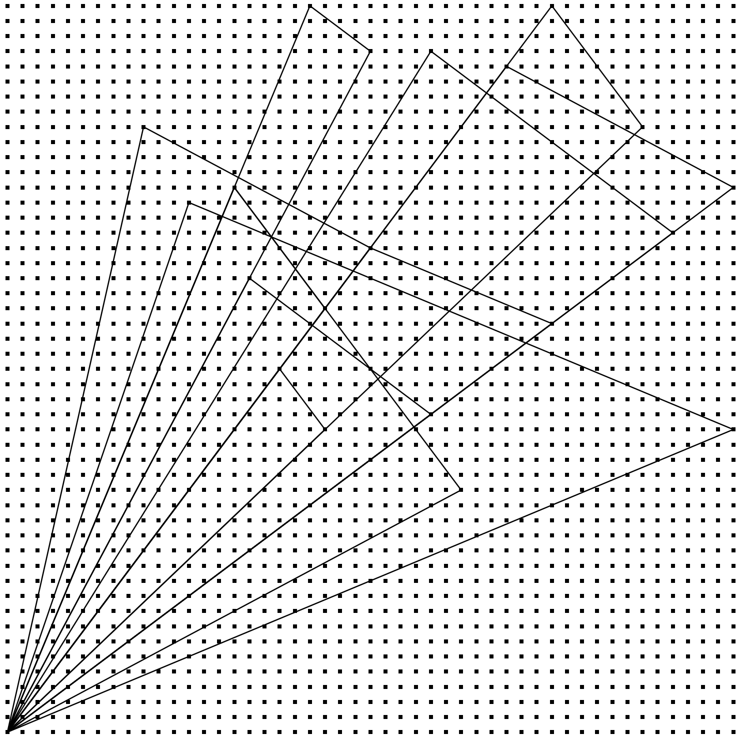
*

ISSN 1350-8539

M500 268



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.

Primes, sums of two squares, and palindromic continued fractions

Roger Thompson

Introduction

Every prime p of the form $4N + 1$ can be expressed as the sum of two squares. Here is a very fast algorithm for calculating these squares.

Find a prime q that is not a quadratic residue of p, i.e. $q^{2N} \equiv -1 \bmod p$. Let $x = q^N \bmod p$. If $x > p/2$, then set $x := p - x$. If $x^2 + 1 = p$, we are finished, otherwise iterate the steps involved in calculating $\gcd(p, x)$.This is done as follows: Let $A = p, B = x$. Set $C := A \bmod B, R := (A - C)/B$. Set $A := B, B := C$, and repeat until $A < \sqrt{p}$. Then $A^2 + B^2 = p$.

Example: $p = 193$, so that $N = 48$. The lowest q that is not a quadratic residue of p is 5. Now $5^N \equiv 112 \bmod p$, so we use $x = 193 - 112 = 81$. At the entry marked with ****, $A < \sqrt{193}$. This occurs at row K say, so denoting $A_K = A, B_K = B$ at this point, we find $A_K^2 + B_K^2 = 12^2 + 7^2 = 193$. However, if we carry on to the conclusion of the gcd calculation, i.e. when $B = 1$, we notice that the sequence of R values is palindromic.

A	B	R	
193	81	2	
81	31	2	
31	19	1	
19	12	1	
12	7	1	****
7	5	1	
5	2	2	
2	1	2	

By definition, the continued fraction for $81/193$ is $[2, 2, 1, 1, 1, 1, 2, 2]$. Perhaps surprisingly, the continued fraction for $B_K/A_K = 7/12$ is $[1, 1, 2, 2]$, and the convergents for the continued fraction $[2, 2, 1, 1]$ are 1/2, 2/5, 3/7, 5/12, with the denominators of the last two convergents being B_K and A_K.

To discover how the above algorithm works, we need to explore the properties of palindromic continued fractions.

Palindromic continued fractions and the algorithm

Denoting the nth partial quotient (starting from $n = 1$) by a_n and the nth convergent by r_n/s_n, we will use the following standard properties of continued fractions:

$$\begin{aligned} r_{n-1}s_n - r_n s_{n-1} &= (-1)^n, \\ r_n &= a_n r_{n-1} + r_{n-2}, \\ s_n &= a_n s_{n-1} + s_{n-2}. \end{aligned}$$

We first look at concatenating two continued fractions. Let

$$[a_1, a_2, \cdots, a_n] \;=\; \frac{r_n}{s_n}, \quad [b_1, b_2, \cdots, b_n] \;=\; \frac{t_n}{u_n}.$$

Then by replacing partial quotient a_n with $a_n + t_n/u_n$, we find that the concatenated continued fraction $[a_1, a_2, \cdots, a_n, b_1, b_2, \cdots, b_n]$ is

$$\frac{\left(a_n + \dfrac{t_n}{u_n}\right) r_{n-1} + r_{n-2}}{\left(a_n + \dfrac{t_n}{u_n}\right) s_{n-1} + s_{n-2}} = \frac{u_n(a_n r_{n-1} + r_{n-2}) + t_n r_{n-1}}{u_n(a_n s_{n-1} + s_{n-2}) + t_n s_{n-1}} = \frac{u_n r_n + t_n r_{n-1}}{u_n s_n + t_n s_{n-1}}.$$

Next, we look at the continued fraction $[a_n, a_{n-1}, \cdots, a_1]$, where $[a_1, a_2, \cdots, a_n] = r_n/s_n$. Since $s_n = a_n s_{n-1} + s_{n-2}$, we have

$$\frac{s_{n-1}}{s_n} \;=\; \frac{1}{a_n + \dfrac{s_{n-2}}{s_{n-1}}}.$$

We repeat for s_{n-2}/s_{n-1} etc. Finally, $s_1/s_0 = a_1 + s_{-1}/s_0 = a_1$ since $s_0 = 1, s_{-1} = 0$, so $s_0/s_1 = 1/a_1$, giving $[a_n, a_{n-1}, \cdots, a_1] = s_{n-1}/s_n$. Substituting into the concatenation expression derived above, we have

$$[a_1, a_2, \cdots, a_n, a_n, a_{n-1}, \cdots, a_1] \;=\; \frac{r_n s_n + r_{n-1}}{s_n^2 + s_{n-1}^2} \;=\; \frac{x}{p},$$

say (not entirely arbitrarily)! We have

$$\begin{aligned} x^2 + 1 \;&=\; r_{n-1}^2 s_{n-1}^2 + r_n^2 s_n^2 + 2 r_{n-1} s_n r_n s_{n-1} + 1 \\ &=\; (r_{n-1}^2 + r_n^2)p + 2 r_{n-1} s_n r_n s_{n-1} - r_n^2 s_{n-1}^2 - r_{n-1}^2 s_n^2 + 1. \end{aligned}$$

Using $r_{n-1}s_n - r_n s_{n-1} = (-1)^n$ and some messy algebra, all but the first term cancel out, leaving $x^2 + 1 = (r_{n-1}^2 + r_n^2)p$, and of course $s_n^2 + s_{n-1}^2 = p$.

We have shown that palindromic continued fractions give rise to x and p with the right properties, but we need to show that for x and p to have the right properties, the corresponding continued fraction must be palindromic. This is very straightforward. A necessary (but not sufficient) condition for a, b with $a < b$, where $a^2 + b^2$ is prime, is that $\gcd(a, b) = 1$. All we therefore have to show is that it is possible, for any such a and b, to construct a continued fraction with $s_{n-1} = a, s_n = b$. This is easy, for we have already done it. Namely, take the continued fraction for a/b and reverse the order of the partial quotients.

It should also now be apparent why x was constructed as it was. By construction, $x = q^N \bmod p$, where $q^{2N} \equiv -1 \bmod p$, so x^2+1 is a multiple of p, and from above, we now know what that multiple is. In our example, $r_{n-1} = 3, r_n = 5$, so $x^2 + 1 = 6562 = (3^2 + 5^2)193$.

Next, we have to show how s_n, s_{n-1} turn up as A, B entries. From the definition of the A, we have $A_{n-1} = A_n R_{n-1} + A_{n+1}$. If we remap the order of the A so that $n + k \to m - k - 1$, we have $A_m = A_{m-1} R_m + A_{m-2}$, the relationship for evaluating a continued fraction, so the A_n, reading backwards, are successive denominators of $[a_n, a_{n-1}, \cdots, a_1]$. Since $B_{m+1} = A_m$ (still reading backwards), there will be an entry with $A = s_n, B = s_{n-1}$.

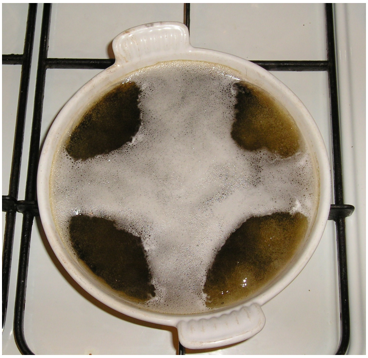
Finally, we need to see why the first $A < \sqrt{p}$ identifies A_K, B_K such that $A_K^2 + B_K^2 = p$. Reading forward again, we have $A_{K-1} = A_K R_{K-1} + B_K$, $B_{k-1} = A_K$, so $A_{K-1}^2 \geq (A_K + B_K)^2 > A_K^2 + B_K^2 = p$, so $A_{K-1} > \sqrt{p}$.

Reference

S. Wagon (1990) 'Editor's Corner: The Euclidean Algorithm Strikes Again', *The American Mathematical Monthly*, Vol. 97, No. 2, pp 125–129.

Mathematics in the kitchen – X

Tony Forbes



I think this experiment requires a gas-operated cooking device. Take a shallow vessel of diameter about 20 cm, place it on the stove and almost fill it with water. Add a small amount of washing-up liquid; about 25ml should suffice. Heat. When the water has reached boiling point adjust the gas so that the mixture is simmering vigorously. Observe.

When I did it I was surprised to see a neat cross-like pattern develop and then maintain itself with remarkable stability. Can anyone explain? I suspect that the alignment of the four iron supports with the four arms of the cross might not be entirely coincidental. The dark coloration is irrelevant; it is merely the result of a previous overcooking incident.

Please do not perform this experiment unless you are willing to accept full responsibility for accidents. Boiling water is dangerous and can cause severe scalding.

Solution 264.3 – Determinant

> An $n \times n$ matrix has a in each entry on the diagonal and b everywhere else. What is its determinant?

Edward Stansfield

Solution

The determinant is given by

$$(a-b)^{n-1}[a+(n-1)b].$$

Preface to proof

At first sight I thought that the solution to this problem would have a simple expression, and a quick experiment with MATHEMATICA confirmed that this is indeed the case (as shown above). However, when I set about trying to prove what MATHEMATICA suggested, it turned out to be far from easy. I tried various matrix decompositions, all to no avail, until I came across a proof of 'Sylvester's Determinant Theorem'. One version of this states that for suitably dimensioned (not necessarily square) matrices A and B, $\det(I+AB) = \det(I+BA)$, where I is an identity matrix. The proof of this theorem provided me with a clue to finding a solution. The proof involves a square matrix Q of dimension $n+p$, containing a sub-matrix A with dimension $p \times n$ and a sub-matrix B with dimension $n \times p$, such that it has the partitioned form and a block LU decomposition given by

$$Q \;=\; \begin{pmatrix} I_p & -A \\ B & I_n \end{pmatrix} \;=\; \begin{pmatrix} I_p & 0 \\ B & I_n \end{pmatrix} \begin{pmatrix} I_p & -A \\ 0 & I_n+BA \end{pmatrix}.$$

In this equation, I_p is an identity matrix of order p, and similarly I_n is an identity matrix of order n. It turns out that the determinant of Q is given by

$$\det(Q) \;=\; \det(I_n+BA).$$

To see this, observe that, since the left-hand matrix of the block LU decomposed form is lower triangular with unity values along the main diagonal, its determinant is unity. This can be shown by expanding along the top row to reduce the dimension by one, and repeating this process until the dimension is just one. For the right-hand matrix of the block LU decomposition, we can expand along the first column to reduce the dimension by one. This process can be repeated p times, at which point we are left with just the determinant of the lower right-hand side sub-matrix. The result immediately follows.

Proof

Let H_n be the $n \times n$ matrix of the desired form, which can be written as

$$H_n = \begin{pmatrix} a & b & b & \dots & b \\ b & a & b & \dots & b \\ b & b & a & \dots & b \\ \dots & \dots & \dots & \dots & \dots \\ b & b & b & \dots & a \end{pmatrix} = (a-b)I_n + b\, i_n\, i_n^{\mathrm{T}}$$

$$= (a-b)\left(I_n + \frac{b}{a-b}\, i_n\, i_n^{\mathrm{T}}\right) = (a-b)P_n.$$

Here, i_n is a unity column vector of length n (i.e. every element is unity). Observe that

$$\det(H_n) = (a-b)^n \det(P_n).$$

Next consider a related square matrix Q_{n+1} of order $n+1$ whose partitioned and block LU decomposed form is given by

$$Q_{n+1} = \begin{pmatrix} 1 & -\beta\, i_n^{\mathrm{T}} \\ \beta\, i_n & I_n \end{pmatrix} = \begin{pmatrix} 1 & \phi_n^{\mathrm{T}} \\ \beta\, i_n & I_n \end{pmatrix} \begin{pmatrix} 1 & -\beta\, i_n^{\mathrm{T}} \\ \phi_n & I_n + \beta^2\, i_n\, i_n^{\mathrm{T}} \end{pmatrix}.$$

Here, ϕ_n is a zero vector of length n. The left-hand matrix in the decomposed form is lower-triangular with unity values on the main diagonal, and hence its determinant is unity. The determinant of the right-hand matrix in the decomposed form is $\det(I_n + \beta^2\, i_n\, i_n^{\mathrm{T}})$. If we set $\beta = \sqrt{b/(a-b)}$ then it can be seen that

$$\det(Q_{n+1}) = \det(P_n).$$

Observe mow that Q_{n+1} has the (recursive) partitioned form

$$Q_{n+1} = \begin{pmatrix} Q_n & -\beta\, j_n \\ \beta\, j_n^{\mathrm{T}} & 1 \end{pmatrix}.$$

Here, j_n is a column vector of length n whose first element is unity and all other elements are zero. This suggests that $\det(Q_{n+1})$ can be expressed simply in terms $\det(Q_n)$ if we expand along the bottom row, which contains just two non-zero elements. That is,

$$\det(Q_{n+1}) = \beta(-)^{n+2} m_{n+1,1} + (-)^{2n+2} \det(Q_n).$$

In this equation, $m_{n+1,1}$ is the minor of Q_{n+1} when row $n+1$ and column 1 are deleted. By expanding down column n, which contains just one non-zero element, this takes the form

$$m_{n+1,1} = \det\begin{pmatrix} -\beta\, i_{n-1}^{\mathrm{T}} & -\beta \\ I_{n-1} & \phi_n \end{pmatrix} = -\beta(-)^{n+1} \det(I_{n-1}) = -\beta(-)^{n+1}.$$

Back substitution back then yields the following recursion for $\det(Q_n)$:

$$\det(Q_{n+1}) \;=\; \det(Q_n) + \beta^2.$$

Starting with $\det(Q_2) \;=\; 1+\beta^2$ we quickly obtain by induction the general case $\det(Q_{n+1}) \;=\; 1 + n\beta^2$. Finally, again with $\beta = \sqrt{b/(a-b)}$, we have that

$$\det(H_n) \;=\; (a{-}b)^n \det(P_n) \;=\; (a{-}b)^n \det(Q_{n+1}) \;=\; (a{-}b)^n \left(1 + n\,\frac{b}{a-b}\right).$$

This leads directly to the result:

$$\det(H_n) \;=\; (a-b)^{n-1}[a + (n-1)b].$$

I found it very satisfying to discover that this formula is exactly what my Mathematica program had suggested some days previously.

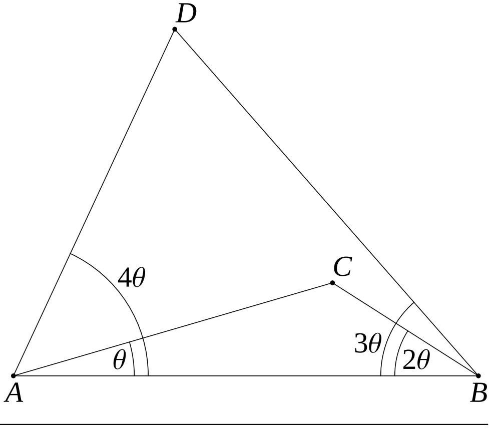
Conclusion

This really is a deceptively simple problem with a simple solution, but my proof is certainly not trivial. I cannot but wonder if there is a much simpler way to prove the simple formula for the determinant. I look forward to receiving future issues of the M500 Magazine to see if anyone has succeeded in finding one.

Problem 268.1 – Two triangles

Find two triangles ABC and ABD (so that they share a common base) such that (i) angles CAB, CBA, DBA and DAB are in the ratio $1:2:3:4$, and (ii) $|AB|$, $|AC|$, $|BC|$, $|DA|$ and $|DB|$ are positive integers.

I (TF) am of the opinion that it is difficult to make $|DC|$ an integer as well. Thanks to Dick Boardman for suggesting this problem.



Solution 232.2 – Angles

Suppose $A + B + C = 45^\circ$. Show that

$$\begin{aligned}(\cos A + \sin A)(\cos B + \sin B)(\cos C + \sin C)&\\ = 2(\cos A \cos B \cos C + \sin A \sin B \sin C).&\end{aligned}$$

Dave Wild

We have

$$\begin{aligned}&(\cos B + \sin B)(\cos C + \sin C)\\ &\quad= (\cos B \cos C + \sin B \sin C) + (\sin B \cos C + \cos B \sin C)\\ &\quad= \cos(B + C) + 2 \sin B \sin C + \sin(B + C)\\ &\qquad \text{or} \quad -\cos(B + C) + 2 \cos B \cos C + \sin(B + C).\end{aligned}$$

So

$$\begin{aligned}&(\cos A + \sin A)(\cos B + \sin B)(\cos C + \sin C)\\ &\quad= \cos A(-\cos(B + C) + 2 \cos B \cos C + \sin(B + C))\\ &\qquad + \sin A(\cos(B + C) + 2 \sin B \sin C + \sin(B + C))\\ &\quad= 2(\cos A \cos B \cos C + \sin A \sin B \sin C) + (\sin(B + C) \cos A\\ &\qquad + \cos(B + C) \sin A) - (\cos A \cos(B + C) - \sin A \sin(B + C))\\ &\quad= 2(\cos A \cos B \cos C + \sin A \sin B \sin C)\\ &\qquad + \sin(A + B + C) - \cos(A + B + C).\end{aligned}$$

Therefore if, as in this problem, $\sin(A+B+C) = \cos(A+B+C)$ then the given identity is satisfied.

Problem 268.2 – Induction

What's wrong with this argument? We wish to prove that

$$\sum_{k=1}^{n} k = O(n). \qquad (*)$$

Clearly $\sum_{k=1}^{1} k = 1 = O(1)$. Using induction, we assume $(*)$ is true for some $n \geq 1$. Then we have $\sum_{k=1}^{n+1} k = O(n) + n + 1 = O(n + 1)$. Hence $(*)$ is true for all $n \geq 1$. □

A nice result except that it is actually false. On the other hand, it is true that $\sum_{k=1}^{n} k = O(n^2)$.

Solution 188.1 – Ones

> Throw n dice. The total score is s. What is the expected number of ones?

Reinhardt Messerschmidt

We will:

- summarize some facts about the discrete uniform distribution and sums of independent discrete uniform random variables;
- derive the exact conditional distribution of the number of ones given the total score;
- generate a numerical example;
- approximate the exact distribution with the normal distribution for large n.

For the necessary background knowledge on probability generating functions, the central limit theorem and the bivariate normal distribution, see (for example) *Introduction to Probability and Mathematical Statistics* by L. J. Bain & M. Engelhardt.

The discrete uniform distribution

Suppose a, b are non-negative integers with $a \le b$. The *discrete uniform distribution* with start point a and end point b is the distribution that assigns a probability of $1/(b-a+1)$ to each of the elements of $\{a, a+1, \ldots, b\}$. It will be denoted by $\mathrm{DU}(a,b)$. If U is a $\mathrm{DU}(a,b)$ random variable, then its expected value is

$$\frac{1}{b-a+1}\sum_{j=0}^{b-a}(a+j) \;=\; \frac{a+b}{2},$$

and its variance is

$$\begin{aligned}
&\frac{1}{b-a+1}\sum_{j=0}^{b-a}(a+j)^2 - \left(\frac{a+b}{2}\right)^2 \\
&= \frac{1}{b-a+1}\left(a^2\sum_{j=0}^{b-a}1 + 2a\sum_{j=0}^{b-a}j + \sum_{j=0}^{b-a}j^2\right) - \left(\frac{a+b}{2}\right)^2 \\
&= \frac{(b-a+1)^2-1}{12}.
\end{aligned}$$

The probability generating function G_U of U is

$$G_U(z) \;=\; \mathbb{E}[z^U] \;=\; \frac{1}{b-a+1}\sum_{j=0}^{b-a} z^{a+j} \;=\; \frac{z^a}{b-a+1}\frac{1-z^{b-a+1}}{1-z}.$$

Sums of independent discrete uniform random variables

Suppose $U_1, U_2, \ldots, U_m$ are independent $\mathrm{DU}(a,b)$ random variables. The expected value of $\sum_{j=1}^{m} U_j$ is

$$\sum_{j=1}^{m} \mathbb{E}[U_j] \;=\; \frac{m(a+b)}{2},$$

and its variance is

$$\sum_{j=1}^{m} \mathrm{var}[U_j] \;=\; \frac{m((b-a+1)^2-1)}{12}.$$

The probability generating function $G_{(\sum U_j)}$ of $\sum U_j$ is

$$G_{(\sum U_j)}(z) \;=\; \mathbb{E}\Big[z^{\sum_{j=1}^{m} U_j}\Big] \;=\; \prod_{j=1}^{m} G_{U_j}(z) \;=\; \frac{z^{am}}{c^m}\left(\frac{1-z^c}{1-z}\right)^m,$$

where $c = b-a+1$. By the binomial theorem,

$$(1-z^c)^m \;=\; \sum_{j=0}^{m}\binom{m}{j}(-z^c)^j 1^{m-j} \;=\; \sum_{j=0}^{m}(-1)^j\binom{m}{j}z^{cj},$$

and by Taylor's theorem,

$$\frac{1}{(1-z)^m} \;=\; \sum_{k=0}^{\infty}\binom{m+k-1}{m-1}z^k;$$

therefore

$$G_{(\sum U_j)}(z) \;=\; \frac{1}{c^m}\sum_{j=0}^{m}\sum_{k=0}^{\infty}(-1)^j\binom{m}{j}\binom{m+k-1}{m-1}z^{am+cj+k}.$$

Substituting $r = am+cj+k$,

$$G_{(\sum U_j)}(z) \;=\; \frac{1}{c^m}\sum_{j=0}^{m}\sum_{r=am+cj}^{\infty}(-1)^j\binom{m}{j}\binom{r-(a-1)m-cj-1}{m-1}z^r.$$

Changing the order of summation,

$$G_{(\sum U_j)}(z)$$

$$= \sum_{r=am}^{\infty} \left[\frac{1}{c^m} \sum_{j=0}^{\lfloor (r-am)/c \rfloor} (-1)^j \binom{m}{j} \binom{r-(a-1)m-cj-1}{m-1} \right] z^r. \qquad (1)$$

By the properties of probability generating functions, $\mathbb{P}[\sum U_j = r]$ is equal to the coefficient of z^r in (1). Since $\sum U_j \leq bm$ with probability 1, the coefficients of z^{bm+1}, z^{bm+2}, ... simplify to 0.

Exact conditional distribution of number of ones given the total score

Suppose d is an integer with $d \geq 2$ and $X_1, X_2, \ldots, X_n$ are independent $\mathrm{DU}(1,d)$ random variables. If $d = 6$ then $X_1, X_2, \ldots, X_n$ represent n dice rolls. Let Y_n be the number of elements in the sequence $(X_1, X_2, \ldots, X_n)$ that are 1. The random variable Y_n has a binomial distribution with parameters n and $1/d$, therefore if $y \in \{0, 1, \ldots, n\}$ then

$$\mathbb{P}[Y_n = y] \;=\; \binom{n}{y} \left(\frac{1}{d}\right)^y \left(1 - \frac{1}{d}\right)^{n-y}.$$

Let $S_n = \sum_{j=1}^{n} X_j$. The probability $\mathbb{P}[S_n = s]$ is equal to the coefficient of z^s in (1), with $a = 1$, $b = d$, $c = d$ and $m = n$.

For the conditional probability $\mathbb{P}[Y_n = y \,|\, S_n = s]$ to exist, we must have $s \in \{n, n+1, \ldots, dn\}$, otherwise $\mathbb{P}[S_n = s] = 0$. Since Y_n of the elements in $(X_1, X_2, \ldots, X_n)$ are 1, the remaining $n - Y_n$ elements have values in $\{2, 3, \ldots, d\}$, therefore

$$Y_n + 2(n - Y_n) \;\leq\; S_n \;\leq\; Y_n + d(n - Y_n)$$

with probability 1. This implies that, given $s \in \{n, n+1, \ldots, dn\}$, the probability $\mathbb{P}[Y_n = y \,|\, S_n = s]$ will be positive if and only if $y \in \{0, 1, \ldots, n\}$ and

$$y + 2(n - y) \;\leq\; s \;\leq\; y + d(n - y),$$

i.e. if and only if $y \in \{0, 1, \ldots, n\}$ and

$$2n - s \;\leq\; y \;\leq\; \frac{dn - s}{d - 1}.$$

If (y, s) is such that $\mathbb{P}[Y_n = y \mid S_n = s]$ exists and is positive, then

$$\begin{aligned}\mathbb{P}[Y_n = y \mid S_n = s] &= \frac{\mathbb{P}[Y_n = y,\ S_n = s]}{\mathbb{P}[S_n = s]} = \frac{\mathbb{P}[S_n = s \mid Y_n = y]\ \mathbb{P}[Y_n = y]}{\mathbb{P}[S_n = s]} \\ &= \frac{\mathbb{P}[T_{n-y} = s - y]\ \mathbb{P}[Y_n = y]}{\mathbb{P}[S_n = s]},\end{aligned}$$

where T_{n-y} is the sum of $n - y$ independent $\mathrm{DU}(2, d)$ random variables. The probability $\mathbb{P}[T_{n-y} = s - y]$ is equal to the coefficient of z^{s-y} in (1), with $a = 2$, $b = d$, $c = d - 1$ and $m = n - y$. It follows that

$$\mathbb{P}[Y_n = y \mid S_n = s] = \frac{\displaystyle\binom{n}{y} \sum_{j=0}^{\lfloor (s-2n+y)/(d-1) \rfloor} (-1)^j \binom{n-y}{j} \binom{s-n-(d-1)j-1}{n-y-1}}{\displaystyle\sum_{j=0}^{\lfloor (s-n)/d \rfloor} (-1)^j \binom{n}{j} \binom{s-dj-1}{n-1}}.$$

Numerical example

Let $d = 3$ and $n = 8$. The following table shows the unconditional distribution of Y_n and its conditional distributions given small, medium and large values of S_n (with rounding to four decimal places).

y	$\mathbb{P}[Y_n = y]$	$\mathbb{P}[Y_n = y \mid S_n = s]$		
		$s = 12$	$s = 16$	$s = 20$
0	0.0390		0.0009	0.2632
1	0.1561		0.0506	0.6316
2	0.2731		0.3794	0.1053
3	0.2731		0.5059	
4	0.1707	0.2632	0.0632	
5	0.0683	0.6316		
6	0.0171	0.1053		
7	0.0024			
8	0.0002			
$\mathbb{E}[\cdot]$	2.6667	4.8421	2.5799	0.8421
$\sqrt{\mathrm{var}[\cdot]}$	1.3333	0.5861	0.6904	0.5861

Approximation of the exact distribution with the normal distribution

We have

$$\begin{aligned} \mathbb{E}[Y_n] &= \frac{n}{d}, & \operatorname{var}[Y_n] &= \frac{n}{d}\left(1 - \frac{1}{d}\right), \\ \mathbb{E}[S_n] &= \frac{n(d+1)}{2}, & \operatorname{var}[S_n] &= \frac{n(d^2-1)}{12}. \end{aligned}$$

Furthermore,

$$\begin{aligned} \mathbb{E}[Y_n S_n] &= \sum_y \sum_s ys\, \mathbb{P}[Y_n = y,\ S_n = s] \\ &= \sum_y \sum_s ys\, \mathbb{P}[S_n = s \mid Y_n = y]\, \mathbb{P}[Y_n = y] \\ &= \sum_y y\, \mathbb{P}[Y_n = y] \sum_s s\, \mathbb{P}[T_{n-y} = s - y] \\ &= \sum_y y\, \mathbb{P}[Y_n = y] \sum_t (y+t)\, \mathbb{P}[T_{n-y} = t] \\ &= \sum_y y^2\, \mathbb{P}[Y_n = y] + \sum_y y\, \mathbb{P}[Y_n = y]\, \mathbb{E}[T_{n-y}] \\ &= \sum_y y^2\, \mathbb{P}[Y_n = y] + \sum_y y\, \mathbb{P}[Y_n = y] \frac{(n-y)(d+2)}{2} \\ &= \mathbb{E}[Y_n^2] + \frac{n(d+2)}{2}\, \mathbb{E}[Y_n] - \frac{d+2}{2}\, \mathbb{E}[Y_n^2] \\ &= \frac{n^2(d+1) - n(d-1)}{2d}; \end{aligned}$$

therefore

$$\operatorname{cov}[Y_n, S_n] = \mathbb{E}[Y_n S_n] - \mathbb{E}[Y_n]\mathbb{E}[S_n] = \frac{-n(d-1)}{2d}.$$

By the central limit theorem, if n is large then the distribution of (Y_n, S_n) is approximately bivariate normal. By the properties of the bivariate normal distribution, the conditional distribution of Y_n given $S_n = s$ is approximately normal with expected value

$$\mathbb{E}[Y_n] + \frac{\operatorname{cov}[Y_n, S_n]}{\operatorname{var}[S_n]}(s - \mathbb{E}[S_n]) \;=\; \frac{n}{d} - \frac{6}{d(d+1)}\left(s - \frac{n(d+1)}{2}\right), \qquad (2)$$

and variance

$$\operatorname{var}[Y_n] - \frac{\operatorname{cov}[Y_n, S_n]^2}{\operatorname{var}[S_n]} \;=\; \frac{n}{d}\left(1 - \frac{1}{d}\right) - \frac{3n(d-1)}{d^2(d+1)}.$$

Equation (2) confirms that $\mathbb{E}[Y_n \mid S_n = s] \approx \mathbb{E}[Y_n]$ if $s = \mathbb{E}[S_n]$, and that $\mathbb{E}[Y_n \mid S_n = s]$ is approximately linear in s.

Problem 268.3 – Sequences

Let S_1 denote the sequence $(1/2!)$. Suppose $S_n = (s_1, s_2, \ldots, s_N)$, where $N = 2^{n-1}$. For $i = 1, 2, \ldots, N$, suppose $s_i = \dfrac{\pm 1}{a_i!\, b_i! \ldots}$, where the ordering of the factorials is relevant, and from s_i create two new expressions,

$$s_i' \;=\; \frac{\mp 1}{(a_i+1)!\, b_i! \ldots} \quad\text{and}\quad s_i'' \;=\; \frac{\pm 1}{2!\, a_i!\, b_i! \ldots}.$$

Define $S_{n+1} = (s_1', s_1'', s_2', s_2'', \ldots, s_N', s_N'')$. Thus

$$S_2 \;=\; \left(\frac{-1}{3!}, \frac{1}{2!\,2!}\right), \qquad S_3 \;=\; \left(\frac{1}{4!}, \frac{-1}{2!\,3!}, \frac{-1}{3!\,2!}, \frac{1}{2!\,2!\,2!}\right),$$

$$S_4 \;=\; \left(\frac{-1}{5!}, \frac{1}{2!\,4!}, \frac{1}{3!\,3!}, \frac{-1}{2!\,2!\,3!}, \frac{1}{4!\,2!}, \frac{-1}{2!\,3!\,2!}, \frac{-1}{3!\,2!\,2!}, \frac{1}{2!\,2!\,2!\,2!}\right),$$

and so on, with the number of terms doubling at each step.

Now for the problem. Prove that when n is odd and greater than 1 the terms in S_n sum to zero.

The construction is due to S. C. Woon (Generalization of a relation between the Riemann zeta function and Bernoulli numbers, arXiv: math/9812143v1) and the sum is actually $B_n/n!$, where B_n is the n-th Bernoulli number; see also *Theorem of the Day* number 238, which can be found at http://www.theoremoftheday.org/. However, for odd n, we are particularly interested in a simple solution that avoids explicit reference to the Bernoulli numbers.

Solution 245.10 – Every other day

> Find a simple function F, say, that maps a date to either 0 or 1 such that $F(\text{today}) = 1 - F(\text{yesterday})$. This is not just an academic exercise. Such a function will be very useful in those situations where the label on the packet says, 'Take 1 tablet every 2 days'.

Mike Lewis

The Julian Day Number is the continuous count of days since the beginning of the Julian Period and is primarily used by astronomers. Clearly a function or algorithm based on determining the parity of this quantity would satisfy the requirement implied in the problem statement. Although it is not a function, an algorithm for determining the Day Number exists [1].

A Little History

The *Julian day number* is based on the *Julian Period* proposed by Joseph Scaliger (1540 – 1609) in 1583, at the time of the Gregorian calendar reform, as it is the least common multiple of the length in years of three calendar cycles used with the Julian calendar:

> 15 (Indiction cycle – a dating system for medieval manuscripts) × 19 (Metonic cycle – 19 years is almost exactly equal to 235 lunar months) × 28 (Solar cycle – 7 possible start days to a leap year and the 4 year interval) = 7980 years.

Its epoch falls at the last time when the first year of all three cycles (if they are continued backward far enough) coincided. Scaliger chose this because it preceded all historical dates. Years of the Julian Period are counted from the year 4713 BC, which was chosen to be before any historical record [2]. The start of the period now used is 4800 BC.

Having established this highly unlikely set of numbers as a basis for the algorithm we will now proceed.

Calculating the Day Number

Adjustment for first month of the year in the Julian Calendar,

$$a = \left\lfloor \frac{14 - \text{month}}{12} \right\rfloor$$

results in 1 for January (month 1) and February (month 2). The result is 0 for the other 10 months.

Calculate the Julian Year,

$$y = \text{year} + 4800 - a.$$

Calculate Julian Month Number,

$$m \; = \; \text{month} + 12a - 3.$$

The effect of the combined calculation of y and m is to adjust for the year beginning in March and ending in February in accordance with the Julian Calendar.

Calculate the Julian Day Number, JDN,

$$\text{JDN} \; = \; \text{day} + \left\lfloor \frac{153m+2}{5} \right\rfloor + 365y + \left\lfloor \frac{y}{4} \right\rfloor - \left\lfloor \frac{y}{100} \right\rfloor + \left\lfloor \frac{y}{400} \right\rfloor - 32045;$$

day is the day of the month, and $\lfloor (153m+2)/5 \rfloor$ calculates the number of days in the months prior to the first month of the Julian Year. The next four terms calculate the number of days in a year adjusted for leap years and 32045 adjusts for the Julian Date January 1st 4713 BC being day 0 on the Julian Calendar.

The final part of the calculation is to determine the JDN for the start of the sequence of days and check its parity. Subsequently it is only necessary to calculate the JDN for each day as it occurs and only take whatever action is called for on the days that have the same parity as the first day.

Date Converters

A Julian Date Converter can be found at the US Naval observatory site http://aa.usno.navy.mil/data/docs/JulianDate.php.

MATLAB has a function juliandate. EXCEL has a function DATEVALUE that converts a text format date to the date number based on January 1st 1900. This is used within the spreadsheet and can be used to calculate a date a given number of days ahead from the current or some other date. Useful for calculating the dates of payments, such as pensions, made at 28 day intervals.

References

[1] CS 1063 *Introduction to Programming: Explanation of Julian Day Number Calculation.* (2011). Computer Science Department, University of Texas at San Antonio. http://www.cs.utsa.edu/∼cs1063/projects/Spring2011/Project1/jdn-explanation.html.

[2] E. G. Richards, Calendars, in: S. E. Urban & P. K. Seidelmann, eds. *Explanatory Supplement to the Astronomical Almanac*, 3rd ed. (2013), (pp 585–624), University Science Books, Mill Valley, Calif., ISBN 978–1–89138–985–6.

Solution 265.7 – Population control

> In an overpopulated country the law restricts a woman to one child if it is a boy and at most two if her first child is a girl. How is the population affected?

Richard Gould

First we note that, irrespective of the initial gender distribution in the population, the distribution in each successive generation will depend only on the number of women in the previous generation. The male population needs only to be of a size sufficient to provide enough fathers (traditional or donor) for their offspring.

Initially we develop a simple model where it is assumed that all the women in the population are fertile and have as many children as the stated rules allow. If there are N women initially and the probability of a male birth is p then the next generation will comprise $pN + (1-p)pN$ men and $(1-p)N + (1-p)^2N$ women. Thus, if the numbers of men and women in the nth generation are m_n and w_n respectively

$$\begin{aligned} m_n &= p(2-p)w_{n-1}, \\ w_n &= (1-p)(2-p)w_{n-1}, \quad n = 1, 2, \ldots. \end{aligned}$$

Note that, even if the overall population declines, the male population may increase in the first generation (perhaps if it was previously depleted by war or some genetic factor). This will be the case if

$$p(2-p)w_0 \;>\; m_0.$$

The generation on generation ratio of the male population can be found as follows:

$$\begin{aligned} \frac{m_n}{m_{n-1}} &= \frac{p(2-p)w_{n-1}}{p(2-p)w_{n-2}} \\ &= \frac{p(2-p)(1-p)(2-p)w_{n-2}}{p(2-p)w_{n-2}} \\ &= (1-p)(2-p). \end{aligned}$$

So, after the first generation, the male population grows or declines at the same rate as the female population. *Should this have been expected?*

For the overall population to increase we therefore require

$$(1-p)(2-p) \;>\; 1.$$

Completing the square on the LHS gives

$$\begin{aligned}\left(p^2 - 3p + \frac{9}{4}\right) + 2 - \frac{9}{4} &> 1,\\ \left(p - \frac{3}{2}\right)^2 &> \frac{5}{4};\end{aligned}$$

so either

$$p > \frac{3}{2} + \frac{\sqrt{5}}{2},$$

or

$$p < \frac{3}{2} - \frac{\sqrt{5}}{2}. \tag{1}$$

The first solution gives $p > 1$, which is not possible. The second gives $p < 0.382$ which, though feasible mathematically, is not consistent with historical or current birth data which give p values of around $0.512 - 0.517$. In general, then, we would expect the population to decline and this tendency would be increased if fewer than the maximum number of births occurred in each generation.

Having got this far, let's assume that some genetic anomaly has drastically reduced the male birth rate so that an increasing population becomes possible. We could improve on the first model by assuming that only a proportion k_1 of women have one child and that, of those, a proportion k_2 go on to bear a second child. With an initial female population N, the next generation will now comprise $pk_1N + p(1-p)k_1k_2N$ men and $(1-p)k_1N + (1-p)^2k_1k_2N$ women. Hence, we now have

$$\begin{aligned}m_n &= \{1 + (1-p)k_2\}pk_1w_{n-1},\\ w_n &= \{1 + (1-p)k_2\}(1-p)k_1w_{n-1}, \quad n = 1, 2, \ldots.\end{aligned}$$

The condition for population growth becomes

$$1 - p + k_2(1-p)^2 > \frac{1}{k_1}.$$

Completing the square again (after some manipulation)

$$\left(p - \frac{1 + 2k_2}{2}\right)^2 > \frac{k_1 + 4k_2}{4k_1k_2}.$$

As before, growth is possible if

$$0 < p < \frac{1 + 2k_2}{2} - \frac{1}{2}\sqrt{\frac{k_1 + 4k_2}{k_1k_2}}. \tag{2}$$

Setting $k_1 = k_2 = 1$ in equation (2) recovers equation (1), as we would expect. If $k_2 = 1, k_1 \neq 1$ we have positive growth if

$$\frac{3}{2} > \frac{1}{2}\sqrt{\frac{k_1+4}{k_1}}$$

from which $k_1 > 1/2$.

For $k_1, k_2 \neq 1$ if we take, for example, $k_1 = 3/4$, equation (2) shows that population growth is possible provided

$$12k_2^3 + 12k_2^2 - 13k_2 - 3 > 0$$

which, for $0 < k_2 < 1$ has solution $k_2 > 0.785$.

Problem 268.4 – Triangles in a grid

Nine dots are arranged in a 3 × 3 grid.

(a) How many triangles can you make with the dots as vertices?

(b) How many distinct triangles can you make? Two triangles are distinct if they are not congruent to each other.

Of course that was just a warm-up for the general problem. There are n^2 dots are arranged in an $n \times n$ grid.

(i) How many triangles can you make with the dots as vertices?

(ii) How many distinct triangles can you make?

(iii) How many distinct integer triangles can you make? A triangle is integer if its three sides are integers.

(iv) How many distinct integer, non-Pythagorean, non-isosceles triangles can you make that have one vertex at coordinates $(0, 0)$, the bottom-left corner of the grid, and the other two on the grid at coordinates (A_x, A_y) and (B_x, B_y) with positive A_x, A_y, B_x, B_y?

Apologies for the long-winded nature of (iv). However, this is the most interesting part—in opinion of me (TF). Also it might be worth recalling a corollary of Pick's theorem. The area of a triangle drawn with its vertices on an integer grid must be half an integer.

Shorties

Eddie Kent

Ralph Hancock sent me an email. It said: This is said to be the shortest known paper published in a serious mathematics journal. It was in the *Bulletin of the American Mathematical Society* 72/6, 1966; see http://goo.gl/okjjVe. I looked so you don't need to. The entire paper, including two lines of title, is 12 lines long. J. L. Lander & T. R. Parkin give a counterexample to a conjecture of Euler, showing that even the greatest sometimes get it wrong. But this reminded me of a famous incident.

F. N. Cole, at a meeting of the AMS on 31 October 1903, walked to the blackboard in silence and calculated M_{67}, and then worked through $193,707,721 \times 761,838,257,287$ to show that they both come to $147,573,952,589,676,412,927$. He then sat down to a standing ovation. The whole business took him about an hour and he didn't say a word. He said later that finding the factors had taken him 'three years of Sundays.'

Of course the real mathematics happened in 1876 when Édouard Lucas demonstrated that M_{67}, or $2^{67}-1$, the 67th Mersenne number, is composite. Cole published a paper in the *Bulletin of the AMS* Vol. 10 in 1903 explaining about how he did it, how Lucas had done his bit, and how 'Some curious misinformation in regard to these numbers was published by Mersenne in the preface of his *Cogitata physico-mathematica* (1644).'

Cole, in *On the factoring of large numbers*, explained 'In resolving a large number N into its prime factors, a table of quadratic remainders of N can be made to render efficient service in several different ways.' So I guess he did use some real mathematics too.

Problem 268.5 – Factorization

Tony Forbes

The above reminds me of another silly story involving positive integers and the factorization thereof. You might recall that Fortuné Landry is credited with the discovery in 1880 that $2^{64}+1$ is composite (See Wilfrid Keller's *Fermat Factoring Status* at http://homes.cerias.purdue.edu/~ssw/fdub.html).

This was actually part of a project to factorize $2^n \pm 1$ for $n \leq 64$, an activity which kept Landry busy for many years. He describes one particularly stubborn case, 'None of the numerous factorizations of the numbers $2^n \pm 1$ gave as much trouble and labour as that of $2^{58}+1$.' However, Landry was unaware that this number actually has an algebraic factorization based on a general method found in 1871 by Léon–François–Antoine Aurifeuille. With this discovery the task is so simple we can set it as a problem.

Factorize $2^{4n+2}+1$. Hence or otherwise completely factorize $2^{58}+1$.

Scarne

Ralph Hancock

Mike Lewis's mention of the book *Scarne on Dice* (Solution 260.3 – Three dice) prompted me to look it up. It was written by John Scarne (original name Orlando Carmelo Scarnecchia, 1903–1985), a successful stage magician specializing in card tricks. The book was a simple guide to gambling games written in non-mathematical language for distribution to American troops coming over to Europe during the war, on the admirable principle that the wily Europeans were going to rob these naive boys blind and they should understand what they were in for.

Scarne also gave lectures at army and navy bases.

His hands may be seen in a scene the 1973 film *The Sting*, substituted for Paul Newman's where the character has to manipulate cards.

Scarne invented several games including a very simple board game called Teeko, which was successful for a few years and then faded from sight.

It is played on a plain board of 5 × 5 squares. Each player has four identical pieces, such as black and white draughtsmen. You win by getting your pieces in a straight line, horizontal, vertical or diagonal, or in a square on four adjacent board squares. Players have alternate turns. In the first eight turns they place their pieces on the board wherever they like. Then each player can move any one of his pieces one square in any direction, until one player wins or the world ends—since no pieces can be captured, it would be possible to play for ever.

Teeko has been analysed by the computer scientist Guy Steele, a developer of Java, who found that it was impossible for either side to force a win as long as the opponent played accurately—the sign of a well designed game.

In 1955 Scarne played ten simultaneous games against a bunch of celebrities including Judy Holliday, offering $1000 to any of them who could beat him. He won all the games. In the picture http://goo.gl/45Cp1Q Judy Holliday looks appalled, but perhaps she is just yawning because she is bored. She is said to have had an IQ of 170, which perhaps she needed to play dumb blondes.

Q. Can you make an anagram of Banach Tarski?

A. Banach Tarski Banach Tarski.

Sent by Jeremy Humphries.

Problem 268.6 – Squares with even digits

(i) Squares which have all of their digits even are very common: 0, 4, 64, 400, 484, 4624, 6084, 6400, 8464, 26244, 28224, 40000, ... Show how to construct infinitely many.

(ii) If we restrict ourselves to non-zero even digits, there still appear to be plenty: 4, 64, 484, 4624, 8464, 26244, 28224, 68644, 228484, 446224, 824464, 868624, 2862864, 8282884, 8868484, 22448644, 26646244, 44462224, 82228624, 82664464, ... Are there infinitely many?

(iii) On the other hand, squares with all digits odd seem to be very rare. Either show that 1 and 9 are the only examples, or find another one.

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.

Primes, sums of two squares, and palindromic continued fractions
Roger Thompson 1

Mathematics in the kitchen – X
Tony Forbes 3

Solution 264.3 – Determinant
Edward Stansfield 4

Problem 268.1 – Two triangles 6

Solution 232.2 – Angles
Dave Wild 7

Problem 268.2 – Induction 7

Solution 188.1 – Ones
Reinhardt Messerschmidt 8

Problem 268.3 – Sequences 13

Solution 245.10 – Every other day
Mike Lewis 14

Solution 265.7 – Population control
Richard Gould 16

Problem 268.4 – Triangles in a grid 18

Shorties
Eddie Kent 19

Problem 268.5 – Factorization
Tony Forbes 19

Scarne
Ralph Hancock 20

Problem 268.6 – Squares with even digits 21

M500 Mathematics Revision Weekend 2016 21

Problem 268.7 – Interest 22

04.00

Problem 268.7 – Interest

I deposit 50 pence in a bank account that offers interest at 2 per cent per annum. How much will I have after 200 years (i) if the interest is calculated annually, (ii) if the interest is calculated every six months?

Front cover Eleven triangles in a 49 × 49 grid (page 18).