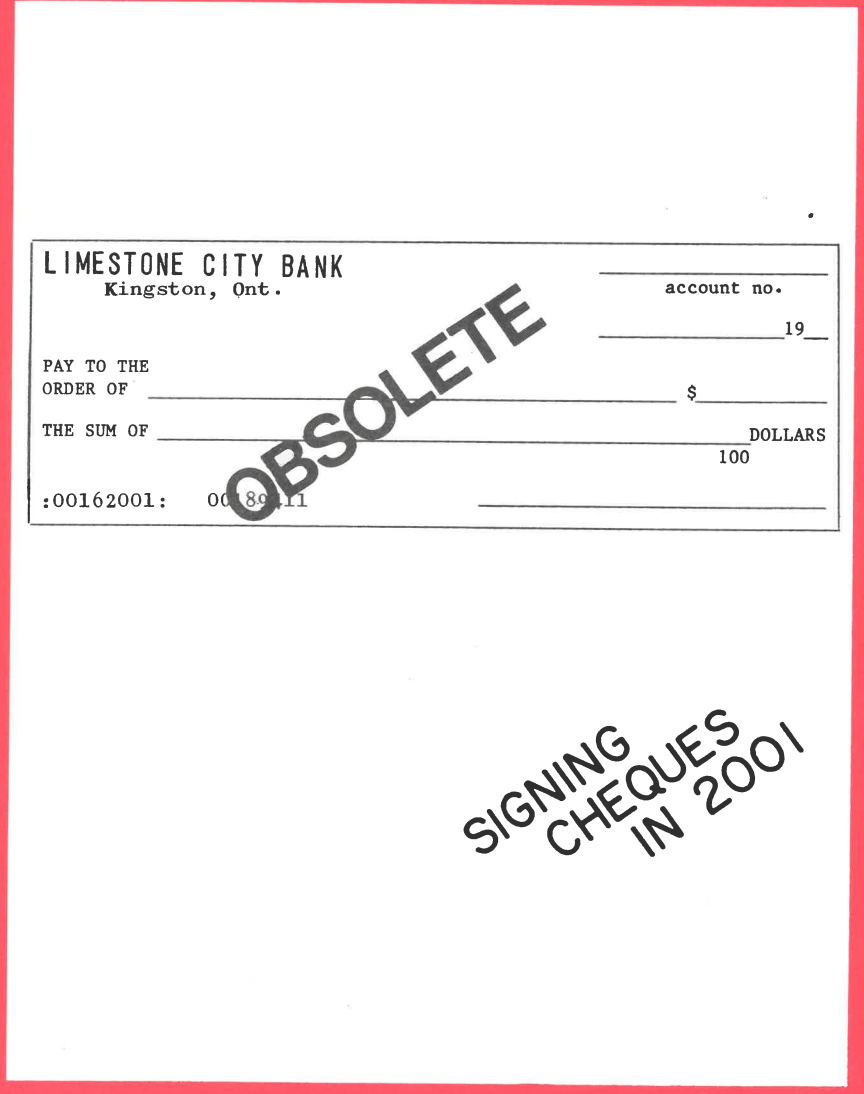
QUEEN'S MATHEMATICAL COMMUNICATOR

November
1981



An aperiodical issued at Kingston, Ontario by the
Department of Mathematics and Statistics, Queen's University

SIGNING CHEQUES IN 2001

by

Peter Taylor

We've all read articles about what day to day life will be like in 20 years time; predictions range from the absurd [books will be obsolete] to the sublime [men will be able to get pregnant]. It is a great game in which the imagination can run wild, tempered only by a thin veneer of scientific credibility. Which is why writing an article like this is rather fun.

I propose to examine one small aspect of the matter about which I know a modest amount: What will a cheque look like in 20 years?

Books will still be around in 20 years because marvellous things can be said in a book that can really be said in no other way. But there are other things besides books that are written on paper and many of these can and will be said in a much better way. Small pieces of paper, in particular, are a nuisance. They travel slowly, they get lost easily and they are often hard to read. Certainly in the business world, and probably at home as well, they will be replaced by electronic signals that are faster, clearer and easier to store.

A group of six Queen's professors from three departments is engaged in research into computer security systems. Professors S.E. Tavares and P.J. McLane from Electrical Engineering, S.G. Akl and G.H. MacEwen from Computer Science and L.L. Campbell and P.D. Taylor from Mathematics and Statistics, have been funded by a Strategic Grant from NSERC. One of the more fascinating "hot" topics in this field is public key cryptography, and the study of digital signatures arises from this. What I have called a signature function in this article, goes by the general name of trapdoor one-way function. An elementary account of these topics can be found in an article of Hellman in Scientific American, Aug. 1979, 146-57

Let's be specific. The year is 2001 AD. I return home from work one evening [Being a teacher I am one of those people who still travel to and from my place of work every day] press a button on the terminal in my den, and read the day's mail on my 32" TV screen. Along with a nice note from my grandaughter wishing me a happy 60th birthday [10 days late; some things never change, but at least she can't say it got lost in the mail], I perceive that I owe the PUC $827.62 for the months of September and October. [Inflation didn't change either.] I deal with the matter immediately so I don't forget about it [neither did interest rates] and, flicking a switch on the terminal I quickly send a message to my bank asking them to transfer the required amount to the PUC account (whose number appeared on my "bill"). Essentially I have just written a cheque to the PUC. Now here's the question: how did I sign it?

Obviously it is important that I be the only one who can transfer money out of my account. The bank can only respond to such a request if they are certain it came from me. I must add to the request my "signature". But what kind of signature can be sent along a wire which essentially just carries zeros and ones? What is an electronic signature to look like?

Here's one answer which doesn't really work. Suppose I have a device (perhaps a magnetic card) which produces on my terminal the signal required to form a photograph of my signature on a TV monitor. I add this signal to my message and the bank teller can flash it on a screen and compare it with my speciman signature, just as is done today. This is really a 20th century solution adapted to a 21st century problem. The reason it doesn't work, is that everything should be done automatically without the intervention of a teller. Thousands of messages may have been received by the bank during the

night. To process them all first thing in the morning through a phlanx of sleepy tellers would be a colossal waste of time. [So what do the tellers do? You guessed it. They don't work there any more. In fact the bank isn't even there any more. My message goes to a computer in Toronto!] Indeed a computer will process my request. So a computer will read my signature. And a computer that can recognize such a signature can be made to reproduce it. So it won't be particularly hard for someone else to discover how to sign my cheques. That is why it doesn't work.

What in fact do we require of an electronic signature? A computer must be able to identify it and associate it to me, but I must be the only one who can produce it. That turns out to be a tall order. Think about it for a moment. What can be read and readily identified, but not reproduced (forged!)?

An incredibly nice answer to this problem has been provided over the past 5 years by mathematicians at Stanford and MIT. It hinges on one simple concept: that of a signature function. A signature function is an invertible function f with the following properties.

1) f is easy to compute: given any x it is easy to find $y = f(x)$.
2) f is hard to invert: given some y in the range of f it is hard to find the x for which $f(x) = y$. [This x is denoted $f^{-1}(y)$.]
3) There is some secret information which makes f^{-1} easy to compute.

In 1) and 3), "easy" means a few seconds of computer time. In 2) "hard" means a lot of computer time is required (like a million years!). Let me emphasize that knowledge of the function f must give no real help in calculating f^{-1} or in finding the secret information.

Don't puzzle too hard over this strange definition; it's not at all clear such functions can even exist. But suppose they do. Let's see how the system would work. Every customer of the bank would construct his own signature function and keep the secret information needed to invert it to himself. He gives the bank the instructions for computing f. [This is the analogue of the speciman signature card]. Every time he communicates with the bank, it sends him a number y, possibly generated randomly on the spot. Using his secret information he calculates $x = f^{-1}(y)$ and appends it to his message, along with his account number. The bank finds the function f belonging to his account and calculates $f(x)$. When it sees that $f(x) = y$, the number sent out, it is certain that the message is authentic; only the owner of that account could generate the inverse image of y.

In practice the collection of signature functions used by a bank would all be structurally similar, differing by the value of one or two parameters. Each customer would provide his parameter set k which the bank could plug in to a standard program for the calculation of his function f (now written f_k). It's a nice system: simple and reliable. If only we could find such functions.

Interestingly enough the definition of these functions, given above, was formulated by two Stanford mathematicians, Hellman and Diffie, before any examples were known. They appreciated the significance of the idea, but were not certain it could be realized. The first example was produced a year later by Rivest, Shamir and Adelman at MIT. It is called the RSA system, and to explain how it works, I will suppose it is the one used by my bank.

When I opened my account at the bank I picked two large prime numbers p and q, calculated the product $n = pq$ and gave that to the bank (my "speciman signature"). The function f is calculated as follows

$$f(x) = x^{101} \pmod{n} .$$

That is, raise x to the power 101, and reduce modulo n. The function can be easily calculated by any large computer who knows n.

It turns out that if 101 is not a factor of $p-1$ or $q-1$, (and we now take this as a further stipulation on p and q) then f is invertible and its inverse has the form

$$g(x) = x^{k} \pmod{n}$$

for some integer k. The value of k is found from the formula $101k \equiv 1 \pmod{m}$ where $m = (p-1)(q-1)$. To solve such an equation for k you need only remember the elementary result that if $\gcd(m,101) = 1$ then there exist integers h and k for which $1 = mh + 101k$. To prove that $g = f^{-1}$ you need some elementary number theory. It is a good exercise for an inquiring student.

Using these functions, let us follow once more the process of writing a cheque. I take the number y generated by the bank and with my secret number k, I calculate $g(y) = y^{k} \pmod{n}$. [My terminal contains a small computer which will do this without fuss.] I append $g(y)$ to my message. The bank accepts the message, and locates my file, in which my number n is recorded. It computes $g(y)^{101} \pmod{n}$, and, finding that this is equal to y, judges the message authentic.

How easy is it to forge my "signature"? Presumably anyone who knew enough about computers to steal from my account, would have no trouble discovering my value of n. [It might even be public knowledge to facilitate transfers to my account.] But forging my signature requires knowledge of k, and only I know k. Of course k can be deduced easily from p and q [I described the method above] and p and q are mathematically determined by n [they are the unique prime factors of n], but in practice how easy is it to factor numbers? It is not so hard for small numbers (like $n = 91$) but turns out to be a long process for large values of n. For example if n has 200 decimal digits, the best techniques available today require a million years of computer time!

Now 200 digit numbers are not easy to write down or remember, but they pose no problem for the computer in my den. The program to calculate the function g (including the numbers k and n will perhaps be stored on a small plastic card (like a credit card) which I keep in a safe place or in my wallet and which is inserted into a slot in my terminal. For extra security, in case the card is stolen, it may require a password to be typed in before it will divulge its program.

Incidently, signatures are not only used for business; we use them in personal letters. When the letter travels over the cable, will it be signed by such a system? For example how can I be sure my birthday greeting came from my granddaughter? I know for a fact she doesn't care a fig about birthdays. Did the message really come from her mother who was afraid I'd be offended if my granddaughter forgot. I wouldn't of course, but all the same I'd like to know if my granddaughter really sent that message.

In fact there's no reason why the system we've just described couldn't be used for personal communication. Everyone has his public n and his private k. I keep a list of my friends' n-values in the little black book I kept phone numbers in 20 years ago. [Actually I don't! These numbers are big and hard to write down; they are all stored in my computer.] In particular I have my granddaughter's n. Now how does she sign her letter? She first needs the number x which essentially must come from me. She could phone my computer and get it to generate a number at random, or she could use some agreed upon algorithm for obtaining it such as the time of transmission 358 34 42 16 14 11 2021 (from milliseconds to years) obtained from the time stamp in the computer. The only kinds of x which wouldn't be acceptable to me are those which a forger could have obtained by choosing first some y and then letting $x = y^{101} \pmod{n}$.

Let's suppose the time stamp is the universal method of producing x. This number appears at the top of her message, and underneath she (actually her computer) writes y which is $x^k \pmod{n}$. When I see her name at the bottom, I look up her n, then calculate $y^{101} \pmod{n}$. If I get the time stamp x, I have validated her "signature".

Of course if someone writes me whom I don't know, and therefore whose n I don't know, I can't validate the signature right away. But I can't under the present system either. Validation today requires a specimen signature and, when matters are disputed, possibly a handwriting expert. And even then things may not be certain. But the "signature function" system requires only knowledge of the appropriate n. This may even be publicly listed. And then we can be certain.

Of course it may not be like this at all! The field is still wide open for ideas. Got any?

EDITORIAL PAGE

The Communicator begins in this issue a new regular feature: an editorial page which includes letters to the editor. Here we hope for a lively discussion of issues and ideas of interest to the readership of the magazine: teachers, students and graduates of mathematics and statistics. In the editorial we will have a chance to express our views, and in the letters we will be able to listen to, and pass on, yours.

These letters might be rather interesting. Issues come up all the time which involve mathematics or statistics in education, in a research project or in the daily workings of society. Often they cry out for comment. Perhaps you have read an article recently which raised your blood pressure or started you along a novel train of thought. [Please give references!] Perhaps you've had a strange encounter with a teacher or student which raised a number of questions. Perhaps you've heard a priceless anecdote you'd like to relate. The open sharing of ideas and opinions can turn a widely scattered group of people into a community.

And the letters may be more than interesting; they may be important. Times are getting tough, especially in the university world. Budgets continue to be cut, even when no flexibility seems to remain. Entire programs are questioned; drastic measures are contemplated. It is possible that the next decade will force a change in the fundamental character of our universities. At times like these it is valuable to have good lines of communication between the university and its constituency. It is important for

us to tell you what we are trying to do, what we think we really do, and what we'd like to do if we had the resources. And it's important for you to react to this, and declare what seems to have value for you. What are your priorities? They may be quite different from ours or from those of the government you elected to represent you.

In particular what are your views concerning programs in mathematics and statistics? What should be the major objectives of such programs. What students should they be attracting? Are these the students they currently get? For example, the past few years have seen a substantial movement of many bright students into Faculties of Commerce. We sometimes feel that many of the more quantitatively oriented students might be better to take a basic degree in mathematics or statistics, and then go on to an MBA. What do you think of that? How do you advise such students?

Let's hear from you. After all, communication is what the Communicator is all about!

All correspondence should be addressed to The Communicator, Department of Mathematics and Statistics, Queen's University, Kingston, Ont. K7L 3N6.

PDT

DEPARTMENTAL NEWS

Douglas Hoover has been appointed as assistant professor effective August 1, 1981. His field is Logic and he obtained his Ph.D. from University of Wisconsin under the supervision of H.J. Keisler.

Norm Pullman is on Sabbatical leave this year at Simon Fraser University, whence he will travel to Australia for the second half of the year.

Ian Hughes has a two year visiting appointment at the University of Nairobi, partly supported by a CIDA program administered by WUSC. While in Kenya, Ian will teach undergraduate and graduate courses, supervise graduate students, and continue his research. At the moment he is doing mostly the latter as the university is temporarily closed, apparently for political reasons. Last month he sent urgent requests back to Canada for a linear algebra text book. Since then, 40 copies of this book have been donated, and are on their way to Nairobi.

Cedric Schubert has been appointed Chairman of Graduate Studies. He takes over from Tony Geramita for a 3 year term.

Tony Geramita spent three weeks in Europe this May lecturing on his work at Oberwohlfach, W. Germany; University of Paris, University of Lyon and University of Genoa.

John Ursell attended the Canadian Conference on Applied Statistics held at Montreal on April 29 to May 1, 1981, and presented a paper entitled "A Statistical Model to Explain the Length of the Year of the Ancient Egyptians." Later in May he also presented the paper to the meeting of the Statistical Society of Canada held at Halifax on May 24 to 26, 1981. While in Halifax he also attended the meetings of the Canadian Colloquium on the Computer Processing of Textual Data (May 22 to 23) and of the Canadian Sociology and Anthropology Association (May 28 to 31).

QUEEN'S PROGRAM FOR JOURNEYMAN STATISTICIANS

Statistics is useful in all areas of research, government, industry and business. A growing awareness of the value of effective application of statistics is creating a demand for competent applied statisticians. This demand is documented in the National Science Foundation publication "Science and Engineering Education for the 1980's and Beyond": "... in 1990 the supply of scientists and engineers at all degree levels will likely be more than adequate to meet demand in all fields except for the computer professions, statistics and some fields of engineering." The figures for mathematical sciences (in thousands) are:

	Graduates B.Sc., M.Sc.	Job Openings 1978-1990
Mathematics	129	3
Statistics	8	19
Computing	157	549

Quoting again, "These comparisons point to two fields with large deficits of people with bachelors and masters degrees: the computer professionals and statistics. Such gaps would be expected to attract large numbers of people with training in other fields, particularly mathematics, where degrees are expected to be many times larger than job openings."

M.Sc. Degree in Statistics

Queen's response to this projected need has been to develop a Masters program to train journeyman statisticians. Graduates of the program will be able to apply a sound understanding of statistical principles to real-world problems.

The program is designed to appeal to a variety of students, such as:

- a student with a degree in mathematics who wishes to learn and apply statistics,
- a recent graduate who wishes to change careers and move into an area offering more challenge and opportunity,
- a graduate in biology or engineering who wishes to continue work in this field or who wishes to take the degree in preparation for a Ph.D.

Students in the program will work with faculty actively engaged in research and able to teach the latest developments in modern statistics. The faculty and students at Queen's gain practical experience in a wide variety of disciplines through STATLAB, a campus-wide statistical consulting service which provides researchers with advice and assistance on statistical aspects of their work. Students will obtain a first-hand knowledge of statistical practice by participating in this service.

Queen's two IBM 4341's are equipped with the most recent statistical computing packages from Canada, the U.S.A. and Great Britain. Students at Queen's have free access to interactive and batch computing facilities from terminals throughout the campus.

Program Structure

The student takes the equivalent of eight one-term courses in topics such as experimental design, regression analysis, sample surveys, categorical data, time series, stochastic process, multivariate analysis, computing and data management.

In addition each student participates in an in-depth statistical consulting project by interacting with a client from fields such as Medicine, Engineering, Psychology and Biology. The student is expected to become involved in the activities of experimental design, analysis and interpretation of results, as well the communication of the results and their significance.

The length of time to complete the degree is normally twelve months, from September to August.

Background Needed: A Science Degree

Students may enter this program with either an honours degree (or equivalent) in the natural, social or mathematical sciences or a degree in Engineering. Background must include linear algebra, calculus of several variables, some statistics and some computing. A preparatory summer course in statistical inference is available for students who have not studied this material as undergraduates.

Enquiries should be addressed to the Statistics Chairman, Department of Mathematics and Statistics.

Special Lectures on Multiplicity Theory at Queen's

It's an old and famous fact that a polynomial (whose coefficients are complex numbers) always has a complex root and that, if you count properly, a polynomial of degree n has n roots. Those n roots can be looked at as the points of intersection of the graph of $y = f(x)$ (if $f(x)$ is the polynomial) and the line $y = 0$. So, one says that a line and a curve of degree n, in the plane, meet in n points (properly counted). This theorem has fascinated mathematicians for a long time and attempts to generalize it have been going on for centuries. The most famous is Bezout's Theorem which says that a curve of degree n and a curve of degree m (both in the plane) meet in $m.n$ points (if we count the intersections properly and don't forget to count intersections at infinity!

The way to "count properly" is, of course, the whole point and one wants a method to do this not only for curves, but for the intersections of higher dimensional objects (like surfaces). There are numerous open questions and problems and also competing definitions for this counting principle and the whole area is a lively one for current research.

Tony Geramita of our Department has had an interest in these problems and to deepen his understanding and that of his students has invited one of the world's experts on these matters - Professor W. Vogel - Martin Luther University (Halle, E. Germany) to spend

three months at Queen's (October-December) lecturing on his research in this area. Coupled with Vogel's visit, six other mathematicians have been invited to each spend one week here lecturing on their work related to this problem. They are E.D. Davis (SUNY - Albany), D. Buchsbaum and D. Eisenbud (Brandeis), C. Hunecke (U. of Illinois), C. Weibel (Rutgers) and H. Bresinsky (Maine).

MASTER'S DEGREES AWARDED RECENTLY BY THE DEPARTMENT

Name	Supervisor	Title
POPLOVE, Alan L.	L.L. Campbell	Retransmission Strategies for Error Control in Data Communication Networks
DEMIRHAN, Fatih	M.T. Wasan	Concentration Functions
BOURDEAU, Marie	L.B. Jonker	The Classification of Singularities of Singularities of Smooth Vector Fields
ANDERSON, P. Murray	T.W.F. Stroud	Heritability of Intelligence and the Cyril Burt Affair
HOUSTON, David	R. Hirschorn	A Sufficient Condition for Invertibility of Nonlinear Control Systems
FARR, Barbara D.	B.J. Kirby & R. Davidson	A Control Theory Model of the Firm
MILLETTE, René	J.H. Davis	A Zeolite Based House Heating Model

Ph.D.'s AWARDED RECENTLY BY THE DEPARTMENT

NASHIER, Budh S.	A.V. Geramita	Efficient Generation of Ideals in Polynomial Rings

NEWS FROM GRADUATES

Send us news of your activities; let us know what you are doing!

1980

ROSS ETHIER, who is completing his M.Sc. at the University of Waterloo in applied mathematics, intends to do research on problems involving fluid flow in biological systems; he hopes to study for his Ph.D. at MIT next year.

TIM VENUS, is working for Spar Aerospace in Toronto where he is using numerical methods for solving the heat equation in connection with heat transfer in re-entry of space vehicles.

Papers Published by Math and Engineering Students

A number of our 4th year Mathematics and Engineering students have published the results of their final year project. Last year a paper appeared by S. Crozier, M. Wilson, K. Moreland, J. Camelon and P. McLane, entitled Microprocessor-based implementation and testing of a simple Viterbi detector, in Canadian Electrical Engineering J., Vol 6, 1-8 (July '81).

From the class of 1980, B. Ross and G. Woodruff travelled to Houston, Texas to present the paper, Microprocessor realization of an adaptive Viterbi detector, at the 1980, IEEE National Telecommunications Conference Nov. 30 - Dec. 4, 1980. The paper was co-authored by L. Wilner and P.J. McLane.

PROBLEMS

The problems section assumes a new format this issue in the hope of encouraging greater reader participation not only in solving but in suggesting new problems. Please send solutions to old problems and suggestions for new ones (with or without solutions) to the Communicator, Dept. of Mathematics and Statistics, Queen's University, Kingston, Ont. K7L 3N6. This issue we have problems submitted by two members of the Department.

Problem 5. $\frac{16}{64} = \frac{1}{4}$

The correct answer is obtained by cancelling the sixes. How many quotients of two digit numbers are there for which a common digit can be cancelled?

Ole Nielsen

Problem 6.

Find integers m and n so that $3.14159 < \sqrt{m} - \sqrt{n} < \pi$.

Norman Rice

SOLUTIONS TO PAST PROBLEMS

Problem 4.

Summing The Harmonic Series

This problem will teach you something about one of the standard mathematical constants, not quite so famous as π and e, but worth knowing about all the same. (This is your hint!)

Every series nut knows that the harmonic series $\sum_{n=1}^{\infty} 1/n$ diverges. That is, given any $M > 0$ we can always find a sufficiently large N such that

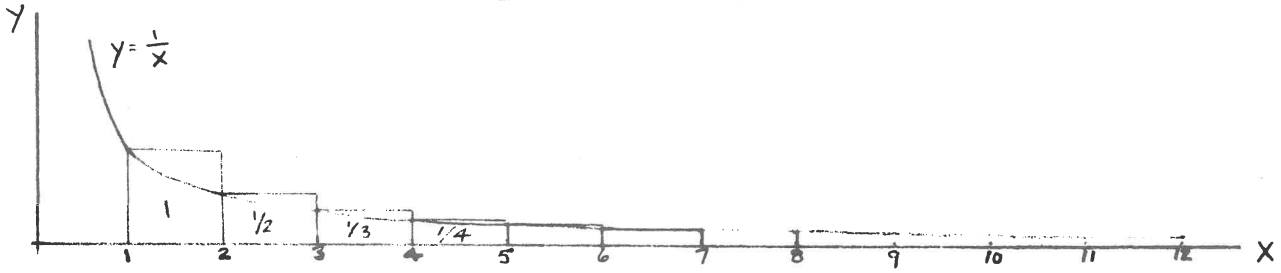
$$1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \cdots + \frac{1}{N} \geq M \quad .$$

Take $M = 10$ and find the smallest N for which this inequality holds. No computers or programmable hand calculators please. (Though you can use them to check.) I want an easily verifiable analytic solution available 50 years ago.

Solution.

Let $S_n = 1 + 1/2 + 1/3 + \ldots + 1/n$. It is clear from the graph below that

$$S_n > \int_1^{n+1} \frac{dx}{x} = \ell n(n+1)$$



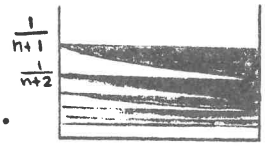
The difference $Sn - \ell n(n+1)$ is the sum of the n triangular regions between 1 and $n+1$. The sum of the areas of all these triangular regions is Euler's constant $\gamma = 0.577215665...$ Hence

$$\lim_{n\to\infty} \; Sn - \ell n(n+1) = \gamma$$

It is convenient to let ε_n be the sum of the infinitely many triangular regions from $n + 1$ onwards. Hence

$$Sn = \ell n(n+1) + \gamma - \varepsilon_n \; . \qquad (1)$$

By the "stacking principle" the triangles making up n all fit into a box of width 1 and height $1/(n+1)$.



Since the bottoms of the triangles are concave up, the triangles occupy more than half of the box. Thus

$$\frac{1}{2(n+1)} < \varepsilon_n < \frac{1}{n+1} \; .$$

With these estimates, and equation (1) it is clear from the following table that the answer is $N = 12367$.

n	$\frac{1}{2(n+1)}$	$\frac{1}{(n+1)}$	$\ell n(n+1) + \gamma$
12366	.0000404		10.0000026
12367		.0000809	10.0000834

Correct solutions were received from Joseph Hagge and Rolf Clack. The above solution is a slight simplification of Clack's.

PDT