposes to eliminate bias. However, in large scale simulation experiments, tables are of little use since millions of random numbers are required.

With the birth of computers classes of random generators such as linear congruential, multiple

recursive, Tausworthe, lagged-Fibonacci, generalized feedback shift register, and several combined generators just to name a few, were invented. Numbers generated with deterministic algorithms are called *pseudorandom* numbers. Since these types of generators are not the main subject of this paper, only a brief description of the most commonly used generators, the linear congruential family along with some cautionary notes will be given in Section 2.

The purpose of this article is to suggest that the billions of decimals of π now available are a natural source of a random number generator. In Section 3 we provide a brief history of π. This section includes the empirical determination of the value of π which cover the geometrical estimation of π, analytical expression for π, the calculation of its decimals and new algorithms for π. Section 4 examines the statistical studies on the decimals of π in order to investigate their randomness and makes some recommendations toward the future uses of π's decimals as a natural source of random numbers.

2 Uniform random number generators

With the invention of the computer, scientists began to explore the possibility of efficient methods of obtaining a sequence $(U_i) = U_0, U_1, U_2, \ldots$ of independent random numbers with computer programs by deterministic functions with a specified distribution. The most common distribution used in stochastic simulations for generating a sequence of random numbers is the *uniform distribution* on [0,1[. A uniform distribution over a finite set of numbers is one in which each possible number has equal probability. For example, each of the ten digits 0, 1, ..., 9 will occur about 1/10 of the time in a sequence of random digits. Each pair of two successive digits should occur about 1/100 of the time, and so on.

The pioneer work of John von Neumann (1951), the "*middle square*" which was first introduced in about 1949, has proved to be a poor source of random numbers. An n digit number is squared to produce a $2n$ digit number from which some middle n digits are taken for the next number and the process is repeated. The sequence gets into a short cycle of repeating elements, specially if a zero appears as an element of the sequence it will continually perpetuate itself.

Lehmer (1951) introduced a method called the *linear congruential*. In this method, the sequence X_i of random numbers integers is obtained by

$$X_{i+1} = (aX_i + c) \bmod m, i \geq 0, \tag{2.1}$$

where X_0 $(0 \leq X_0 < m)$ is the starting value, a $(0 \leq a < m)$, the multiplier, c $(0 \leq c < m)$, the increment and $m > 0$ is the modulus. The random sequence (U_i) is determined by (2.1) and $U_i = X_i/m$ (real valued between zero and one) once the starting value (*seed*) is given. The optimal choices of a, c, X_0 and the modulus are still subject to extensive research.

Since then hundreds of attempts have been made to produce many classes of generators of random numbers with long cycles, repeatability, speed, and good approximation to the uniform distribution. For extensive bibliographies on random generation and testing covering the periods of 1927–1971 and 1972–1976 the reader is referred to two papers by Sowey (1972) and (1978). In both articles about 450 references are listed chronologically and also under specially devised classification scheme. For a classical reference on pseudorandom numbers and especially on linear congruential sequences, see Niederreiter (1978). Rubinstein (1981), Ripley (1987), L'Ecuyer (1994) and Tezuka (1995) provide detailed surveys of the most recent papers on the uniform random number generators.

Ripley (1990) compares several generators across a wide range of machines. While recommending a couple of generators, he writes: "The whole history of pseudorandom number generation is riddled with myths and extrapolations from inadequate examples. A healthy dose of scepticism is needed in reading the literature."

Knuth (1981) provides a complete chapter of 177 pages on *random numbers*. The chapter includes all that one should know about the science of generating random numbers such as what is a random number, methods of generating random sequences, statistical tests for, algorithms and computer programs. In page 173 he writes : "The authors of many contributions to the science of random number generation were unaware that particular methods they were advocating would prove to be inadequate. Perhaps further research will show that even the random number generators recommended here are unsatisfactory; we hope this is not the case, but the history of the subject warns us to be cautious. The most prudent policy for a person to follow is to run each Monte Carlo program at least twice using different sources of random numbers, before taking the answers of the program seriously; this not only will give an indication of the stability of the results, it also will guard against the danger of trusting in a generator with hidden deficiencies. (*Every random number generator will fail in at least one application*)." For example, L'Ecuyer & Cordeau (1996) show that the random number generator of type (2.1) with $m = 2^{31} - 1$ and $a = 16807$ (IMSL) and another one with $m = 2^{32}$, $a = 69069$ and $c = 1$ do not pass the nearest pair test.

In what follows an attempt is made to present a random numbers generator, that passes all the current and future statistical tests with probability one. It is called a *natural random number generator.*

3 A brief history of π

The history of π is the story of man from the magnificent era of Babylonian–Egyptians to our modern day time, covering over 4000 years of history of mankind. The number was defined as the ratio of the circumference and the diameter of a circle, and by about 2000 B.C., the Babylonians found its approximate value to be 3 1/8 and the Egyptians had arrived at the value of $4(8/9)^2$.

The Old Testament (1 Kings 7:23, and 2 Chronicles 4:2), contains the verse: "Also he made a molten of sea of ten cubits from on brim to brim, round in compass, and five cubits the high thereof; and a line thirty cubits did compass it round about."

The molten of sea, is round; it measures 30 cubits round about in circumference and 10 cubits from brim to brim in diameter and hence the biblical (implicit) value of π is 30/10=3. According to Chabert *et al.* (1994) the Bible citation is probably written around 600 B.C. and during this period better estimates of π existed. Consequently this passage should not be interpreted to mean an estimate for π. However, van der Waerden (1983, pp.187–191) in discussing the Mishnat ha-Middut (a Hebrew treatise on mensuration which is assumed to be written by Rabbi Nehemiah around 150 A.D) writes: "Next follows a discussion of a passage in the Bible, in which it is said that a molten sea, round in compass, measures 10 cubits from brim to brim, while its circumference is said to be 30 cubits. The author tries to bring this into accord with the opinion of the "people of the world" who say that the circumference of a circle contains $3 + \frac{1}{7}$ times the diameter. According to his interpretation, the difference is due to the thickness of the sea at the two brims. The author's opinion seems to be that the diameter of 10 cubits included the walls of the sea, while the circumference excluded them." Thus confirming the Biblical citation to be an estimation of π.

3.1 Geometrical Estimation of π

Archimedes of Syracuse (287–212 B.C.) was the first to give a method of calculating π to any desired degree of accuracy. He considered inscribed and circumscribed polygons of 96 sides and gave the estimate of

$$3\ 10/71 < \pi < 3\ 1/7.$$

To improve on Archimedes estimate, it is sufficient to increase the number of sides and calculate

the perimeters or areas of the polygons more accurately. Archimedes calculated π to the equivalent of two decimal places.

According to van der Waerden (1983), Apollonios of Perge (225 B.C.) wrote a treatise entitled "Rapid Delivery", in which he improved on Archimedes' estimate of π. Tannery (1893) conjectured that Apollonios' estimate of π was $\pi = 3.1416$.

Heron (62 A.D.) calculates the area of a circle as $3 + \frac{1}{7}$ times the square of the radius, and the circumference as $3 + \frac{1}{7}$ times the diameter. According to van der Waerden (Chapter 7), the Chinese geometer Liu Hui (263 A.D.) gives two estimates for π

$$\pi = 3.14 \text{ and } \pi = 3.1416$$

and Tsu Ch'ung-Chih (430–501 A.D.) presented a more accurate value

$$\pi = 355/133 = 3.1415929...$$

Li Shung-Feng (7th century A.D.) used the value of 22/7 for π. Aryabhata (6th century) the Hindu astronomer gives the fraction 62832/20000 the same fraction in the reduced form 3927/1250. According to van der Waerden (1983, p.186) the estimates given by Liu Hui, Aryabhata and Bhaskara II all are derived from one and the same source which is probably due to Apollonios.

Anthoniszoom (1527–1607) found the value 355/113, which is correct to 6 decimal places. Von Rouman (1561–1615) used Archimedean polygons with 2^{30} sides to calculate π with 15 decimals. Ludolph van Ceulen (1539–1610) used a polygon with 6×2^{29} sides to calculate π with 20 decimal places. (Germans call π the Ludolphine number).

3.2 Analytical Expressions for π

Viète (1593) was the first to give π by an analytical expression of an infinite sequence of algebraic operations as

$$\frac{2}{\pi} = \sqrt{\frac{1}{2}} \cdot \sqrt{\frac{1}{2} + \frac{1}{2}\sqrt{\frac{1}{2}}} \cdot \sqrt{\frac{1}{2} + \frac{1}{2} + \sqrt{\frac{1}{2} + \frac{1}{2}\sqrt{\frac{1}{2}}}} \cdot \ldots \tag{3.1}$$

He derived this formula by relating the area of an n-sided polygon to that of a $2n$-sided polygon. Viète did not use (3.1) for calculation of π correct to 9 decimals. He used the Archimedean method by taking a polygon of 393 216 sides.

Wallis (1656) derived the infinite product expression for π as

$$\frac{\pi}{2} = \frac{2}{1} \cdot \frac{2}{3} \cdot \frac{4}{3} \cdot \frac{4}{5} \cdot \frac{6}{5} \cdot \frac{6}{7} \cdot \frac{8}{7} \cdot \frac{8}{9} \cdot \ldots\ldots, \tag{3.2}$$

and Lord Brouncker in 1658 found the infinite continued fraction development

$$\frac{4}{\pi} = 1 + \cfrac{1^2}{2 + \cfrac{3^2}{2 + \cfrac{5^2}{2 + \cfrac{7^2}{2 + \ldots}}}} \tag{3.3}$$

Leibniz (1682) obtains π by an alternating series

$$\frac{\pi}{4} = 1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \frac{1}{9} - \frac{1}{11} + \ldots\ldots \tag{3.4}$$

Leibniz discovered (3.4) in 1673 but it was published 9 years later in *Acta Eruditorum*. To obtain even two decimal places one is required 300 terms of (3.4).

Before the work of Leibniz, Gregory discovered in 1671 the development of arctan x

$$\arctan x = x - \frac{x^3}{3} + \frac{x^5}{5} - \frac{x^7}{7} + \ldots\ldots, \qquad -1 \leq x \leq 1 \tag{3.5}$$

but failed to note explicitly the special case corresponding to $x = 1$, which is (3.4) due to Leibniz. In a letter to Oldenburg dated October 24, 1676, Newton discovered the power series

$$\arcsin x = x + \frac{1}{2}\frac{x^3}{3} + \frac{1 \cdot 3}{2 \cdot 4}\frac{x^5}{5} + \ldots \qquad -1 \leq x \leq 1 \tag{3.6}$$

and by setting $x = 1/2$ he obtained $\arcsin(1/2) = \pi/6$ which converges more quickly than that of (3.5). To obtain 15 correct decimal places for π, he used

$$\pi = \frac{3\sqrt{3}}{4} + 24\left(\frac{1}{12} - \frac{1}{5 \cdot 2^5} - \frac{1}{28 \cdot 2^7} - \frac{1}{72 \cdot 2^9} - \ldots\right) \tag{3.7}$$

The astronomer Abraham Sharp (1651–1742), at the suggestion of Halley, the English astronomer and mathematician substituted $x = \sqrt{(1/3)}$ in (3.5) and with this new series calculated π to 72 decimal places in 1699.

In 1705 John Machin derived a new formula to make (3.5) rapidly convergent and easy to calculate. The formula which is named after him is

$$\pi/4 = 4 \arctan\left(\frac{1}{5}\right) - \arctan\left(\frac{1}{239}\right) \tag{3.8}$$

Substituting the Gregory series for the two arctan in (3.8), he obtained

$$\begin{aligned} \pi/4 =& 4\left(\frac{1}{5} - \frac{1}{3 \cdot 5^3} + \frac{1}{5 \cdot 5^5} - \ldots\right) \\ &- \left(\frac{1}{239} - \frac{1}{3 \cdot 239^3} + \frac{1}{5 \cdot 239^5} - \ldots\right) \end{aligned} \tag{3.9}$$

Machin used (3.9) to calculate π with 100 decimal places. Machin's formula and the value calculated for π was published by William Jones in 1706 in his *Synopsis Palmariorum Matheseos* or a New Introduction to Mathematics.

De Lagny (1719) using a new series for arctan

$$\pi/4 = \arctan\left(\frac{1}{2}\right) + \arctan\left(\frac{1}{3}\right) \tag{3.10}$$

calculated 127 decimal places for π (the 113th place has a unit error).

Using the relation (3.10), Euler (1748) finds

$$\pi/4 = \sum_{n\geq 0} \frac{(-1)^n}{(2n+1)\,2^{2n+1}} + \sum_{n\geq 0} \frac{(-1)^n}{(2n+1)\,3^{2n+1}} \tag{3.11}$$

which has a better rate of convergence. Euler denote this formula by π, the symbol which was employed for the first time by Jones (1706) for the circle ratio.

Finally in 1755, using arctan formula, Euler found one that converged much faster than any other:

$$\arctan x = \left(\frac{y}{x}\right)\left(1 + \frac{2}{3}\,y + \frac{2\cdot 4}{3\cdot 5}\,y^2 + \frac{2\cdot 4\cdot 6}{3\cdot 5\cdot 7}\,y^3 + \ldots\right) \tag{3.12}$$

where $y = x^2/(1+x^2)$. Using the Machin-like formula

$$\pi = 20 \arctan\left(\frac{1}{7}\right) + 8 \arctan\left(\frac{3}{79}\right) \tag{3.13}$$

coupled with (3.12) allowed Euler to calculate π to 20 digits in under one hour.

Vega (1794) employed (3.13) in conjunction with (3.5) to compute π to 140 decimal places, of which 136 were correct. Vega's result showed that De Lagny's digits of π had a 7 instead of an 8 in the 113th decimal place. Rutherford (1841) based on Euler's new formula

$$\pi/4 = 4 \arctan\left(\frac{1}{5}\right) - \arctan\left(\frac{1}{70}\right) \arctan\left(\frac{1}{99}\right) \tag{3.14}$$

computed π to 208 decimal places of which 152 were correct.

Dahse (1844) at the age of 20 used the formula due to Strassnitzky

$$\pi/4 = \arctan\left(\frac{1}{2}\right) + \arctan\left(\frac{1}{5}\right) + \arctan\left(\frac{1}{8}\right)$$

to calculate 200 decimal places of π within a period of two months. In 1847 Thomas Clausen employed the formula

$$\pi/4 = 2 \arctan\left(\frac{1}{3}\right) + \arctan\left(\frac{1}{7}\right)$$

to compute 248 decimal places. The same formula was used by Lehmann (1853) to calculate π with 261 decimal places.

Shanks (1853) used Machin's (3.8) formula to calculate π to 607 decimal places, correct to 527 decimal places. Later Shanks (1873a,b) published the extension to 707 decimals carrying with it the errors committed in his book of 1853.

Loney (1893) and Störmer (1896) independently discovered the formula

$$\pi/4 = 3 \arctan\left(\frac{1}{4}\right) + \arctan\left(\frac{1}{20}\right) + \arctan\left(\frac{1}{1985}\right) \tag{3.15}$$

and with this formula, Ferguson (1946) in one of the last hand calculations produced 530 decimal places. Ferguson then discovered a discrepancy between his results and that obtained by Shanks beginning with the 528th decimal place. Ferguson (1946) published Shanks error as a note, and continued his calculation of π to 620 decimal places. Using a desk calculator Smith, Wrench & Ferguson (1946–1947) calculated π to 710 decimals and finally Ferguson & Wrench (1948–1949) reached 808 decimal places.

For a complete history of computation of π from down (2000 B.C.) to 1970 readers are referred to an excellent book on the subject by Beckmann (1977).

3.3 Computer Age

The calculation of π with computer programs started with ENIAC (Electronic Numerical Integrator and Computer) by Reitwiesner (1950). In 70 hours using Machin's formula, Reitwiesner obtained 2037 digits of π. A calculation of π was performed on the NORC (Naval Ordnance Research Calculator) by Nicholson & Jeenel (1955) at the Watson Scientific Computing Laboratory produced 3089 digits. The formula used was the same as that employed for the ENIAC computation in conjunction with the Gregory series (3.4).

The form of the expression used for the NORC computation was

$$\pi/4 = \sum_{n=0}^{\infty} (-1)^n \left[\frac{100(0.2)^{2n+3} - (1/239)^{2n+1}}{2n+1} \right].$$

Felton (1957) reported 10,000 digits in 33 hours on Pegasus Computer at the Ferranti Computer Center in London. He used the relation which was discovered by Klingenstierna in 1730

$$\pi/4 = 8 \arctan\left(\frac{1}{10}\right) - \arctan\left(\frac{1}{239}\right) - 4 \arctan\left(\frac{1}{515}\right). \tag{3.16}$$

The formula (3.16) was rediscovered by Schellbach (1832). A check calculation using formula (3.17) showed that, due to machine error, Felton's result was incorrect after 7480 decimal places.

Genuys (1958) had computed in 100 minutes on IBM 704 using Machin's formula in conjunction with Gregory's series 10,000 digits.

$$\pi = \sum_{k=0}^{\infty} \frac{(-1)^k}{(2k+1)} \left\{ \frac{16}{5^{2k+1}} - \frac{4}{239^{2k+1}} \right\}.$$

Shanks & Wrench (1962) on an IBM 7090 computed 100,000 digits of π in 8 hours and 43 minutes using the formula

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

They checked their findings using Gauss's (1863) formula :

$$\pi = 48 \arctan\left(\frac{1}{18}\right) + 32 \arctan\left(\frac{1}{57}\right) - 20 \arctan\left(\frac{1}{239}\right) \tag{3.17}$$

and according to their report, the 100,000 decimal places are entirely free from error. They also raised the question of computing π to 1,000,000 decimals. Shanks and Wrench proposed to compute $1/\pi$ by Ramanujan's (1914) formula :

$$\frac{1}{\pi} = \frac{1}{4}\left(\frac{1123}{882} - \frac{22583}{882^3}\frac{1}{2} \cdot \frac{1 \cdot 3}{4^2} + \frac{44043}{882^5}\frac{1 \cdot 3}{2 \cdot 4} \cdot \frac{1 \cdot 3 \cdot 5 \cdot 7}{4^2 \cdot 8^2} - \ldots\right). \tag{3.18}$$

Shanks (1982) proposed the formula

$$\pi = \frac{6}{\sqrt{3502}}\left[\log(u) + 4\left(\frac{1}{u^6} - \frac{47}{2u^{12}} + \frac{2488}{3u^{18}} - \frac{138799}{4u^{24}} + \ldots\right)\right]$$

where

$$u = 2 \cdot \left(\frac{1071}{2} + 92\sqrt{34}\right) \cdot \left(\frac{1553}{2} + 133\sqrt{34}\right) \cdot \left(429 + 304\sqrt{2}\right) \cdot \left(\frac{627}{2} + 221\sqrt{2}\right)$$

which gives 79 exact decimals per term calculated.

Mauron (1992) computed the first 1,000,000 digits of π using Leibniz, Machin and Störmer formulas. The complete Computer programs along with the material used for such calculation is provided at the end of the book.

3.4 New Algorithms for π

All algorithms given in the above subsections have an approximately linear convergence to π. This means that n iterations of the algorithm used (that is the calculation of n terms in the chosen expansion for π) give a multiple of n exact digits of π.

Brent (1976) and Salamin (1976) discovered independently an algorithm that has a quadratic convergence to π. This means that the number of correct digits obtained by this algorithm approximately doubles from one iteration to another. This formula is a direct consequence of Gauss' arithmetic-geometric mean and of Legendre's relation for elliptic integrals. The arithmetic geometric mean of two numbers a_0 and b_0 is defined as follows:

$$agm(a_0, b_0) = \lim_{n\to\infty} a_n = \lim_{n\to\infty} b_n$$

where the sequences (a_n) and (b_n) are defined recursively such that

$$a_n = (a_{n-1} + b_{n-1})/2 \text{ and } b_n = \sqrt{a_{n-1} \cdot b_{n-1}}.$$

The formula for π is then the following

$$\pi = \frac{4 \cdot agm^2(a_0, b_0)}{1 - \sum_{j=1}^{\infty} 2^{j+1} c_j^2}$$

where

$$\begin{aligned} a_0 &= 1 \\ b_0 &= 1/\sqrt{2} \\ c_n^2 &= a_n^2 - b_n^2. \end{aligned}$$

Salamin (1976) notes that "it is quite surprising that such an easily derived formula for π has apparently been overlooked for 155 years". The fact is that Gauss in 1818 and Legendre in 1811 had already discovered the necessary results to derive this new formula for π.

To approach π using this formula, we have to calculate

$$\pi_n = \frac{4a_{n+1}^2}{1 - \sum_{j=1}^{n} 2^{j+1} c_j^2}. \tag{3.19}$$

Then π_{19} is correct to over one million digits of π whereas π_{26} to almost 200 million. Kanada & Tamura (1983) used this algorithm to compute π over 16 million decimal digits in less than 30 hours on a Hitachi S-810/20. Using the same formula Kanada (1988) calculated π to 201,326,000 correct decimal places on HITAC S-820/80 in 5 hours and 57 minutes.

Borwein & Borwein (1984) discovered another quadratically convergent algorithm for π which is a refin of the Brent–Salamin formula and can be stated as follows. Let $\alpha_0 = \sqrt{2}$, $\beta_0 = 0$ and

$\pi_0 = 2 + \sqrt{2}$. Then define sequences (α_n), (β_n) and (π_n) such that

$$\begin{aligned} \alpha_{n+1} &= (\sqrt{\alpha_n} + \sqrt{1/\alpha_n})/2 \\ \beta_{n+1} &= \sqrt{\alpha_n} \cdot \frac{\beta_n + 1}{\beta_n + \alpha_n} \\ \pi_{n+1} &= \pi_n \cdot \beta_{n+1} \cdot \frac{1 + \alpha_{n+1}}{1 + \beta_{n+1}}. \end{aligned}$$

Then π_{20} is correct to about 2 million digits of π.

In Borwein & Borwein (1987), Bailey (1988a) and then in Borwein, Borwein & Bailey (1989) we find cubically, quartically and quintically convergent algorithms for $1/\pi$. This means that each iteration triples, quadruples, respectively quintuples the number of correct digits obtained.

Borwein's quartically convergent algorithm for $1/\pi$ can be stated as follows: Let $\alpha_0 = 6 - 4\sqrt{2}$ and $y_0 = \sqrt{2} - 1$. Iterate

$$y_{n+1} = \frac{1 - \left(1 - y_n^4\right)^{1/4}}{1 + \left(1 - y_n^4\right)^{1/4}}$$

and

$$\alpha_{n+1} = (1 + y_{n+1})^4 \alpha_n - 2^{2n+3} y_{n+1} \left(1 + y_{n+1} + y_{n+1}^2\right)$$

then

$$0 < \alpha_n - 1/\pi < 16 \cdot 4^n e^{-2 \cdot 4^n \pi}$$

and α_n converges to $1/\pi$ quartically. Each successive iteration approximately quadruples the number of correct digits in the result. It is with the quartically convergent algorithm that Bailey (1988b) computes π to 29,360,000 decimals in about 40 hours on a Cray-2.

On July 28th, 1995, the program of Takahashi, a member of Kanada Laboratory used HITAC S-3800/480 at the Computer Centre, University of Tokyo, to compute 4,294,697,296 ($= 2^{32}$) decimal digits of π with Borwein's 4th order convergent algorithm. The verification program started on August 11, 1995 at 21:31 and ended on 14th August, 1995 at 15:54 using Gauss–Legendre algorithms. On September 24th, 1995, the same group of Tokyo under the leadership of Kanada used Borwein's 4th order convergent algorithm with Gauss–Legendre algorithm for verification on October 6th, 1995 calculated π to 6,442,450,938 ($=3 \cdot 2^{31}$) decimal digits. It is the actual world record.

Borwein's quintically convergent algorithm for $1/\pi$ is the following: Let $s_0 = 5\left(\sqrt{5} - 2\right)$ and $\alpha_0 = 1/2$. Iterate

$$s_{n+1} = \frac{25}{(z + x/z + 1)^2 s_n},$$

where

$$x = 5/s_n - 1, \quad y = (x - 1)^2 + 7$$

and

$$z = \left[\frac{1}{2} x \left(y + \sqrt{y^2 - 4x^3}\right)\right]^{1/5}$$

Iterate

$$\alpha_{n+1} = s_n^2 \cdot \alpha_n - 5^n \left\{\frac{s_n^2 - 5}{2} + \sqrt{s_n \left(s_n^2 - 2s_n + 5\right)}\right\}$$

Then

$$0 < \alpha_n - \frac{1}{\pi} < 16 \cdot 5^n e^{-5^n \pi}$$

and α_n converges to $1/\pi$ quintically. Each additional iteration of the algorithm quintuples the number of correct digits. To obtain around one billion digits of π requires just thirteen iterations of the algorithm.

More recently, Bailey, Borwein & Plouffe (1995) discovered an algorithm that is able to compute the d-th hexadecimal digit of π without computing all precedent digits (but the convergence is only linear). It is based on the new formula

$$\pi = \sum_{n=0}^{\infty} \left(\frac{1}{16^n}\right)\left(\frac{4}{8n+1} - \frac{2}{8n+4} - \frac{1}{8n+5} - \frac{1}{8n+6}\right)$$

4 Statistical studies on π

The calculation of the decimal digits of π may have had many different reasons since the early efforts of the Babylonians and Egyptians. For most applications computing few decimals is enough. The major motivation behind computation of π in modern time concern the normality (see Section 4.2) or randomness of its digits. The extended precision calculation is also used to detect hardware errors. Large scale calculations of π are now used routinely as a quality control to check super-computers before leaving the factory.

In this section we provide a summary of statistical tests that have been applied to decimals of π in order to investigate their randomness. First we consider empirical statistical tests and later a theoretical aspect of the randomness of digits of π is discussed.

4.1 Empirical Statistical Tests

The null hypothesis is H_0: "The sequence is a sample of i.i.d. U(0,1) random variables", and a statistical test tries to find empirical evidence against this hypothesis. If a generator passes all existing empirical statistical tests, it does not imply that it will not fail the future one. However, researchers who use random numbers like to find generators that pass with high probability all the existing statistical tests in some reasonable CPU time.

Kendall & Babington-Smith (1938) suggested four tests for deciding whether a given set of digits is locally random. These are, the frequency test, serial test, poker test and gap test. The authors, however, warn the reader that these tests are not sufficient to establish the existence of local randomness, although they are necessary.

Kendall & Babington-Smith (1939a) were first to raise the random nature of π's decimals but at that time, the number of known decimals of π was not enough to be used as such.

For testing the hypothesis that the empirical frequencies of n-long strings of digits are random the χ^2 test is used. The χ^2 statistic is defined to be

$$\chi^2 = \sum_{i=1}^{k} \frac{(O_i - E_i)^2}{E_i}$$

where O_i and E_i are the observed and the expected value of the random variable respectively.

Metropolis, Reitwiesner & von Neumann (1950) carried out a statistical treatment of values of first 2000 decimal digits of e and π by studying the frequency distribution of the various digits (0,1,2,.....,9) calculated on the ENIAC by Reitwiesner (1950). Using the χ^2 test, they concluded that the first 2000 digits of e have no random character (too good to be true) but their survey failed to disclose any significant deviations from randomness for π.

Greenwood (1955) found that the coupon-collector test was satisfied by the first 2035 digits in the decimal expansion of π given by Reitwiesner (1950). This study was extended to about 3000 decimal places by Nicholson & Jeenel (1955).

Wrench (1960) used a χ^2 test for goodness of fit on 16,167 (16,000 were tabulated and tested) decimal digits of π and found no abnormal behaviour in the distribution of digits. He also raised the question of normality of π.

Pathria (1962) made statistical study of randomness among the first 10,000 digits of π computed by Genuys (1958). By applying the frequency test, serial test, poker test and the gap test of Kendall & Babbington-Smith (1938) as well as Yule (1938), the five-digit sum test, he reported that, the first 10,000 digits of π are in fact random.

Esmenjaud-Bonnardel (1965) reports the result of four statistical tests on the first 100,000 digits of π calculated by Shanks & Wrench (1962). She also gives the results of tests applied to the first 100,000 digits of the table published by RAND Corporation (1955). Her final conclusion is that, the use of the first 100,000 digit decimals of π as random numbers is perfectly justifiable.

Lauro (1972) also studies the decimals of π and arrives at the same conclusion as Esmenjaud-Bonnardel.

Bailey (1988b) calculated 29,360,000 digits of π and provides the frequencies of n-long string for randomness up to $n = 6$. The results of Bailey's frequencies for one digit strings is given in Table 1 along with the standardized normal deviates or z-score. Based on three statistical tests, namely the frequency test, the serial test and the run test he concluded that the decimal expansion of π appears to be completely random.

Table 1

Single digit statistics on 29,360,000 decimals of π (source: Bailey, 1988b)

Digit	Count	Deviation	z-score
0	2,935,072	-928	-0.5709
1	2,936,516	516	0.3174
2	2,936,843	843	0.5186
3	2,935,205	-795	-0.4891
4	2,938,787	2787	1.7145
5	2,936,197	197	0.1212
6	2,935,504	-496	-0.3051
7	2,934,083	-1917	-1.1793
8	2,935,698	-302	-0.1858
9	2,936,095	95	0.0584

Johnson & Leeming (1990) examine the first 100,000 digits in the decimal expansion of π, e, $\sqrt{2}$, $\sqrt{3}$, $\sqrt{5}$, $\sqrt{7}$, $\sqrt{11}$, and $\sqrt{13}$ for properties of randomness based on several different runs statistics. They showed that both π and $\sqrt{7}$ achieved higher randomness ratings than the best of 10 independent 100,000-digit runs from each of the two random number generator routines, namely URAND and C05DYF.

Kanada (1988, 1995) provides summary of frequency for the first 6,000,000,000 digits of π as well as of the corresponding χ^2 values (see Table 2 and Figure 1). It is remarkable to note that none

of the χ^2 values are significative up to a level of 20% and hence the decimal places up to 6 billions have not disclosed any irregularity.

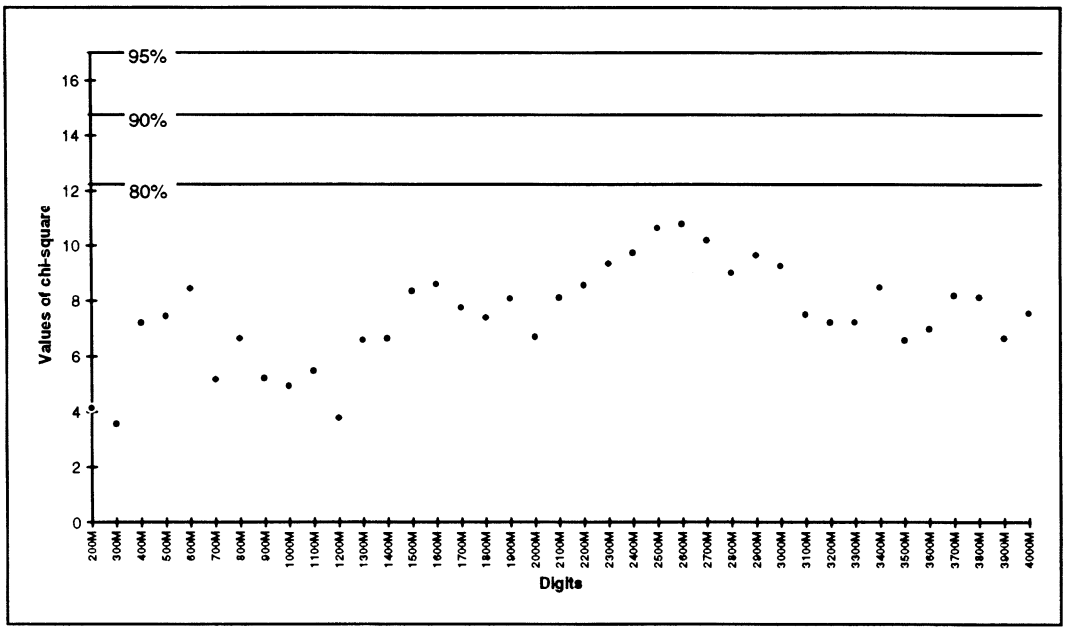

Figure 1. *Plot of the calculated χ^2 values for the first 4 billions digits of π*

As a conclusion of the above empirical studies on decimals of π we can cite Gardner (1966, p.99): "So far π has passed all statistical tests for randomness. This is disconcerting to those who feel that a curve so simple and beautiful as the circle should have a less-disheveled ratio between the way around and the way across, but most of mathematicians believe that no pattern or order of any sort will ever be found in π's decimal expansion."

4.2 Does π Satisfy All Statistical Tests?

What if you slept? And what if, in your sleep, you dreamed? And what if, in your dream, you went to heaven and there plucked a strange and beautiful flower? And what if, when you awake, you had the flower in your hand? Ah, what then?

Samuel Coleridge (1772–1834)
English Poet and Philosopher

The nature of π has been studied by mathematicians since the middle of the eighteenth century to present day. Lambert (1771) proved the irrationality of π by means of continued fractions and Lindemann (1882) established its transcendence. (The Lindemann result showed that squaring the circle is impossible).

A question which arises now is whether there is an alternative way to prove that the digits of π are really random, with arguments other than empirical considerations. It is very difficult to answer this question because the concept of randomness is not well defined. Knuth (1981) in Section 3.5 entitled "What is a random sequence?" tries to make it precise. It appears that the concept of "randomness" for

Table 2

Summary of frequency for the first 6,000,000,000 digits of π and corresponding chi-square values (source: Kanada, 1988, 1995)

Digits	0	1	2	3	4	5	6	7	8	9	χ^2
1-100	8	8	12	11	10	8	9	8	12	14	4.20
1-500	45	59	54	50	53	50	48	36	53	52	6.88
1-1K	93	116	103	102	93	97	94	95	101	106	4.74
1-10K	968	1026	1021	974	1012	1046	1021	970	948	1014	9.32
1-50K	5033	5055	4867	4947	5011	5052	5018	4977	5030	5010	5.86
1-100K	9999	10,137	9908	10,025	9971	10,026	10,029	10,025	9978	9902	4.09
1-500K	49,915	49,984	49,753	50,000	50,357	50,235	49,824	50,230	49,911	49,791	7.73
1-1M	99,959	99,758	100,026	100,229	100,230	100,359	99,548	99,800	99,985	100,106	5,51
1-10M	999,440	999,333	1,000,306	999,964	1,001,093	1,000,466	999,337	1,000,207	999,814	1,000,040	2.78
1-20M	2,001,162	1,999,832	2,001,409	1,999,343	2,001,106	2,000,125	1,999,269	1,998,404	1,999,720	1,999,630	4.17
1-30M	2,999,157	3,000,554	3,000,969	2,999,222	3,002,593	2,999,997	2,999,548	2,998,175	2,999,592	3,000,193	4,34
1-50M	4,999,632	5,002,220	5,000,573	4,998,630	5,004,009	4,999,797	4,998,017	4,998,895	4,998,494	4,999,733	6.17
1-100M	9,999,922	10,002,475	10,001,092	9,998,442	10,003,863	9,993,478	9,999,417	9,999,610	10,002,180	9,999,521	7.27
1-200M	19,997,437	20,003,774	20,002,185	20,000,410	19,999,846	19,993,031	19,999,161	20,000,287	20,002,307	20,000,562	4.13
1-3000M	299,999,143	299,995,932	299,989,126	299,992,290	300,002,257	299,979,016	300,025,447	299,975,510	300,016,550	300,024,729	9.24
1-6000M	599,963,005	600,033,260	599,999,169	600,000,243	599,957,439	600,017,176	600,016,588	600,009,044	599,987,038	600,017,038	9.00

a sequence formed by the digits of a real number is not so far away from the concept of "normality" of this number (see also Wagon, 1985).

A number is said to be normal in base 10 if all digits 0,1,...,9 appear with equal frequency in its decimal expansion, as well as all blocks of digits of the same length. A number is then said to be (absolutely) normal if this statement is true whatever the base chosen to write its digits. Such a number has effectively the remarkable particularity that the sequence of its digits satisfy all known statistical tests for randomness such as those presented above (see Knuth, 1981, pp.151–152).

Borel (1909) proved that almost all irrational numbers (in the sense of Lebesgue measure) are normal (see also Franklin, 1963 and Levin, 1975). The probability that π is normal is hence equal to one. Thus, as shown in Dodge & Rousson (1996), "A random sequence formed by the digits of π will satisfy all statistical tests of randomness with probability one". And "A random sequence formed with the help of any artificial algorithm will satisfy all these tests with probability zero".

Following Robert R. Coveyou's (1969) famous article entitled "Random number generation is too important to be left to chance" which is cited in numerous papers and books on random number generators, we suggest to replace the 1,000,000 random numbers published by the RAND Corporation (1955) by the 1,000,000 first decimals of π that can be found in Mauron (1992)! We also suggest to store on a CD-ROM some billions of decimals of π to be used as a natural random number generator which leaves no space for chance.

Acknowledgments

The author wishes to express his gratitute to Olivier Besson, David Cox, Pierre L'Ecuyer, Peter Huber, Yasumasa Kanada, Thierry Murier, Simon Plouffe, Valentin Rousson, Guenther Sawtzki and Joe Whittaker for their generous and kind help.

References

Bailey, D.H. (1988a). Numerical Results on the Transcendence of Constants Involving π, e, and Euler's Constant. *Math. Comp.*, **50**, 275–281.

Bailey, D.H. (1988b). The Computation of π to 29,360,000 Decimal Digits Using Borweins' Quartically Convergent Algorithm. *Math. Comp.*, **50**, 283–96.

Bailey, D., Borwein, P. & Plouffe, S. (1995). On the Rapid Computation of Various Polylogarithmic Constants. [to appear].

Beckmann, P. (1977). *A History of Pi.* Golem Press, Boulder, Colorado, 4th Edition.

Borel, E. (1909). *Rend. Circ. Mat. Palermo*, **27**, 247–271.

Borwein, J.M. & Borwein, P.B. (1984). The Arithmetic-Geometric Mean and Fast Computation of Elementary Functions. *SIAM Rev.*, **26**, 351–365.

Borwein, J.M. & Borwein, P.B. (1987). *Pi and the AGM - A Study in Analytic Number Theory and Computational Complexity.* New York: John Wiley.

Borwein, J., Borwein, P. & Bailey, D.H. (1989). Ramanujan, Modular Equations and Approximations to pi. *Amer. Math. Monthly*, **96**, 201–219.

Brent, R.P. (1976). Fast Multiple-Precision Evaluation of Elementary Functions. *J. ACM*, **23**, 242–251.

Chabert, J.-C., Barbin, E., Guillemot, M., Michel-Pajus, A., Borowczyk, J., Djebbar, A. & Martzloff, J.-C. (1994). *Histoire d'algorithmes, du caillou à la puce.* Paris: Belin. Chapitre 5.

Coveyou, R.R. (1969). Random Number Generation is too Important to be Left to Chance. *Appl. Math.*, **3**, 70–111.

Dahse, Z. (1964). Der Kreis-Umfang für den Durchmesser 1 auf 200 Decimalstellen berechnet. *Journal für die reine und angewandte Mathematik*, 281–283.

De Lagny, T.-G. (1719). *Mémoire sur la quadrature du cercle. Histoire de l'Académie Royale des Sciences*, Paris, 135–145.

Dodge, Y. & Rousson, V. (1996). Does π Satisfy all Statistical Tests? *Technical Report*, **96-2**, Statistics Group, University of Neuchâtel.

Euler, L. (1748). *Introductio in analysin infinitorum.* Paris: Lausanne, trad. J.-B. Labey.

Esmenjaud-Bonnardel, M. (1965). Etude statistique des décimales de pi. *Chiffres*, **8**, 295–306.

Felton, G.E. (April 8–18, 1957). Electronic Computers and Mathematicians. *Abbreviated Proceedings of the Oxford Mathematical Conference for Schoolteachers and Industrialists at Trinity College, Oxford,* 12–17, footnote 12–53.

Ferguson, D.F. (1946). Value of π. *Nature*, **157**, 342. See also D.F. Ferguson (1946). Evaluation of π. Are Shanks' Figures Correct? *Mathematical Gazette*, **30**, 89–90.

Ferguson, D.F. & Wrench, J.W., Jr. (1948–1949). A New Approximation to π (conclusion). *Mathematical Tables and other Aids to Computation*, **3**, 18–19. See also R. Liénard (1948). Constantes mathématiques et système binaire. *Intermédiaire des Recherches Mathématiques*, **5**, 75.

Fisher, R.A. & Yates, F. (1938). *Statistical Tables for Biological, Agricultural and Medical Research.* Oliver and Boyd. 1st ed. (6th ed. 1963).

Franklin, J.N. (1963). Deterministic Simulation of Random Processes. *Math. Comp.*, **17**, 28–59.

Gardner, M. (1966). *New Mathematical Diversions from Scientific American*. New York: Simon and Schuster.

Gauss, C.F. (1863; 2nd ed., 1876, 2, 499–502). Göttingen: Weke.

Genuys, F. (1958). Dix milles décimales de π. *Chiffres*, **1**, 17–22.

Greenwood, R.E. (1955). Coupon Collector's Test for Random Digits. M.T.A.C. **9**, 1–5. (Errata in *M.T.C.A.* (1955), **9**, 224 and 229).

Johnson, B. & Leeming, D. (1990). A study of the digits of π, e, and certain other irrational numbers. *Sankhya*, **52**, 183–189.

Jones, W. (1706). *Synopsis Palmariorum Matheseos*. London, 263.

Kanada, Y. (1988). *Vectorization of Multiple-Precision Arithmetic Program and 201,326,000 Decimal Digits of π Calculation.* Reprinted from Supercomputing, 1988, volume 2, science and applications.

Kanada, Y. (1995). Internet address: ftp.www.cc.u-tokyo.ac.jp.

Kanada, Y. & Tamura, Y., preprint (1983). Calculation of π to 4,196,393 Decimals Based on Gauss-Legendre Algorithm.

Kendall, M.G. & Babington-Smith, B. (1938). Randomness and Random Sampling Numbers. *R. Stat. Soc.* A, **101**, 147–166.

Kendall, M.G. & Babington-Smith, B. (1939a). Second Paper on Random Sampling Numbers. *R. Stat. Soc.* B, supplement **6**, 51–61.

Kendall, M.G. & Babington-Smith, B. (1939b). A table of Random Sampling Numbers. Tracts for Computers no. 24, C.U.P.

Knuth, D. (1981). *The Art of Computer Programming, Seminumerical Algorithms*, volume 2, Reading, Mass: Addison-Wesley, 2nd edition.

Lambert, J.H. (1771). Sur quelques propriétés remarquables des quantités transcendantes circulaires et logarithmiques. *Mémoires de l'Académie de Berlin, t.* **17**, 265–322; *Mathematische Werke, t.* **II**, 112–159.

Lauro, N. (1972). Sulla distribuzione statistica delle cifre decimale di π. *Studi Economici, Giannini, Napoli*, 77–93.

L'Ecuyer, P. (1994). Uniform Random Number Generation. *Annals of Operations Research*, **53**, 77–120.

L'Ecuyer, P. & Cordeau, J.-F. (1996). Tests sur les points rapprochés pour des générateurs pseudo-aléatoires. *ASU* **96**, 479–482.

Legendre, A.M. (1811). Exercices de calcul intégral, Vol. 1.

Lehmann, W. (1853). Beitrag zur Berechnung der Zahl π welche das Verhältniss des Kreis-Durchmessers zum Umfang ausdrückt. *Archiv des Mathematic und Physik*, **21**, 121–174.

Lehmer, D.H. (1951). Mathematical Methods in Large Scale Computing Units. *Annals Comp. Lab. Harvard*, **26**, 141–146.

Leibniz, G.-W. (1682). De vera proportione circuli ad quadratum circumscriptum in numeris rationalibus, Acta eruditorum. Mathematische Schriften, t. V, 118–122, Olms, Hildesheim, 1962. Trad. Marc Parmentier, (1989) : Expression en nombres rationnels de la proportion exacte entre un cercle et son carré circonscrit, in Leibniz, Naissance du calcul différentiel, Vrin, Paris.

Levin, L.A. (1975). On the Uniform Distribution of the Sequence $\{\alpha\lambda^x\}$. *Mat. Sb. (N.S.)*, **98**, 207–222 = *Math. USSR-Sb.*, **27**, 183–197.

Lindemann, F. (1882). Über die Zahl π. *Mathematische Annalen*, **20**, 213–225.

Loney, S.L. (Cambridge, 1893). Plane Trigonometry, 277.

Mauron, C, (1992). π. Fribourg, Switzerland: Mauron and Lachat.

Metropolis, N., Reitwiesner, G. & von Neumann, J. (1950). Statistical Treatment of Values of First 2000 Decimals Digits of e and π, Calculated on ENIAC. *M.T.A.C.* **4**, 109–111.

von Neumann, J. (1951). Various Techniques Used in Connection with Random Digits. In the *Monte Carlo Method* (ed. A.S. Householder et al., 36–38). *Nat. Bur. Standards Appl. Math Ser.* no. **12**.

Nicholson, S.C. & Jeenel, J. (1955). Some Comments on a NORC Computation of π. *Mathematical Tables and other Aids to Computation*, **9**, 162–164.

Niederreiter, H. (1978). Quasi-Monte Carlo Methods and Pseudorandom Numbers. *Bulletin of the math. society*, **84**, 957–1041.

Pathria, R.K. (1962). A Statistical Study of Randomness Among the First 10,000 Digits of π. *Math. Comp.*, **16**, 188–197. (Comment by Pathria, R.K. (1961), *Mathematical Gazette*, **45**, 142–143).

Peatman, J.G. & Shafer, R. (1942). A Table of Random Numbers from Selective Service Numbers. *J. of Psychology*, **14**, 295–305.

Ramanujan, S. (1914). Modular Equations and Approximations to π. *Quart. J. Math*, **45**, 350–72; Collected papers of Srinivasa Ramanujan, Cambridge, 1927, 23–39.

RAND Corporation (1955). *A Million Digits with 100,000 Normal Deviates*. Glencoe Free Press.

Reitwiesner, G. (1950). An ENIAC Determination of π and e to more than 2000 Decimal Places. *M.T.A.C.*, **4**, 11–15.

Ripley, B.D. (1987). Stochastic Simulation. New York: John Wiley.

Ripley, B.D. (1990). Thoughts on Pseudorandom Number Generators. *J. Comput. Appl. Math.*, **31**, 153–163.

Royo, J. & Ferrer, S. (1954a). Tables of Random Numbers Obtained from Numbers in the Spanish National Lottery. (In Spanish). *Trabajos de Estadistica*, **5**, 247–256.

Royo, J. & Ferrer, S. (1954b). A Table of Random Numbers (In Spanish). In their *Tablas Estadisticas*, 3–127. Instituto de Investigaciones Estadisticas, Madrid.

Rubinstein, R.Y. (1981). *Simulation and the Monte Carlo Methods*, New York: John Wiley.

Rutherford, W. (1841). Computation of the Ratio of the Diameter of a Circle to its Cirumference to 208 places of figures. *Philosophical Transactions of the Royal Society of London*, **131**, 281–283.

Salamin, E. (1976). Computation of π Using Arithmetic-Geometric Mean. *Math. Comp.*, **30**, 565–570.

Schellbach, K.H. (1832). Ueber den Ausdruck $\pi = (2/i) \log i$. *Journal für die reine und angewandte Mathematik*, **9**, 404–406.
Shanks, W. (1853). *Contributions to Mathematics Comprising Chiefly of the Rectification of the Circle to 607 Places of Decimals*, London: G. Bell.
Shanks, W. (1873a). On the Extension of the Numerical Value of π. *Proceedings of the Royal Society of London*, **21**, 318.
Shanks, W. (1873b). On Certain Discrepancies in the Published Numerical Value of π. *Proceedings of the Royal Society of London*, **22**, 45–46.
Shanks, D. & Wrench, J.W., Jr. (1962). Calculation of π to 100,000 Decimals Mathematics of Computation, **16**, 76–79.
Shanks, D. (1982). Dihedral Quadratic Approximation and Series for π. *Journal of Number Theory*, **14**, 397–423.
Smith L.B., Wrench, J.W., Jr. & Ferguson, D.F. (1946–1947). A New Approximation to π. *M.T.A.C.*, **2**, 245–248.
Sowey, E.R. (1972). A Chronological and Classified Bibliography on Random Number Generation and Testing. *Int. Stat. Rev.*, **40**, 355–371.
Sowey, E.R. (1978). A Second Classified Bibliography on Random Number Generation and Testing. *Int. Stat. Rev.*, **46**, 89–102.
Steinhaus, H. (1954). Table of Shuffled Fourdigit Numbers. (In Polish, Russian and English). *Rozprawy Matematyczne*, **6**, 1–46. (Lehmer D.H. (1954). *Math. Reviews*, **15**, 636).
Störmer, C. (1896). Sur l'application de la théorie des nombres entiers complexes à la solution en nombres rationnels x_1, x_2, ..., x_n, c_1, c_2,..., c_n, k de l'équation c_1, arctg x_1+c_2 arctg x_2 +....+ c_n arctg $x_n = k_\pi/4$. *Archiv for Mathematik og Naturvidenskab*, **19**, 70.
Tannery, P. (1893). *Recherches sur l'histoire de l'astronomie ancienne*. Paris, 64–66.
Tezuka, S. (1995). *Uniform Random Numbers: Theory and Practice*. Boston: Kluwer Academic Publishers.
Tippett, L.H.C. (1927). *Random Sampling Numbers*. Tracts for Computers no. 15, C.U.P. (Reprinted 1952).
Vega, G. (1794). *Thesaurus Logarithmorum Completus*. Leipzig, 633. (Reprinted by G.E. Strechert & Co., New York, 1946).
Viète, Fr. (1593). *Variorum de rebus mathematicis responsorum*, Liber VIII, Tours. *Opera Mathematics*, Leyde, 1646.
van der Waerden, B.L. (1983). *Geometry and Algebra in Ancient Civilization*. Berlin: Springer-Verlag.
Wagon, S. (1985). Is π Normal? *The Math Intelligencer*, **7**, 65–67.
Wallis, J. (1656). *Arithmetica Infinitorum Oxford*. Opera Mathematics, Oxford, 355–478.
Wrench, J.W., Jr. (1960). The Evolution of Extented Decimal Approximation to π. *The Mathematics Teacher*, **53**, 644–650.
Yule, G.U. (1938). A Test of Tippett's Random Numbers, *R. Stat. Soc.* A, **101**, 167–172.

Résumé

Depuis l'introduction en 1949 par John von Neumann de la méthode "middle-square" pour générer des nombres "pseudo-aléatoires", des centaines d'autres méthodes ont été proposées. Bien que chacune d'entre elles présente quelques avantages, aucune n'émerge réellement du lot. Le problème de trouver un générateur uniformément supérieur aux autres est rendu difficile par les nombreuses propriétés qu'un tel générateur se doit de satisfaire comme de n'avoir pas de comportement cyclique et de passer avec succès les nombreux test statistiques. Le but de cet article est de suggérer comme source de nombres aléatoires celui qui nous paraît le plus naturel d'entre tous, les décimales de π. Aucun cycle n'y a encore été décelé et les distributions de toute séquence finie de décimales sont uniformes de telle sorte que ce générateur satisfait tous les tests actuels. Il est d'ailleurs conjecturé qu'il satisfera tout autre test avec probabilité un. De plus, l'histoire de π, de sa découverte et de ses approximations successives est en rapport étroit avec l'histoire de l'humanité.

[*Received June 1996, accepted July 1996*]