LIMESTONE CITY BANK
Kingston, Ont.

account no.

19__

PAY TO THE
ORDER OF $

THE SUM OF DOLLARS
100

:00162001: 0(

SIGNING
CHEQUES
IN 2001

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

SIGNING CHE UES 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 arena in which the imagination can run wild, tempered

20 years?

only by a thin veneer of scientific credibility. Which is why

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 granddaughter 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] [illegible]

[illegible]

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. [illegible]

So a computer will read my signature. And a computer that can recognize such a signature can be made to [illegible]

[redacted]

at all clear such functions can ever exist. But suppose they do

[redacted]

When I opened my account at the bank I picked two large

[redacted]

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

[redacted]

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

[redacted]

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 [illegible]

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 [illegible]

In fact there's no reason why the system we've just describe

[illegible]

the little black book I kept phone numbers in 20 years ago. [Actually

[illegible]

EDITORIAL PAGE

The Communicator begins in this issue a new regular feature: an editorial page which includes letters to the editor. [illegible] 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

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

PDT

DEPARTMENTAL NEWS

Dou las 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 Hu hes has a two year visiting appointment at the University of Nairobi, partly supported by a CIDA program administered by WUSC.

UEEN'S PROGRAM FOR JOURNEYMAN STATISTICIANS

Statistics is useful in all areas of research, government,

[illegible]

industry and business. A growing awareness of the value of

[illegible]

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

[illegible]

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

Special Lectures on Multiplicity

Theor at ueen's

It's an old and famous fact that a polynomial (whose coefficients are complex numbers) always has a complex root and that, <u>if</u> you count properly, a polynomial of degree n [illegible]

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 [illegible] three months at Queen's (October-December) lecturing on his research

[redacted]

Name

[redacted]

have been invited to each spend one week here lecturing on their

work related to this problem. They are E.D. Davis (SUNY - Albany)

[redacted]

Su ervisor Title

[redacted]

Ph.D.'s AWARDED RECENTLY BY THE DEPARTMENT

[redacted]

NEWS FROM GRADUATES

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

1980

[redacted]

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

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 [illegible]

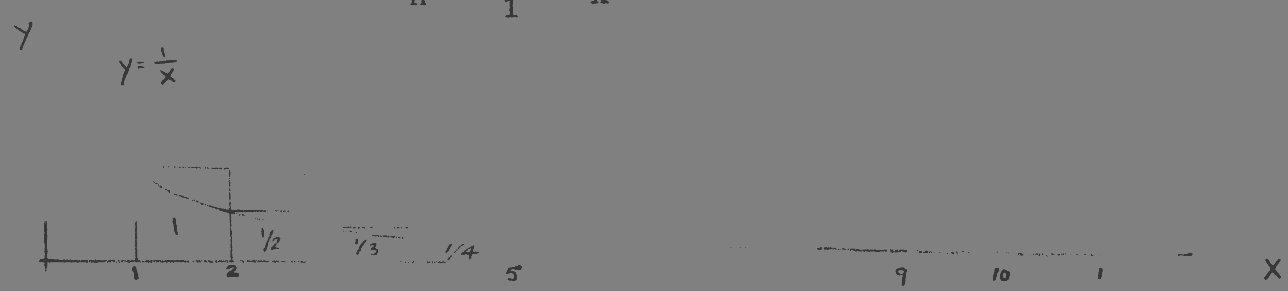
$$1 + \qquad + \cdots + \frac{1}{N} \geq M \; .$$

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

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



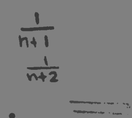
The difference $S_n - \ell n(n+1)$ is the sum of the n triangular regions [illegible]

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

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

$$Sn = \ell n(n+1) + \gamma - \varepsilon_n \,. \tag{1}$$

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 [illegible] half of the box. Thus [illegible]

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

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