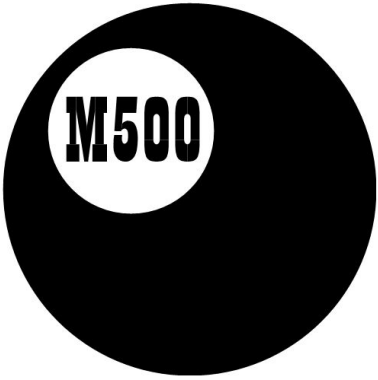
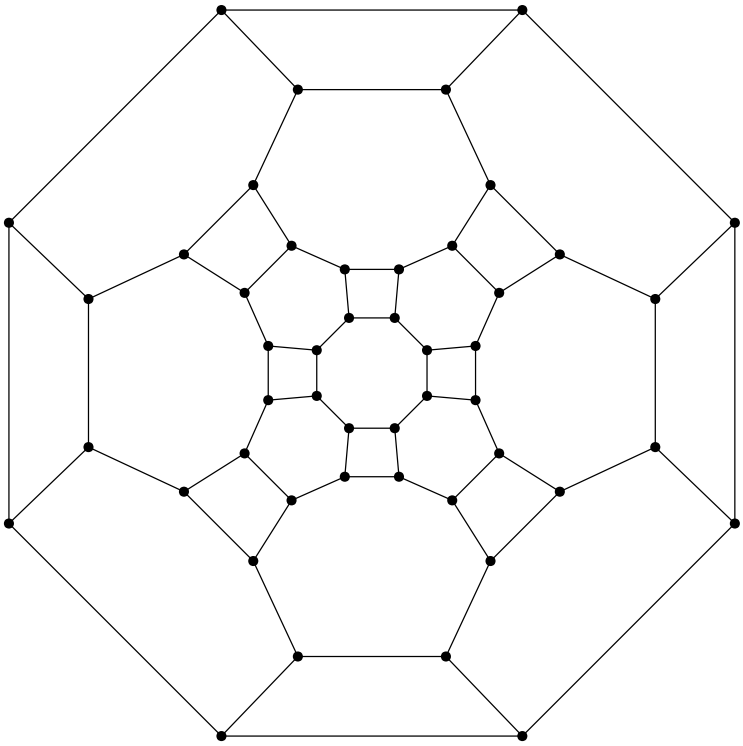
*

ISSN 1350-8539



M500 269



The M500 Society and Officers

The M500 Society is a mathematical society for students, staff and friends of the Open University. By publishing M500 and by organizing residential weekends, the Society aims to promote a better understanding of mathematics, its applications and its teaching. Web address: m500.org.uk.

The magazine M500 is published by the M500 Society six times a year. It provides a forum for its readers' mathematical interests. Neither the editors nor the Open University necessarily agree with the contents.

The Revision Weekend is a residential Friday to Sunday event providing revision and examination preparation for both undergraduate and postgraduate students. For full details and a booking form see m500.org.uk/may.

The Winter Weekend is a residential Friday to Sunday event held each January for mathematical recreation. For details see m500.org.uk/winter.htm.

Advice to authors We welcome contributions to M500 on virtually anything related to mathematics and at any level from trivia to serious research. Please send material for publication to the Editor, above. We prefer an informal style and we usually edit articles for clarity and mathematical presentation.

Problem 269.1 – Random sequences

Tony Forbes

The Erdős Discrepancy Conjecture, which was proved by Terence Tao in September 2015, states that for any function $F : \{1, 2, \dots\} \to \{-1, 1\}$,

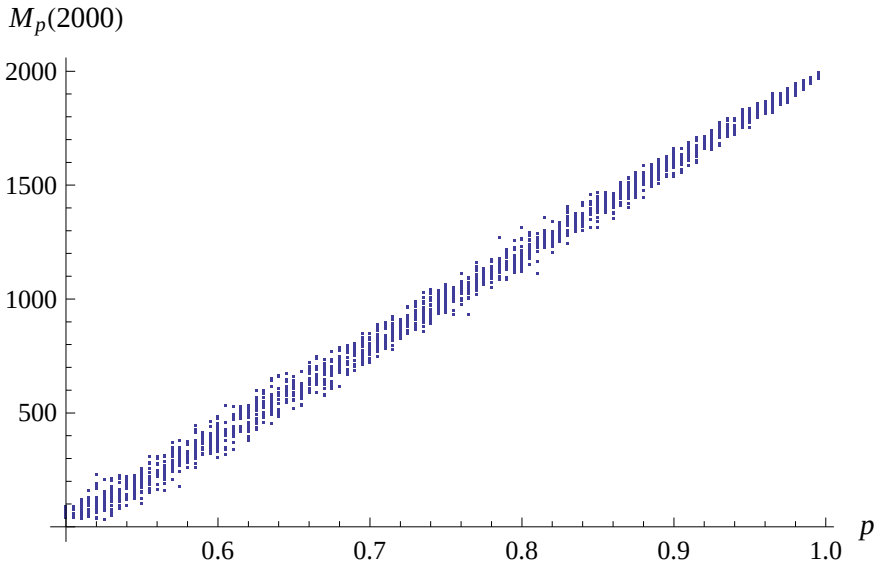
$$\sup_{n,d\ge 1} \left| \sum_{j=1}^{n} F(jd) \right| \;=\; \infty.$$

See, for example, http://www.theoremoftheday.org, number 209.

However, we are concerned with finite sequences. Let N be a (large) positive integer and let $p \in [0.5, 1]$. Let $S_p(i)$, $i = 1, 2, \dots, N$ be a random sequence of $\{-1, 1\}$ such that $S_p(i) = 1$ with probability p. Compute

$$\mathbb{E}[M_p(N)], \quad \text{where} \quad M_p(N) \;=\; \max_{1\le d\le N,\ 1\le n\le N/d} \left| \sum_{j=1}^{n} S_p(jd) \right|.$$

I believe the problem might be doable. In the graph we compute $M_p(2000)$ for 20 random sequences S_p for each of various values of p. What is the relationship between p and $\mathbb{E}[M_p(N)]$?



Solution 267.1 – Trigonometric integral

Compute $\displaystyle\int_0^1 \arcsin\cos\sin\arccos x\,dx$.

John Davidson

Noting the result for $0 \le x \le 1$: $\arccos x = \arcsin\sqrt{1-x^2}$, we have

$$\begin{aligned}
&\sin\arccos x = \sqrt{1-x^2} \\
&\quad\Rightarrow\ \cos\sin\arccos x = \cos\sqrt{1-x^2} = \sin\left(\frac{\pi}{2} - \sqrt{1-x^2}\right) \\
&\quad\Rightarrow\ \arcsin\cos\sin\arccos x = \frac{\pi}{2} - \sqrt{1-x^2} \\
&\quad\Rightarrow\ \int_0^1 \arcsin\cos\sin\arccos x\,dx = \int_0^1 \left(\frac{\pi}{2} - \sqrt{1-x^2}\right) dx \\
&\qquad\qquad\qquad\qquad = \frac{\pi}{2} - \int_0^1 \sqrt{1-x^2}\,dx \qquad (1)
\end{aligned}$$

As a standard integral or by the substitution $x = \sin\theta$, it is readily shown that

$$\int \sqrt{1-x^2}\,dx \;=\; \frac{1}{2}\left(\arcsin(x) + x\sqrt{1-x^2}\right);$$

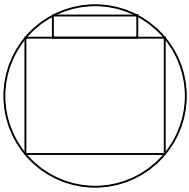
so from equation (1),

$$\int_0^1 \arcsin\cos\sin\arccos x\,dx \;=\; \frac{\pi}{2} - \frac{1}{2}\left[\arcsin(x) + x\sqrt{1-x^2}\right]_0^1 \;=\; \frac{\pi}{4}.$$

Similarly, it is readily shown that

$$\int_0^1 \arccos\sin\cos\arcsin x\,dx \;=\; \frac{\pi}{4}.$$

Problem 269.2 – Two rectangles

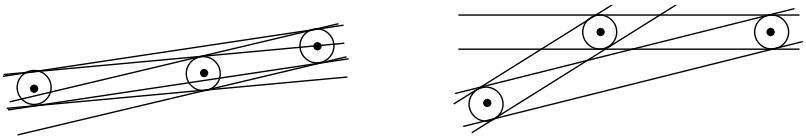


Tony Forbes

Two rectangles are packed inside a circle of radius 1. What is the largest area they can occupy?

Problem 269.3 – Three in a line

There are N circles of radius r distributed at random in a 1×1 square. Assuming r is small, say $r \ll 1/N^2$, what is the probability that there exist three circles that are approximately aligned? Three circles are *approximately aligned* if there are two of them, C_1 and C_2, say, such that the centre of the third circle lies between the two parallel lines that are simultaneously tangent to both C_1 and C_2. For example the circles on the left, below, are approximately aligned but not the three on the right.



Problem 269.4 – Three-sided dice

Is it possible to make a three-sided die. Can it be done for any odd number of sides?

We leave it for your imagination to decide exactly what constitutes a valid die. However, we insist that the probabilities of landing on the various sides must be calculable. And to save time, let us rule out blatant forms of cheating—such as a cube with the faces numbered in pairs. Thanks to Mike Lewis for suggesting this problem.

Problem 269.5 – Coins

Simplify

$$\sum_{i=0}^{n} |n-2i| \binom{n}{i},$$

where n is a positive integer. Hence or otherwise determine

$$\lim_{n\to\infty} \frac{1}{\sqrt{n}}\, \mathbb{E}[\Delta(n)], \qquad \text{where} \qquad \mathbb{E}[\Delta(n)] \;=\; \frac{1}{2^n} \sum_{i=0}^{n} |n-2i| \binom{n}{i}.$$

Coin tossers might recognise $\mathbb{E}[\Delta(n)]$ as the expected value of the discrepancy (i.e. $|(\text{number of heads}) - (\text{number of tails})|$) resulting from randomizing the orientations of n coins. Thanks to Nigel Phillips for suggesting this problem.

Problem 269.6 – Cos pi over seven

John Davidson

We know that $\cos(\pi/n)$ has a nice, simple form when $n = 1$, 2, 3, 4, 5 and 6. What about 7? Find an expression for $\cos(\pi/7)$.

Problem 269.7 – Matches

Tony Forbes

Players A and B initially have a and b matches respectively and proceed to play a sequence of games, which we will refer to as the match. In each game, A wins with probability p, B wins with probability $1 - p$ and loser transfers one match to the winner. The match ends when a player runs out of matches; the winner is the other player. (The matches have no value and are used merely as tokens.) What value must p have to ensure that each player has the same chance of winning the match? For example, when $a = b$ it is clear that the players are evenly matched if $p = 1/2$.

A simple lever

Eddie Kent

Archimedes is reported by Pappus of Alexandria in his *Collection* to have said to Hiero II "Give me but one firm spot on which to stand and I will move the earth." He was talking about levers, of course, as every schoolboy used to know. But did he—Archimedes or the schoolboy—ever stop to consider how long it would take to move the earth?

We (that is, Jacques Ozanam, *Recreations in Science and Natural Philosophy*, p. 202 and I) make the standard assumptions: that any machine used would be frictionless, without mass, and in complete equilibrium, and that the earth weighs 300 pounds per cubic foot, and is spherical with a diameter of 7930 miles.

Suppose that Archimedes is able to maintain an effort of 30 pounds sustained for eight hours at a stretch, moving at 10,000 feet an hour. A law of mechanics states that for any machine 'The space passed over by the weight is to that passed over by the moving power in the reciprocal ratio of the latter to the former.'

Thus a simple calculation shows that by the time the earth has travelled one inch the moving power has passed over 384 343 863 875 439 367 148 379 inches, which would take 3 202 865 532 295 328 060 hours, or 3 653 736 632 780 centuries. But we have agreed he should work no more than eight hours without rest. Also he ought to have weekends off, and an annual holiday; one wouldn't want him growing stale. To get the job finished, therefore, we ought to allocate him twelve trillion centuries. That should be ample time.

Perrin's sequence

Roger Thompson

1. Introduction

Perrin's sequence is defined by $a(0) = 3$, $a(1) = 0$, $a(2) = 2$, $a(n + 3) = a(n+1)+a(n)$ for $n \geq 0$. Calculating a few more values, we get the following.

n	$a(n)$	n	$a(n)$
0	3	16	90
1	$0 = 0 \times 1$	17	$119 = 7 \times 17$
2	$2 = 1 \times 2$	18	158
3	$3 = 1 \times 3$	19	$209 = 11 \times 19$
4	2	20	277
5	$5 = 1 \times 5$	21	367
6	5	22	486
7	$7 = 1 \times 7$	23	$644 = 28 \times 23$
8	10	24	853
9	12	25	1130
10	17	26	1497
11	$22 = 2 \times 11$	27	1983
12	29	28	2627
13	$39 = 3 \times 13$	29	$3480 = 120 \times 29$
14	51	30	4610
15	68	31	$6107 = 197 \times 31$

It appears that if n is prime, then $a(n)$ is divisible by n. We will prove this in the next section. The converse is not true. However, there are only seventeen composite $1 < n < 10^9$ for which $a(n)$ is divisible by n, the lowest being $271441 = 521^2$. The generally accepted convention is that such composites are referred to as **unrestricted Perrin pseudoprimes**, with the definition of Perrin pseudoprimes imposing further restrictions on such composites, as we will see in section 7. Note that some authors use Perrin pseudoprimes when referring to unrestricted Perrin pseudoprimes.

We will also see in section 7 that if a yet unproven conjecture is true, then Perrin's sequence can provide a fast proof of primality for around 5/6 of primes. Although Perrin noted this sequence and its intriguing property in 1899 (actually discovered and more fully analysed by Lucas in a publication of 1876), the first composite n for which $a(n)$ is divisible by n was only discovered in 1982. The proof that there are an infinite number of Perrin pseudoprimes was only made in 2010.

2. Proof that $a(n)$ is divisible by n if n is prime

Let

$$P(x) \;=\; a(2)x + a(3)x^2 + a(4)x^3 + a(5)x^4 + a(6)x^5 + \dots.$$

Then

$$\begin{aligned} x^2P(x) &= a(2)x^3 + a(3)x^4 + a(4)x^5 + \dots, \\ x^3P(x) &= a(2)x^4 + a(3)x^5 + \dots, \end{aligned}$$

and so

$$(1 - x^2 - x^3)P(x) \;=\; a(2)x + a(3)x^2 + [a(4) - a(2)]x^3,$$

since all other terms cancel out. This gives $P(x) = (2x+3x^2)/(1-x^2-x^3)$. Integrating both sides, we get

$$\begin{aligned} &\frac{a(2)x^2}{2} + \frac{a(3)x^3}{3} + \frac{a(4)x^4}{4} + \dots = -\log(1 - x^2 - x^3) = -\log(1 - x^2(1 + x)) \\ &= x^2(1 + x) + \frac{(x^2)^2(1 + x)^2}{2} + \frac{(x^2)^3(1 + x)^3}{3} + \dots \\ &= \frac{(x^2)^1}{1}\sum_{k=0}^{1}\frac{1!\,x^k}{k!(1-k)!} + \frac{(x^2)^2}{2}\sum_{k=0}^{2}\frac{2!\,x^k}{k!(2-k)!} + \frac{(x^2)^3}{3}\sum_{k=0}^{3}\frac{3!\,x^k}{k!(3-k)!} + \dots. \end{aligned}$$

Equating coefficients of x^n on both sides, we get for $n > 0$

$$\frac{a(n)}{n} \;=\; \sum_{\lceil k=n/3\rceil}^{\lfloor n/2\rfloor} \frac{(k-1)!}{(n \bmod k)![k - (n \bmod k)]!}$$

where $\lfloor x\rfloor$ is x rounded down to the nearest integer, and $\lceil x\rceil$ is x rounded up to the nearest integer.

Now

$$\frac{k!}{(k-j)!\,j!} \;=\; \binom{k}{j} \;=\; \frac{k}{j}\frac{(k-1)!}{(k-j)!\,(j-1)!} \;=\; \binom{k-1}{j-1};$$

so $j\binom{k}{j} = k\binom{k-1}{j-1}$. Therefore if $\gcd(k, j) = 1$, $\dfrac{k!}{(k-j)!\,j!}$ is divisible by k. If $\gcd(k, n) = 1$, then $\gcd(k, n \bmod k) = 1$; hence in this case, $\dfrac{k!}{(n \bmod k)![k - (n \bmod k)]!}$ is divisible by k and $\dfrac{(k-1)!}{(n \bmod k)![k - (n \bmod k)]!}$ must be an integer. If this is true for all k between $\lceil n/3\rceil$ and $\lfloor n/2\rfloor$, then $a(n)$ is divisible by n. If n is prime, this is indeed true.

3 The connection with the roots of $x^3 - x - 1 = 0$

We denote the roots of $x^3 - x - 1 = 0$ as x_1, x_2, x_3.

Clearly, $x_1^0 + x_2^0 + x_3^0 = 3 = a(0)$. By definition, $(x - x_1)(x - x_2)(x - x_3) = x^3 - x - 1$. Equating coefficients of powers of x on each side, we get $x_1 + x_2 + x_3 = 0 = a(1)$, $x_1x_2 + x_2x_3 + x_3x_1 = -1$ and $x_1x_2x_3 = 1$. Now

$$x_1^2 + x_2^2 + x_3^2 = (x_1 + x_2 + x_3)^2 - 2(x_1x_2 + x_2x_3 + x_3x_1) = 2 = a(2).$$

This suggests $a(n) = x_1^n + x_2^n + x_3^n$, which we now prove by induction.

Suppose this is true for n, $n-1$, $n-2$. Then

$$\begin{aligned} a(n-1) + a(n-2) &= (x_1^{n-1} + x_2^{n-1} + x_3^{n-1}) + (x_1^{n-2} + x_2^{n-2} + x_3^{n-2}) \\ &= (x_1^{n-1} + x_2^{n-1} + x_3^{n-1}) \\ &\quad - x_1x_2x_3(x_1x_2 + x_2x_3 + x_3x_1)(x_1^{n-2} + x_2^{n-2} + x_3^{n-2}). \end{aligned}$$

Considering x_1^{n-1} terms, the coefficient is

$$\begin{aligned} 1 - x_2^2x_3^2 - x_1x_2^2x_3 - x_1x_2x_3^2 &= 1 - x_2^2x_3^2 - x_1x_2x_3(x_2 + x_3) \\ &= 1 - x_2^2x_3^2 + x_1 = 1 - \frac{1}{x_1^2} + x_1 = \frac{x_1^2 - 1 + x_1^3}{x_1^2}. \end{aligned}$$

Since $x_1^3 - x_1 - 1 = 0$, $x_1^2 - 1 + x_1^3 = x_1^2 - 1 + x_1 + 1 = x_1(x_1 + 1) = x_1^4$; so the coefficient of x_1^{n-1} is $x_1^4/x_1^2 = x_1^2$, i.e. the term is x_1^{n+1}. Repeating for x_2^{n-1}, x_3^{n-1} terms, permuting suffixes, we get $a(n-1) + a(n-2) = a(n+1)$, as required.

The equation $x^3 - x - 1 = 0$ has one real root,

$$x_1 = \sqrt[3]{\frac{1}{2} + \sqrt{\frac{23}{108}}} + \sqrt[3]{\frac{1}{2} - \sqrt{\frac{23}{108}}} = 1.324717957244746\ldots,$$

and two complex roots x_2, $x_3 = (-x_1 \pm i\sqrt{3x_1^2 - 4})/2$. The complex roots have modulus $\sqrt{x_1^2 - 1} = 0.868836961832709\ldots$; so x_2^n, $x_3^n \to 0$ as $n \to \infty$. So for large n, a good approximation to $a(n)$ is $(1.32471795724475)^n$. As we will see in the next section, the sequence can be extended to include negative values of n. In this case, a good approximation to $a(n)$ is

$$\begin{aligned} &2x_1^{-n/2} \cos\left[n\left(\pi - \tan^{-1}\frac{\sqrt{3x_1^2 - 4}}{x_1}\right)\right] \\ &\quad \approx 2(1.1509639252525775)^{-n} \cos(2.50450662237558n). \end{aligned}$$

Some arithmetic will show $[(x_1 - x_2)(x_2 - x_3)(x_3 - x_1)]^2 = -23$. This is called the **discriminant** of $x^3 - x - 1 = 0$, and will be important later.

4 Calculating $a(n)$

Firstly, we need to extend $a(n)$ for negative n. We can do this merely by rearranging the original definition to get $a(n) = a(n+3) - a(n+1)$. The first few values are as follows.

n	$a(n)$	n	$a(n)$
0	3	-16	5
-1	$-1 = 0 \times -1 - 1$	-17	$-18 = 1 \times -17 - 1$
-2	$1 = -1 \times -2 - 1$	-18	25
-3	$2 = -1 \times -3 - 1$	-19	$-20 = 1 \times -19 - 1$
-4	-3	-20	2
-5	$4 = -1 \times -5 - 1$	-21	23
-6	-2	-22	-43
-7	$-1 = 0 \times -7 - 1$	-23	$45 = -2 \times -23 - 1$
-8	5	-24	-22
-9	-7	-25	-21
-10	6	-26	66
-11	$-1 = 0 \times -11 - 1$	-27	-88
-12	-6	-28	67
-13	$12 = -1 \times -13 - 1$	-29	$-1 = 0 \times -29 - 1$
-14	-13	-30	-87
-15	7	-31	$154 = -5 \times -31 - 1$

Much of the previous theory applies unchanged. In particular, $a(n) = x_1^n + x_2^n + x_3^n$ also applies for $n < 0$. However, the divisibility rule becomes: If $n < 0$ and n is prime, then $a(n) + 1$ is divisible by $-n$, which we now prove. Let

$$Q(x) \;=\; a(-1) + a(-2)x + a(-3)x^2 + a(-4)x^3 + a(-5)x^4 + \dots.$$

Then $(1+x-x^3)Q(x) = a(-1)+[a(-2)+a(-1)]x+[a(-3)+a(-2)]x^2$ (similar to the derivation of $P(x)$). This gives $Q(x) = (-1+3x^2)/(1+x-x^3)$. Integrating both sides, we get

$$\begin{aligned} a(-1)x + \frac{a(-2)x^2}{2} + \frac{a(-3)x^3}{3} + \frac{a(-4)x^4}{4} + \dots \;&=\; -\log(1 + x(1-x^2)) \\ &=\; -x(1-x^2) + \frac{x^2(1-x^2)^2}{2} - \frac{x^3(1-x^2)^3}{3} + \dots \\ &=\; \frac{x}{1}\sum_{k=0}^{1}\frac{(-1)^k 1! x^{2k}}{k!(1-k)!} + \frac{x^2}{2}\sum_{k=0}^{2}\frac{(-1)^k 2! x^{2k}}{k!(2-k)!} + \frac{(-1)^k x^3}{3}\sum_{k=0}^{3}\frac{(-1)^k 3! x^{2k}}{k!(3-k)!} + \dots \end{aligned}$$

Equating coefficients of x^n on both sides, we get

$$\frac{a(-n)}{n} \;=\; \sum_{k=0}^{\lfloor n/3\rfloor} (-1)^{n+k} \frac{(n-2k-1)!}{(n-3k)!\,k!}.$$

The $k=0$ term is $(-1)^n(n-1)!/n! = -\dfrac{1}{n}$ for odd n; so for odd n,

$$\frac{a(-n)+1}{n} \;=\; \sum_{k=1}^{\lfloor n/3\rfloor} (-1)^{n+k} \frac{(n-2k-1)!}{(n-3k)!\,k!}.$$

If $\gcd(n,k) = 1$, then $\gcd(k, n-2k) = 1$; so $(n-2k)!/((n-3k)!k!)$ is divisible by $(n-2k)$, and if n is prime, this is true for all $0 < k \le \lfloor n/3\rfloor$.

The table on the previous page shows $a(n)$ as the value -1 for $n = -7$, -11 and -29. It turns out that there are many negative n which are multiples of 7, 11 or 29 for which $a(n)+1$ is divisible by n, e.g. -49, -77, -121, -203, -319. If these are stripped out, there are 24 composite negative n with $|n| < 10^9$ such that $a(n)+1$ is divisible by n.

To calculate $a(n)$ efficiently, we use the relationship $a(2n) = a(n)^2 - 2a(-n)$. This relationship can be seen from the following. Since $a(n) = x_1^n + x_2^n + x_3^n$ for any n,

$$a(n)^2 - 2a(-n) \;=\; (x_1^n + x_2^n + x_3^n)^2 - 2(x_1^{-n} + x_2^{-n} + x_3^{-n}).$$

Since $x_1x_2x_3 = 1$, the last term in brackets is $(x_1^n x_2^n + x_2^n x_3^n + x_3^n x_1^n)$. So

$$a(n)^2 - 2a(-n) \;=\; a(2n).$$

We keep track of the six values

$$S(n) \;=\; \{a(-n-1), a(-n), a(-n+1), a(n-1), a(n), a(n+1)\}.$$

We call this the **signature** of n. We can then calculate $a(-2n-2)$, $a(-2n)$, $a(-2n+2)$, $a(2n-2)$, $a(2n)$, $a(2n+2)$, then fill in the gaps to get $S(2n)$ using, for example, $a(-2n-1) = a(-2n+2) - a(-2n)$ and $a(2n-1) = a(2n+2) - a(2n)$.

Example: $n = 71$. The binary representation of 71 is 1000111, so starting from the most significant bit, we then calculate $S(2)$, $S(4)$, $S(8)$, $S(17)$, $S(35)$, $S(71)$: $S(1)$ is $\{1, -1, 3, 3, 0, 2\}$; $S(2)$ is calculated as above, filling in the gaps: $\{2, 1, -1, 0, 2, 3\}$; $S(4)$ is calculated similarly: $\{4, -3, 2, 3, 2, 5\}$;

$S(8)$ is calculated similarly: $\{-7, 5, -1, 7, 10, 12\}$. To get S(17), we calculate $S(16) : \{-18, 5, 7, 68, 90, 119\}$, then use $a(-18) = a(-15) - a(-17)$, $a(18) = a(15) + a(16)$ to get $S(17)$: $\{25, -18, 5, 90, 119, 158\}$. Similarly, $S(35) = \{309, -241, 86, 14197, 18807, 24914\}$, and finally $S(71) = \{45653, -41465, 20467, 353703731, 468557684, 620706778\}$ giving $a(71) = 468557684$. Clearly, all these calculations can also be done modulo n.

The number of multiplications involved is proportional to $\log_2 n$, as is the case for each attempt in the Miller–Rabin probabilistic primality test, so it is worth examining further as a primality test. The calculation of $a(n) \bmod n$ involves calculation of $S(n) \bmod n$, so it seems sensible to examine the characteristics of $S(p) \bmod p$, where p is prime. To create the strongest primality test we can, we can reject composites that fail these characteristics, which we examine in the next section.

5 Prime classification

To classify a prime p, we examine $(x^3 - x - 1) \bmod p$. In this simplified presentation, examples are given, but no proofs.

We call p an S prime (S is for split) if $(x^3 - x - 1) \bmod p$ has three integer roots. For example, 59 is an S prime since

$$(x - 4)(x - 13)(x - 42) = x^3 - 59x^2 + 766x - 2184 \equiv (x^3 - x - 1) \bmod 59.$$

We note that the discriminant -23 is a **quadratic residue** modulo 59, i.e. it has an integer square root modulo 59, namely 6, since $6^2 = 36 \equiv -23 \bmod 59$. This property is true for all S primes. Note also that 23 is an S prime since $(x - 3)(x - 10)(x - 10) = x^3 - 23x^2 + 160x - 300 \equiv (x^3 - x - 1) \bmod 23$.

We will call p a Q prime (Q is for quadratic) if $(x^3 - x - 1) \bmod p$ has one integer root. For example, 37 is a Q prime since

$$(x - 13)(x^2 + 13x + 20) \;=\; x^3 - 149x - 260 \;\equiv\; (x^3 - x - 1) \bmod 37,$$

but no integer is a root of $(x^2 + 13x + 20) \bmod 37$. However, we can add an element to the field of integers modulo p such that the quadratic term has two roots, much as we can add $\sqrt{-1}$ to the reals to solve any polynomial with integer coefficients. This element is the square root of the discriminant Δ of this quadratic. For ax^2+bx+c, this is b^2-4ac, giving roots $(-b\pm\sqrt{\Delta})/(2a)$. For $(x^2 + 13x + 20) \bmod 37$, this gives

$$(x + 25 + 18\sqrt{15})(x + 25 - 18\sqrt{15}) \;\equiv\; (x^2 + 13x + 20) \bmod 37.$$

By definition, the discriminant cannot be a quadratic residue modulo a Q prime.

Note that we cannot have two and only two integer roots α and β, since the third root γ is such that $\alpha+\beta+\gamma$ is an integer.

Finally, we will call p an I prime (I is for irreducible) if $(x^3-x-1) \bmod p$ has no integer roots. The element to be added to the field of integers modulo p such that the equation has three roots is one of the roots itself, which we will denote by α. Clearly, its inverse is also required to satisfy field closure. For example, 13 is an I prime, and we have

$$\begin{aligned}
&(x-\alpha)\left(x+3+\frac{9}{\alpha}\right)\left(x-3+\alpha+\frac{4}{\alpha}\right)\\
&= x^3+\frac{13x^2}{\alpha}+\left(-\alpha^2+3\alpha-13-\frac{15}{\alpha}+\frac{36}{\alpha^2}\right)x+\left(-3\alpha^2+15-\frac{36}{\alpha}\right)\\
&\equiv x^3+\left(-\alpha^2+3\alpha-\frac{2}{\alpha}-\frac{3}{\alpha^2}\right)x+\left(-3\alpha^2+2+\frac{3}{\alpha}\right) \bmod 13.
\end{aligned}$$

Since $\alpha^3-\alpha-1\equiv 0 \bmod 13$, $\alpha^2=1+1/\alpha$, $1/\alpha^2=\alpha-1/\alpha$, the above $\equiv (x^3-x-1) \bmod 13$. We note that the discriminant -23 is a quadratic residue modulo 13, since $4^2=16\equiv -23 \bmod 13$. This property is true for all I primes.

It turns out that primes of each class have distinct signatures modulo p. We will derive the form of these signatures in the next section.

6 Generalizing Perrin's sequence

We can generalize Perrin's sequence as follows. Let $f=x^3-rx^2+sx-1$, and denote a_f as the sequence corresponding to f, i.e.

$$a_f(-1)=s,\ a_f(0)=3,\ a_f(1)=r,\ a_f(n+3)=ra_f(n+2)-sa_f(n+1)+a_f(n).$$

This gives $a_f(2)=r^2-2s$ and $a_f(3)=r^3-3rs+3$, which we will need later. Note that if $g=x^3-sx^2+rx-1$, then $a_f(-n)=a_g(n)$, so any analysis done for $n\geq 0$ also applies to $n<0$. Perrin's sequence itself corresponds to $r=0$, $s=-1$.

Denoting the roots of $f=0$ as α,β,γ, it can be shown that $a_f(n)=\alpha^n+\beta^n+\gamma^n$ (the proof, along the lines of that in section 3, is left to the reader).

If p is prime, then $a_f(p)\equiv r \bmod p$ and $a_f(-p)\equiv s \bmod p$. This can be

shown as follows:

$$\begin{aligned} a_f(1)^p \bmod p &\equiv (\alpha+\beta+\gamma)^p \bmod p \\ &\equiv \left(\alpha^p+\beta^p+\gamma^p+\sum_{i+j+k=p,\ i,j,k>0} \frac{p!}{i!j!k!}\alpha^i\beta^j\gamma^k\right) \bmod p. \end{aligned}$$

We can treat $\alpha^i\beta^j\gamma^k$ symbolically, provided that there are no values of i, j, k such that $\alpha^i\beta^j\gamma^k = u/(vp)$ where u, v are integers with $\gcd(u, vp) = 1$. In section 5, we showed that this is so, since each root mod p is either an integer, or symbolic. Each coefficient $p!/(i!\,j!\,k!)$ of $\alpha^i\beta^j\gamma^k$ is divisible by p since $0 < i, j, k < p$; so we have $a_f(1)^p \equiv (\alpha+\beta+\gamma)^p \bmod p = a_f(p) \bmod p$. But by Fermat's little theorem, $a_f(1)^p \equiv a_f(1) \bmod p$, so $a_f(p) \equiv a_f(1) = r \bmod p$.

To calculate $a_f(n)$, the relationship $a_f(2n) = a_f(n)^2 - 2a_f(-n)$ derived in section 4 applies, since $\alpha\beta\gamma = 1$. The process of filling in the gaps is similar. We have, for example:

$$\begin{aligned} a_f(n+1) &= ra_f(n) - sa_f(n-1) + a_f(n-2), \\ a_f(n+2) &= ra_f(n+1) - sa_f(n) + a_f(n-1); \\ \text{so}\quad a_f(n+1) &= \frac{a_f(n+2) + (s-r^2)a_f n - ra_f(n-2)}{1-rs}. \end{aligned}$$

Working modulo x, this becomes

$$a_f(n+1) \equiv d[a_f(n+2) + (s-r^2)a_f n - ra_f(n-2)] \bmod (x/c),$$

where $c = \gcd(x, 1-rs)$, $(1-rs)d \equiv c \bmod (x/c)$.

The functional equation techniques used to evaluate $\dfrac{a(n)+r}{n}$ in sections 2 and 4 can be extended, but the form of integral used depends on r, s. The discriminant Δ for $x^3 - rx^2 + sx - 1$ is $r^2s^2 - 4r^3 - 4s^3 + 18rs - 27$. S primes have the signature $\{s^2 - 2r, s, 3, 3, r, r^2 - 2s\}$ modulo p, i.e. $\{a(-2), a(-1), a(0), a(0), a(1), a(2)\}$.

Q primes have the signature $\{A, s, B, B, r, C\}$ modulo p, where $A \equiv a^{-2} + 2a \bmod p$, $B \equiv -ra^2 + (r^2 - s)a \bmod p$, $C \equiv a^2 + 2a^{-1} \bmod p$, and a is the only integer root of $a^3 - ra^2 + sa - 1 \equiv 0 \bmod p$.

I primes have the signature $\{r, s, D, E, r, s\}$ modulo p, where $D + E \equiv rs - 3 \bmod p$, and $(D - E)^2 \equiv \Delta \bmod p$.

We will now show that the above relations arise if the following are true. For S primes, $\alpha^p \equiv \alpha \bmod p$, $\beta^p \equiv \beta \bmod p$, $\gamma^p \equiv \gamma \bmod p$. For Q primes,

$\alpha^p \equiv \alpha \bmod p$, $\beta^p \equiv \gamma \bmod p$, $\gamma^p \equiv \beta \bmod p$, where α is the only integer root. For I primes, $\alpha^p \equiv \beta \bmod p$, $\beta^p \equiv \gamma \bmod p$, $\gamma^p \equiv \alpha \bmod p$.

For S primes, the relations arise immediately from Fermat's little theorem. For other types, we need to do algebraic manipulations on each of the three equivalences shown above. It is convenient to show these in parallel by use of matrices. For Q primes, we want

$$\begin{pmatrix} \alpha^{-1} & \beta^{-1} & \gamma^{-1} \\ 1 & 1 & 1 \\ \alpha & \beta & \gamma \end{pmatrix} \begin{pmatrix} \alpha^n \\ \beta^n \\ \gamma^n \end{pmatrix} \equiv \begin{pmatrix} a_f(n-1) \\ a_f(n) \\ a_f(n+1) \end{pmatrix} \equiv \begin{pmatrix} \alpha^{-1} & \beta^{-1} & \gamma^{-1} \\ 1 & 1 & 1 \\ \alpha & \beta & \gamma \end{pmatrix} \begin{pmatrix} \alpha \\ \gamma \\ \beta \end{pmatrix}$$

$$= \begin{pmatrix} 1+\beta^{-1}\gamma+\gamma^{-1}\beta \\ \alpha+\beta+\gamma \\ \alpha^2+2\beta\gamma \end{pmatrix} = \begin{pmatrix} 1+\alpha(a_f(2)-\alpha^2) \\ r \\ \alpha^2+2\alpha^{-1} \end{pmatrix} = \begin{pmatrix} -r\alpha^2+(r^2-s)\alpha \\ r \\ \alpha^2+2\alpha^{-1} \end{pmatrix}.$$

For I primes, we want

$$\begin{pmatrix} \alpha^{-1} & \beta^{-1} & \gamma^{-1} \\ 1 & 1 & 1 \\ \alpha & \beta & \gamma \end{pmatrix} \begin{pmatrix} \alpha^n \\ \beta^n \\ \gamma^n \end{pmatrix} \equiv \begin{pmatrix} a_f(n-1) \\ a_f(n) \\ a_f(n+1) \end{pmatrix} \equiv \begin{pmatrix} \alpha^{-1} & \beta^{-1} & \gamma^{-1} \\ 1 & 1 & 1 \\ \alpha & \beta & \gamma \end{pmatrix} \begin{pmatrix} \beta \\ \gamma \\ \alpha \end{pmatrix}$$

$$= \begin{pmatrix} \alpha^{-1}\beta+\beta^{-1}\gamma+\gamma^{-1}\alpha \\ \alpha+\beta+\gamma \\ \alpha\beta+\beta\gamma+\gamma\alpha \end{pmatrix} = \begin{pmatrix} \beta^2\gamma+\gamma^2\alpha+\alpha^2\beta \\ r \\ \gamma^{-1}+\alpha^{-1}+\beta^{-1} \end{pmatrix} = \begin{pmatrix} E \\ r \\ s \end{pmatrix}.$$

Setting $D = \alpha^2\gamma + \beta^2\alpha + \gamma^2\beta$, we get

$$D+E = \alpha(\beta^2+\gamma^2)+\beta(\alpha^2+\gamma^2)+\gamma(\alpha^2+\beta^2) = -a_f(3)+a_f(1)a_f(2) = rs-3,$$

and $(D-E)^2 = [(\alpha-\beta)(\beta-\gamma)(\gamma-\alpha)]^2 = \Delta$. Proving that the signatures are actually of the form given above is quite intricate—see Adams and Shanks (1982) for more details.

The signatures modulo p for S, Q and I primes p are distinct except where p is a factor of Δ. In this case, $\Delta = [(\alpha-\beta)(\beta-\gamma)(\gamma-\alpha)]^2 \equiv 0 \bmod p$, so two roots must be identical mod p. Since $x^3 - rx^2 + sx - 1 \equiv (x-b)^2(x-a) \bmod p$ for distinct integers a, b, they are S primes which also have $\Delta \equiv 0 \bmod p$, and the S signature is the same as the Q signature with a being the non-repeated root.

Subsequent sections deal with Perrin pseudoprimes, which are defined as odd. To ensure distinct signatures, we will therefore adopt the convention from now on that 'prime' is taken to mean an odd prime that is not a factor of the discriminant.

7 Perrin pseudoprimes

Finally (and not before time, you might think), we are ready to give a definition of a (restricted) Perrin pseudoprime.

We will call an odd composite n a Perrin pseudoprime for some permitted r, s if one of the following conditions is true.

a) It has an S signature, and the discriminant Δ of $x^3 - rx^2 + sx - 1$ is such that the Jacobi symbol (see below) $\left(\frac{\Delta}{n}\right) = 1$.

b) It has a Q signature, and $\left(\frac{\Delta}{n}\right) = -1$.

c) It has an I signature.

All values of r, s are permitted apart from $(-1,-1)$, $(0,0)$, $(1,1)$, $(2,2)$, $(3,3)$. These are excluded because all the roots of $x^3 - rx^2 + sx - 1 = 0$ have modulus 1, so the associated sequence repeats: $(3,-1)$, $(3,0,0)$, $(3,1,-1,1)$, $(3,2,0,-1,0,2)$, (3) respectively.

The use of the Jacobi symbol needs explanation. In previous sections, we indicated that if a prime p has an S signature for a given r, s, then Δ must be a quadratic residue modulo p, and must not be for a Q signature (for an I signature, we get $\sqrt{\Delta}$ explicitly).

For composite n, Δ is a quadratic residue modulo n only if Δ is a quadratic residue modulo every prime factor of n. Factorizing n defeats the whole purpose of using a generalized Perrin sequence. Instead, we use the Jacobi symbol, whose evaluation is such that if $\left(\frac{x}{y}\right) = -1$, then x is not a quadratic residue modulo y, but that if $\left(\frac{x}{y}\right) = 1$, then x may or may not be a quadratic residue modulo y. The theory associated with the Jacobi symbol and its evaluation can be found in standard textbooks.

Checking that a signature corresponds to that of a particular class requires little computation, since we know r, s. For the Q signature, we require $a = \dfrac{3B + rC - 2rs}{r^2 - 3s} = \dfrac{AB - 3r}{A(r^2 - s) - 2rC}$; so if $(AB - 3r)(r^2 - 3s) = (3B + rC - 2rs)(A(r^2 - s) - 2rC)$, a can be checked to see if it is a root of $x^3 - rx^2 + sx - 1$.

Although factorization of polynomials modulo a prime is unique, this is not necessarily so modulo a composite. This is hardly surprising, since signature classes for prime factors of n are not necessarily the same.

The following are examples of pseudoprimes with multiple factorizations.

Example 1: $r = -2$, $s = -14$, $n = 1649 = 17 \times 97$, which has a Q signature. The calculated root is 943, and as required $(x^3+2x^2-14x-1) \equiv (x-943)(x^2+945x+661) \bmod 1649$, with no integer satisfying $(x^2+945x+661) \bmod 1649$. However, $(x^3+2x^2-14x-1) \equiv (x-858)(x^2+860x+763) \bmod 1649$, with no integer satisfying $(x^2+860x+763) \bmod 1649$, and $(x^3+2x^2-14x-1) \equiv (x-331)(x^2+333x+1375) \bmod 1649$, with no integer satisfying $(x^2+333x+1375) \bmod 1649$. Now $(x^3+2x^2-14x-1) \equiv (x-8)(x^2+10x+15) \bmod 17$, with no integer satisfying $(x^2+10x+15) \bmod 17$, i.e. Q class, and $(x^3+2x^2-14x-1) \equiv (x-40)(x-70)(x-82) \bmod 97$, i.e. S class. The derivations for A, B, C in the previous section used one particular factorization, so the above gives rise to the unique integer root corresponding to that factorization.

Example 2: $r = 2$, $s = -2$, $n = 79003 = 199 \times 397$, which has an S signature, and can be decomposed in six different ways (6^{N-1} ways for N different prime factors):

$(x^3-2x^2-2x-1) \equiv (x-12428)(x-18491)(x-48086) \bmod 79003$,
$(x^3-2x^2-2x-1) \equiv (x-12428)(x-25854)(x-40723) \bmod 79003$,
$(x^3-2x^2-2x-1) \equiv (x-18491)(x-62775)(x-76742) \bmod 79003$,
$(x^3-2x^2-2x-1) \equiv (x-25854)(x-55412)(x-76742) \bmod 79003$,
$(x^3-2x^2-2x-1) \equiv (x-40723)(x-54510)(x-62775) \bmod 79003$,
$(x^3-2x^2-2x-1) \equiv (x-48086)(x-54510)(x-55412) \bmod 79003$.

Again, the derivation is still valid because one particular factorization is considered.

Chebotarev's density theorem applied to x^3-rx^2-sx-1 for most values of r, s shows that for a sufficiently large set of primes, 1 in 6 is an S prime, 1 in 2 is a Q prime, and 1 in 3 is an I prime. Other distributions for permitted r, s occur as follows: 1 in 2 is an S prime, 1 in 2 is a Q prime if $s = r$, or $\Delta+4$ is a perfect square, which seems to occur only for $s = -(r+2)$; 1 in 3 is an S prime, 2 in 3 is an I prime if Δ is a perfect square. Values of r, s for which this is true are mostly scattered, but the following series are easily discernible: $s = -(r+3)$, (r, s) or $(s, r) = (n^2+5, (n+1)^2+5)$, for any n.

How rare are Perrin pseudoprimes, and how effective are the various conditions of their definition? The following data indicate their incidence for composites up to 1.2×10^8, using $|r| < 15, r > s$, and excluding the last two density distributions. This gives 53158353 odd composites for each of 372 permitted r, s values, i.e. about 1.9×10^{10} combinations to be tested. Using the signature alone gives 2236 candidate pseudoprimes (not necessar-

ily distinct). Of these, 278 are rejected for even n, or $\gcd(n, \Delta) > 1$, and another 281 by failing the Jacobi symbol test, giving 1677 Perrin pseudoprimes. Of these, four have Q signatures, 31 have I signatures with n being the square of a small prime (namely twenty 9s, six 25s, one 49 and one 121), and four others having I signatures.

Q signatures (the class of each prime factor is also given):
$r = 2$, $s = -3$, $n = 2001689 = 229(\text{Q}) \times 8741(\text{S})$, roots: 94408 (signature root), 132880, 839116;
$r = 10$, $s = 5$, $n = 2001689 = 229(\text{Q}) \times 8741(\text{S})$, roots: 195731, 1351036 (signature root), 1538816;
$r = 10$, $s = -11$, $n = 12431 = 401(\text{Q}) \times 31(\text{S})$, roots: 2377, 10397, 11199 (signature root);
$r = 12$, $s = -5$, $n = 17261 = 41(\text{Q}) \times 421(\text{S})$, roots: 8872, 12234, 16375 (signature root);
$r = -2$, $s = -14$, $n = 1649 = 17(\text{Q}) \times 97(\text{S})$, roots: 331, 858, 943 (signature root);
$r = 13$, $s = -14$, $n = 33671 = 11(\text{Q}) \times 3061(\text{S})$, roots: 1043, 4607, 31095 (signature root).

Additional Q pseudoprimes found:
$r = 16$, $s = -17$, $n = 74801 = 131(\text{Q}) \times 571(\text{S})$, roots: 13944, 62676, 70143 (signature root);
$r = 17$, $s = 7$, $n = 65 = 5(\text{Q}) \times 13(\text{S})$, roots: 11, 46, 51 (signature root);
$r = 18$, $s = -3$, $n = 119 = 7(\text{Q}) \times 17(\text{S})$, roots: 29, 50 (signature root), 92;
$r = 18$, $s = 4$, $n = 11521 = 41(\text{Q}) \times 281(\text{S})$, roots: 3891, 4301 (signature root), 4752;
$r = 19$, $s = -4$, $n = 391 = 23(\text{Q}) \times 17(\text{S})$, roots: 116, 254 (signature root), 346;
$r = 19$, $s = 18$, $n = 47435009 = 1217(\text{Q}) \times 38977(\text{S})$, roots: 6617807, 23990482, 36081377 (signature root).

I signatures:
$r = 11$, $s = 3$, $n = 315 = 3(\text{I}) \times 3(\text{I}) \times 5(\text{I}) \times 7(\text{I})$;
$r = -3$, $s = -12$, $n = 7291 = 23(\text{I}) \times 317(\text{S})$;
$r = 14$, $s = -9$, $n = 4771 = 13(\text{I}) \times 367(\text{S})$;
$r = -11$, $s = -14$, $n = 86761 = 53(\text{I}) \times 1637(\text{S})$.

The remaining 1638 Perrin pseudoprimes have S signatures. Of these, 249 are actually irreducible (discovered by searching for roots). Of the remaining 1389, 1291 are the product of two prime factors, 95 three prime factors, and 4 four prime factors. There are about 17 million odd composites with two prime factors $< 1.2 \times 10^8$. If this data is representative, then

only about 1 in 5 million composites with two prime factors are pseudoprimes, and 1 in 130 million composites with more than two prime factors are pseudoprimes.

8 Why are pseudoprimes so rare, and why do the vast majority have S signatures?

To answer these questions, we first need to identify the periodicity of $a_f(n) \bmod p$; i.e. to find $W_f(p)$ such that $a_f(n+c) = a_f(n+c+W_f(p)) \bmod p$ for $c = -1, 0, 1$.

For S primes, $\alpha^p \equiv \alpha \bmod p, \beta^p \equiv \beta \bmod p, \gamma^p \equiv \gamma \bmod p$; i.e. $W_f(p)$ is some divisor of $p-1$.

For Q primes, $\alpha^p \equiv \alpha \bmod p, \beta^p \equiv \gamma \bmod p, \gamma^p \equiv \beta \bmod p$, where α is the only integer root, so $(\beta^p)^p = \beta$ and $(\gamma^p)^p = \gamma$; i.e. $W_f(p)$ is some divisor of p^2-1.

For I primes, $\alpha^p \equiv \beta \bmod p$, $\beta^p \equiv \gamma \bmod p$, $\gamma^p \equiv \alpha \bmod p$. Using a similar argument to that for Q primes, this gives $W_f(p)$ is a divisor of p^3-1. We can do better than this, because $1 = \gamma\beta\alpha = ((\alpha^p)^p)(\alpha^p)\alpha = \alpha^{p^2+p+1}$; i.e. $W_f(p)$ is some divisor of p^2+p+1. In all cases, $\gcd(W_f(p), p) = 1$.

The definition of $W(p)$ implies that the signatures $S(p + kW(p)) \equiv S(p) \bmod p$ for any signature class, i.e. $S(np) \equiv S(p) \bmod p$ if $np - p = kW(p)$. For S class primes only, $W(p) = (p-1)/c$, so $S(np) \equiv S(p) \bmod p$ if $np - 1 = kW(p)$. We state without proof that for composite $n = \prod p_i^{\nu_i}$, we have $W(n)$ is a factor of $\dfrac{\prod p_i^{\nu_i - 1} \prod W(p_i)}{\gcd(\{W(p_i)\})}$.

In order for a composite n to have a valid signature, rules apply, summarized in the table on the next page, and adapted from that in Adams (1987), where the appropriate theory is also given. Rather than repeating this here in full, we will derive various aspects of it as we need it in the various examples which follow. Let n be an odd composite with $n = p^\nu k$, where p is a prime, $\nu > 0$; k could be a prime or a composite (not necessarily with any signature), and may or may not be divisible by p. In all cases, we require that $W(p^\nu) = W(p)$.

Suppose p is an S prime, i.e. $f \equiv (x-a_0)(x-b_0)(x-c_0) \bmod p$ for integers a_0, b_0, c_0. We now show that there are integers a, b, c (as used in rows 2 and 3 of the above table) such that $f \equiv (x-a)(x-b)(x-c) \bmod p^\nu$ by using a technique called **Hensel lifting**, which works as follows. If T is a root of $f(x) \equiv 0 \bmod p^k$, and $f'(T) \not\equiv 0 \bmod p$, then V is a root of $f(x) \equiv 0 \bmod p^{k+m}$ for any m, where $V \equiv (T - f(T)[f'(T)^{-1} \bmod p^m]) \bmod p^{k+m}$.

Since we have explicitly excluded primes for which f has repeated roots, $f'(T) \not\equiv 0 \bmod p$. As an example, 4 is a root of $f = x^3 - x - 1 \equiv 0 \bmod 59$. Then $f'(4) = 3{\times}4^2{-}1 \equiv 47 \bmod 59$, and $47{\times}54 \equiv 1 \bmod 59$, so $4{-}54{\times}59 \equiv 299 \bmod 59^2$ is a root of $f = x^3 - x - 1 \equiv 0 \bmod 59^2$.

p	ν	n	Additional conditions
S	Any	S	$k \equiv 1 \bmod W(p)$
S	Any	Q	$a^{k-1} \equiv 1 \bmod p^\nu, b^k \equiv c \bmod p^\nu$ (see below)
S	Any	I	$a^k \equiv b \bmod p^\nu, b^k \equiv c \bmod p^\nu$ (see below)
Q	Even	S	$k \equiv 1 \bmod W(p)$
Q	Odd	S	$k \equiv p \bmod W(p)$
Q	Even	Q	$k \equiv p \bmod W(p)$
Q	Odd	Q	$k \equiv 1 \bmod W(p)$
Q	-	I	impossible
I	0 mod 3	S	$k \equiv 1 \bmod W(p)$
I	1 mod 3	S	$k \equiv p^2 \bmod W(p)$
I	2 mod 3	S	$k \equiv p \bmod W(p)$
I	-	Q	impossible
I	0 mod 3	I	$k \equiv p$ or $p^2 \bmod W(p)$
I	1 mod 3	I	$k \equiv 1$ or $p \bmod W(p)$
I	2 mod 3	I	$k \equiv 1$ or $p^2 \bmod W(p)$

We will illustrate the rarity of pseudoprimes by showing how to construct pseudoprimes from two primes p and q.

1. Constructing a class S pseudoprime from two class S primes.

Suppose $n = pq$, where p, q are different S primes, and $\gcd(p{-}1, q{-}1) = g > 1$, so that $(p-1) = ag, (q-1) = bg$ for some integers a, b. If pq is a pseudoprime, we want $pq - 1 = KW(pq)$ for some integer K. We have $W(p) = (p-1)/x$, $W(q) = (q-1)/y$ for some integers x, y, and $W(pq) = \dfrac{W(p)W(q)}{\gcd(W(p), W(q))e}$ for some integer e. Let $c = \dfrac{xy}{\gcd(x,y)}$, and let $h = \gcd\Big(ca/x, cb/y\Big)$, so $ca/x = hv, cb/g = hw$ for some integers v, w, and $\dfrac{c}{h} = \dfrac{xy}{\gcd(bx, ay)}$ is an integer. We want

$$pq{-}1 = (ag{+}1)(bg{+}1){-}1 = abg^2{+}(a{+}b)g = \frac{Kabg^2}{\gcd\Big(\dfrac{ag}{x}, \dfrac{bg}{y}\Big)xye} = \frac{abcgK}{xyhe},$$

or

$$xyhe\Big(\frac{1}{a}{+}\frac{1}{b}\Big) = \gcd(p{-}1, q{-}1)\frac{(p+q-2)he}{W(p)W(q)} = cK{-}xyghe = cK{-}\frac{c^2abge}{vw}.$$

If $c > 1$, it cannot divide both v and w, so $xyghe$ is divisible by c. We therefore want $\gcd(p-1, q-1)\dfrac{(p+q-2)e}{W(p)W(q)(c/h)}$ to be some integer M.

Unless $W(p) \ll p$ or $W(q) \ll q$, M is likely to be < 1 if $\gcd(p-1, q-1)$ is small. To construct a class S pseudoprime, we construct a list of class S primes, and pick two with a substantial $\gcd(p-1, q-1)$. For example, for $r = 16$, $s = 11$, 18307 and 48817 are class S primes, with $\gcd(18306, 48816) = 6102$, giving $M = 11$, so $893692819 = 18307 \times 48817$ as a valid S class pseudoprime for $r = 16$, $s = 11$. Also $W(18307) = 6102$, $W(48817) = 1017$, and $W(893692819) = 6102$. In terms of factors,

$$x^3 - 16x^2 + 11x - 1 \equiv (x - 2827)(x - 3969)(x - 11527) \bmod 18307,$$

$$x^3 - 16x^2 + 11x - 1 \equiv (x - 2161)(x - 7611)(x - 39061) \bmod 48817,$$

and one of the six factorizations is $x^3 - 16x^2 + 11x - 1 \equiv (x - 304522607)(x - 600261443)(x - 882601604) \bmod 893692819$, with for example, $304522607 \equiv 3969 \bmod 18307 \equiv 2161 \bmod 48817$.

Very few primes have a substantial $\gcd(p-1, q-1)$, hence class S pseudoprimes formed from products of class S primes are rare. We will see in examples below that Class I or class Q pseudoprimes, or class S pseudoprimes formed from products of primes of other classes, are even rarer, and furthermore, class S pseudoprimes so constructed only have S signatures, but no integer roots. As an example, for $r = 0$, $s = -1$, there are 55 Perrin pseudoprimes $< 5 \times 10^{10}$, the lowest being $27664033 = 3037 \times 9109$, and all have S signatures.

2. Conditions for constructing a class Q pseudoprime from a class S prime p and a class Q prime q.

We need $pq - q = kW(pq)$ for q. For p, however, we require it to have a Q signature in $S(pq)$. Recalling the analysis in section 6, the three integer roots α, β, γ for p have $\alpha^p \equiv \alpha \bmod p$, $\beta^p \equiv \beta \bmod p$, $\gamma^p \equiv \gamma \bmod p$. To get a Q signature for $S(pq)$, we require $\alpha^{pq} \equiv \alpha \bmod p$, $\beta^{pq} \equiv \gamma \bmod p$, $\gamma^{pq} \equiv \beta \bmod p$ for some suitable naming of roots. This gives $\alpha^q \equiv \alpha \bmod p$, $\beta^q \equiv \gamma \bmod p$, $\gamma^q \equiv \beta \bmod p$. For example, in the $r = 16, s = -17$ class Q pseudoprime 74801 (=131(Q)×571(S)), $x^3 - rx^2 + sx - 1$ has roots 240, 437, 481 modulo 571, and $240^{131} \equiv 437 \bmod 571$, $437^{131} \equiv 240 \bmod 571$, and $481^{131} \equiv 481 \bmod 571$. The signature root modulo 74801 is therefore α modulo 571, namely 70143. An example of actual construction is given in section 6 of Adams (1987).

3. Constructing a class I pseudoprime from a class S prime p and a class I prime q.

We need $pq - q = kW(pq)$ for q. For p, however, we require it to have an I signature in $S(pq)$. As in the previous example, the three integer roots α, β, γ for p have $\alpha^p \equiv \alpha \bmod p$, $\beta^p \equiv \beta \bmod p$, $\gamma^p \equiv \gamma \bmod p$. To get an I signature for $S(pq)$, we require $\alpha^{pq} \equiv \beta \bmod p$, $\beta^{pq} \equiv \gamma \bmod p$, $\gamma^{pq} \equiv \alpha \bmod p$ for some suitable naming of roots. This gives $\alpha^q \equiv \beta \bmod p$, $\beta^q \equiv \gamma \bmod p$, $\gamma^q \equiv \alpha \bmod p$. For example, in the $r = 85$, $s = -15$ class I pseudoprime 261769 (= 67(I)×3907(S)), $x^3 - rx^2 + sx - 1$ has roots 1765, 3480, 2654 modulo 3907, and $1765^{67} \equiv 3480 \bmod 3907$, $3480^{67} \equiv 2654 \bmod 3907$, and $2654^{67} \equiv 1765 \bmod 3907$.

To construct a class I pseudoprime, we choose any valid r, s values for an initial f_0, and select q as an I prime of f_0. We will choose $f_0 = x^3 - x^2 - x - 1$; i.e. $r_0 = 1$, $s_0 = -1$, and $q = 223$, which has $W(q) = 16651$. Now choose a prime p such that $p \equiv 1 \bmod W(q)$. We choose $p = 99907$, giving $pq = 22279261$. We now want to construct a function f_1 such that p is an S prime with respect to f_1, and whose roots are a, a^q, a^{q^2}, so that the product of the roots $= a^{q^2+q+1} = a^{kW(q)} \equiv 1 \bmod p$ for some k. We therefore need to solve $a^{W(q)} \equiv 1 \bmod p$. One solution is $a = 28$.

Our $f_1 \equiv (x-a)(x-a^q)(x-a^{q^2}) \bmod 99907 \equiv (x-28)(x-68226)(x-12159) \equiv (x^3 - 80413x^2 + 84939x - 1)$; i.e. $r_1 = 80413$, $s_1 = 84939$. We now find r, s such that $r \equiv r_0 \bmod q$, $s \equiv s_0 \bmod q$, $r \equiv r_1 \bmod p$, $s \equiv s_1 \bmod p$. Using the Chinese Remainder Theorem (or brute force), we obtain $r = 17963766$, $s = 8277313$, giving $\Delta \equiv 16900680 \bmod 222769261$.

The signature for 22279261 is $\{r, s, 3825018, 11218781, r, s\}$. We have $rs - 3 \equiv 15043799 \bmod 22279261 = 3825018 + 11218781$, and $(3825018 - 11218781)^2 \bmod 22279261 = 16900680 \equiv \Delta \bmod 22279261$, so the signature is a valid I signature i.e. 22279261 is an I pseudoprime with respect to $x^3 - 17963766x^2 + 8277313x - 1$.

Satisfying $p \equiv 1 \bmod W(q)$ is very difficult, because in general, $W(q)$ is of order q^2 for class I and class Q primes. Trying to construct class I or class Q pseudoprimes from class I and/or class Q primes is even more problematic, and we will need to use a technique of period reduction, which we now explain.

Let p be an odd Q or I prime with respect to $f = x^3 - rx^2 + sx - 1$, with $(x-\alpha)(x-\beta)(x-\gamma) = f \equiv 0 \bmod p$. If $W_f(p)$ is composite, let u be a factor of $W_f(p)$ such that $u(p-1)$ is not divisible by $W_f(p)$. Define $g = (x-\alpha^u)(x-\beta^u)(x-\gamma^u) = x^3 - (\alpha^u + \beta^u + \gamma^u)x^2 + (\alpha\beta\gamma)^u(\alpha^{-u} + \beta^{-u} + \gamma^{-u})x - (\alpha\beta\gamma)^u \equiv x^3 - a_f(u)x^2 + a_f(-u)x - 1 \bmod p$. Then $W_g(p) = W_f(p)/u$, and p is the same type of prime with respect to g as it was to f. This is because we required that $u(p-1)$ is not divisible by $W_f(p)$, so p

cannot be an S prime with respect to g. Furthermore, $\gcd(p^2+p+1, p^2-1) = \gcd(p+2, p^2-1) = \gcd(p+2, 2p+1) = \gcd(p+2, p-1) = \gcd(3, p-1) = 1$, so an I prime with respect to f cannot be a Q prime with respect to g, and vice versa.

As an example, we construct an I pseudoprime as the product of two I primes. We again choose $f_0 = x^3 - x^2 - x - 1$; i.e. $r_0 = 1$, $s_0 = -1$, and find a collection of I primes which have composite periods. Among these, we need to find two I primes p_1, p_2 such that $[p_1 \equiv 1 \bmod W(p_2)$ or $p_1 \equiv p_2 \bmod W(p_2)]$ and $[p_2 \equiv 1 \bmod W(p_1)$ or $p_2 \equiv p_1 \bmod W(p_1)]$.

We will choose $p_1 \equiv 1 \bmod W(p_2)$, $p_2 \equiv p_1 \bmod W(p_1)$. We therefore search for p_1, p_2 such that $G_1 = \gcd(p_1 - 1, W(p_2)) > 1$, $G_2 = \gcd(p_2 - p_1, W(p_1)) > 1$. We can then use period reduction to make $W(p_2) = G_1$, $W(p_1) = G_2$. For instance, $p_1 = 191$, $W(p_1) = 1183 \times 31$, $p_2 = 2557$, $W(p_2) = 7 \times 13 \times 19 \times 97 = 19 \times 8827$, giving $p_1 p_2 = 488387$, $G_1 = 19$, $G_2 = 1183$. The appropriate functions are therefore $f_1 = x^3 - a_{f_0}(31)x^2 + a_{f_0}(-31)x - 1 \equiv x^3 - 54x^2 + 183x - 1 \bmod 191$, $f_2 = x^3 - a_{f_0}(8827)x^2 + a_{f_0}(-8827)x - 1 \equiv x^3 - 687x^2 + 368x - 1 \bmod 2557$.

Solving for $r \equiv 54 \bmod 191$, $r \equiv 687 \bmod 2557$, $s \equiv 183 \bmod 191$, $s \equiv 368 \bmod 2557$, we get $r \equiv 64612 \bmod 488387$, $s \equiv 238169 \bmod 488387$, giving $\Delta \equiv 237085 \bmod 488387$.

The signature for 488387 is $\{r, s, 107935, 369894, r, s\}$. We have $rs - 3 \equiv 477829 \bmod 488387 = 107935 + 369894$, and $(107935 - 369894)^2 \bmod 488387 \equiv \Delta \bmod 488387$, so the signature is a valid I signature; i.e. 488387 is an I pseudoprime with respect to $x^3 - 64612x^2 + 238169x - 1$.

References

W. Adams, Characterizing Pseudoprimes for Third-Order Linear Recurrences, *Mathematics of Computation*, vol. 48 no. 177 (1987), pp. 1–15.

W. Adams and D. Shanks, Strong Primality Tests That Are Not Sufficient, *Mathematics of Computation*, vol. 39 no. 159 (1982), pp. 255–300.

S. Arno, A note on Perrin pseudoprimes, *Mathematics of Computation*, vol. 56 no. 193 (1991), pp. 371–376.

J. Grantham, There are infinitely many Perrin pseudoprimes, *Journal of Number Theory*, vol. 130 no. 5 (2010), pp. 1117–1128.

G. C. Kurtz, D. Shanks and H. C. Williams, Fast Primality Tests for Numbers Less Than $50 \cdot 10^9$, *Mathematics of Computation*, vol. 46 no. 174 (1986), pp. 691–701.

Solution 263.2 – Sequences

Show that the number of binary $\{0,1\}$ sequences of length n that do not contain two consecutive 1s is a Fibonacci number. For example, with $n = 4$ we have

$$\{0000, 0001, 0010, 0100, 0101, 1000, 1001, 1010\},$$

eight sequences, and indeed 8 is a Fibonacci number.

Is there an equally familiar characterization of decimal sequences that avoid consecutive nines? The numbers for $n = 1, 2, \ldots, 6$ are (TF thinks) 10, 99, 981, 9720, 96309, 954261.

Reinhardt Messerschmidt

Suppose b, r are positive integers with $b \geq 2$. Let $B = \{0, 1, \ldots, b-1\}$ and suppose $b_0 \in B$. For every positive integer n, let S_n be the set of all sequences consisting of n terms from B. Let W_n be the set of all elements of S_n that contain a subsequence of r consecutive b_0s, and let $X_n = S_n - W_n$. If $x \in S_n$ and $m = 1, 2, \ldots, n$, let $x|_m$ be the sequence consisting of the first m terms of x, i.e. $x|_m \in S_m$. Let Y_n be the set of all elements of W_n that achieve their first subsequence of r consecutive b_0s *before* their nth term. In other words,

$$Y_n = \begin{cases} \emptyset & \text{if } n = 1, 2, \ldots, r, \\ \left\{ x \in W_n : x|_{(n-1)} \in W_{n-1} \right\} & \text{if } n = r+1, r+2, \ldots. \end{cases}$$

Let Z_n be the set of all elements of S_n that achieve their first subsequence of r consecutive b_0s *at* their nth term. In other words,

$$Z_n = \begin{cases} \emptyset & \text{if } n = 1, 2, \ldots, r-1, \\ \{ \overbrace{(b_0, b_0, \ldots, b_0)}^{r \text{ terms}} \} & \text{if } n = r, \\ \left\{ x \in W_n : x|_{(n-1)} \in X_{n-1} \right\} & \text{if } n = r+1, r+2, \ldots. \end{cases}$$

Let w_n, x_n, y_n, z_n be the number of elements of W_n, X_n, Y_n, Z_n respectively. Let $X_0 = \{\emptyset\}$ and let x_0 be the number of elements of X_0, i.e. $x_0 = 1$.

If $n = 1, 2, \ldots, r-1$, then no element of S_n can contain a subsequence of r consecutive b_0s. If $n = r$, then exactly one element of S_n contains a subsequence of r consecutive b_0s. We therefore have the initial conditions

$$x_n = \begin{cases} b^n & \text{if } n = 0, 1, \ldots, r-1, \\ b^n - 1 & \text{if } n = r. \end{cases} \tag{1}$$

If $n = r+1, r+2, \ldots$, then $x \in Y_n$ if and only if x is the concatenation of a sequence from W_{n-1} and an arbitrary element of B. We therefore have

$$y_n \;=\; w_{n-1}b = (b^{n-1} - x_{n-1})b = b^n - bx_{n-1}.$$

Furthermore, $x \in Z_n$ if and only if x is the concatenation of a sequence from X_{n-r-1}, an element of B other than b_0, and r consecutive b_0s. We therefore have

$$z_n = x_{n-r-1}(b-1).$$

It follows that

$$\begin{aligned} x_n &= b^n - y_n - z_n \\ &= b^n - (b^n - bx_{n-1}) - (b-1)x_{n-r-1} \;=\; bx_{n-1} - (b-1)x_{n-r-1}, \end{aligned}$$

therefore

$$x_n - bx_{n-1} + (b-1)x_{n-r-1} \;=\; 0. \tag{2}$$

This is a homogeneous linear difference equation of order $r+1$ with constant coefficients. Methods for solving such equations are described in many textbooks, for example *Advanced Mathematical Methods for Scientists and Engineers* by Bender & Orszag. We will look at a few special cases.

Case 1. Suppose $b = r = 2$, then (1) and (2) become

$$x_0 = 1, \quad x_1 = 2, \quad x_2 = 3, \tag{3}$$

$$x_n - 2x_{n-1} + x_{n-3} = 0. \tag{4}$$

The initial values in (3) are Fibonacci numbers. If (x_n) satisfies the Fibonacci difference equation, i.e. $x_n = x_{n-1} + x_{n-2}$, then it also satisfies (4), because

$$\begin{aligned} x_n - 2x_{n-1} + x_{n-3} &= x_n - 2x_{n-1} + (x_{n-1} - x_{n-2}) \\ &= x_n - x_{n-1} - x_{n-2} \;=\; = 0. \end{aligned}$$

The Fibonacci sequence (suitably re-indexed) is therefore a solution to (3)-(4).

Case 2. Suppose $r = 2$ and b is arbitrary, then (1) and (2) become

$$x_0 = 1, \quad x_1 = b, \quad x_2 = b^2 - 1, \tag{5}$$

$$x_n - bx_{n-1} + (b-1)x_{n-3} = 0. \tag{6}$$

The characteristic polynomial of (6) is

$$\chi(\lambda) \;=\; \lambda^3 - b\lambda^2 + (b-1) \;=\; (\lambda - 1)\big[\lambda^2 + (1-b)\lambda + (1-b)\big].$$

Its roots are

$$\lambda_1 = 1, \quad \lambda_2 = (b - 1 + \mu)/2, \quad \lambda_3 = (b - 1 - \mu)/2, \tag{7}$$

where

$$\mu \;=\; \sqrt{b^2 + 2b - 3}.$$

Since $b \geq 2$ we have

$$\mu \;=\; \sqrt{b^2 + 2b - 3} \geq \sqrt{b^2} \;=\; b,$$

therefore

$$\lambda_2 \geq b - \tfrac{1}{2} \geq \tfrac{3}{2}, \quad \lambda_3 \leq -\tfrac{1}{2},$$

therefore the roots are distinct. It follows that the general solution of (6) is

$$x_n \;=\; c_1\lambda_1^n + c_2\lambda_2^n + c_3\lambda_3^n, \tag{8}$$

where c_1, c_2, c_3 are constants. By substituting (5) into (8) and using the identities

$$\begin{aligned} \lambda_2 - \lambda_3 \;&=\; \mu, \\ \lambda_2 + \lambda_3 \;&=\; -\lambda_2\lambda_3 \;=\; b - 1, \\ \lambda_2^2 \;&=\; (b-1)(\lambda_2 + 1), \\ \lambda_3^2 \;&=\; (b-1)(\lambda_3 + 1), \end{aligned}$$

we find

$$\begin{aligned} c_1 \;&=\; 0, \\ c_2 \;&=\; \frac{(b-1)^2(\lambda_3+1) - b^2(\lambda_3 - 1) - \mu - 2}{\mu(\mu+b)(\mu-b)}, \\ c_3 \;&=\; \frac{-(b-1)^2(\lambda_2+1) + b^2(\lambda_2 - 1) - \mu + 2}{\mu(\mu+b)(\mu-b)}. \end{aligned} \tag{9}$$

Case 3. If $r = 2$ and $b = 10$, then (7) and (9) give

$$\lambda_2 \approx 9.908327, \quad \lambda_3 \approx -0.908327, \quad c_2 \approx 1.008475, \quad c_3 \approx -0.008475,$$

therefore

$$x_n \approx (1.008475)(9.908327)^n + (-0.008475)(-0.908327)^n.$$

This formula confirms that

$$x_1 = 10, \;\; x_2 = 99, \;\; x_3 = 981, \;\; x_4 = 9720, \;\; x_5 = 96309, \;\; x_6 = 954261. \;\; \square$$

Towers of effort

Ralph Hancock

Interested, in M500 **267**, about the Tower of Hanoi I looked it up. I found that one of the variants of the legend, known as the Tower of Brahma, tells that an Indian temple contains a room with three posts and 64 golden discs which the priests are trying to shift, and that if they make one move a second it will take them $2^{64}-1$ seconds, about 585 billion years, to complete the move, after which the universe will come to an end.

So we have plenty of time yet, unless some idiot were to try to speed things up with a computer. On this matter, see Arthur C. Clarke's science fiction story of 1953 about Tibetan monks who have to list the nine billion names of God written with all the possible combinations of a holy alphabet, after which, similarly, it's all over. To save themselves effort, they rent a computer to list and print the names, and—even with a 1953 computer with about as much power as a cheap digital watch—the job is completed in three months.

The computer technicians are leaving from the airstrip when one of them looks up to the night sky. 'Overhead, without any fuss, the stars were going out.'

M500 Mathematics Revision Weekend 2016

The M500 Revision Weekend 2016 will be held at

Yarnfield Park Training and Conference Centre,
Yarnfield, Staffordshire ST15 0NL
from Friday 13th to Sunday 15th May 2016.

The standard cost, including accommodation (with en suite facilities) and all meals from dinner on Friday evening to lunch on Sunday is £285. The standard cost for non-residents, including Saturday and Sunday lunch, is £170. There will be an early booking period up to the 16th April with a discount of £20 for both members and non-members.

Members may make a reservation with a £25 deposit, with the balance payable at the end of February. Non-members must pay in full at the time of application and all applications received after the 28th February must be paid in full before the booking is confirmed. Members will be entitled to a discount of £15 for all applications. A shuttle bus service will be provided between Stone station and Yarnfield Park on Friday and Sunday. This will be free of charge, but seats will be allocated for each service and must be requested before 1st May. There is free on-site parking for those travelling by private transport. For full details and an application form see the Society's web site at www.m500.org.uk.

The Weekend is open to all Open University students, and is designed to help with revision and exam preparation. We expect to offer tutorials for most undergraduate and postgraduate mathematics OU modules, subject to the availability of tutors and sufficient applications.

04.00

Problem 269.8 – Integral

Show that

$$\int_{-\infty}^{\infty} \frac{\cos x}{1+x^4}\,dx \;=\; \frac{\pi\left(\cos(1/\sqrt{2})+\sin(1/\sqrt{2})\right)}{\sqrt{2}\,e^{1/\sqrt{2}}} \;\approx\; 1.54428.$$

Just in case it might be relevant, recall that in Problem 242.1 we asked you for a proof that $\int_{-\infty}^{\infty} \cos x/(1+x^2)\,dx = \pi/e$.

Front cover The vertex-edge graph of the truncated cuboctahedron. (The Archimedean solid is on the cover of issue 232.)