COMPUTER RECREATIONS

How to pan for primes in numerical gravel

by A. K. Dewdney

No recreation embodies the lure of pure number better than the search for primes. Like nuggets of gold, they hide in the gray gravel of ordinary numbers. A prime is elemental: it cannot be divided evenly by any numbers other than 1 and itself. Primes are precious because they are rare. Common enough among the small numbers near the source of the great Continuum River, they thin out rapidly in the downstream banks.

One can pan for primes, even build a sluice box to mine these nuggets, but no one knows where they all are without looking. There is no formula for primes. There are patterns of sorts, a primitive kind of geology by which we can guess the deposits. Just as amateurs flocked to California and the Yukon to pan distant streams for the elusive yellow, so ordinary readers can set out for Number Country with little more than this primer tucked into a spare pocket.

Few mathematical ideas are as accessible to the average person as the concept of a prime number. It takes about a minute to explain primes to the man or woman in the street. Buy them a coffee and with a little encouragement they will write the primes on a paper napkin: 2, 3, 5, 7, 11, 13, 17 and so on. The number 1 is not normally considered to be prime.

Can one tell a prime just by looking at it? If there are many numbers in the pan, does a prime flash yellow to the eye? Some people think so. Numbers that end in 1 are often precious, such as 11, 31, 41 and 51. But one must beware of such fool's gold as 21 and 81, for example. Eventually the numbers that end in 1 fool us with increasing frequency, so that it is possible to wonder, as a few ancient Greeks did, whether the primes eventually thin out to nothing. There comes an end finally, or does there? Euclid has passed down to us the first proof that there is no end to the prime numbers.

The proof is so simple that one can imagine Euclid drawing forth the demonstration, Socratic fashion, from a slave. I prefer the conversation between the tyro and the old-timer on the banks of the Continuum River:

TYRO: Hey, mister! How far downstream do the primes go?

YUKE: Why, boy, all the way to the Sea of Infinity.

TYRO: I don't believe you. Here we are at the millions and I haven't seen color all day.

YUKE: You tenderfeet gotta be told everything. Look, suppose you came to the last prime. No more after that, right?

TYRO: Uh, right.

YUKE: Call it n. You take and form the product of all the primes there are right on up to n. O.K.? That's $2 \times 3 \times 5 \times \ldots \times n$. Now add 1 to the product and call the number you finally get p.

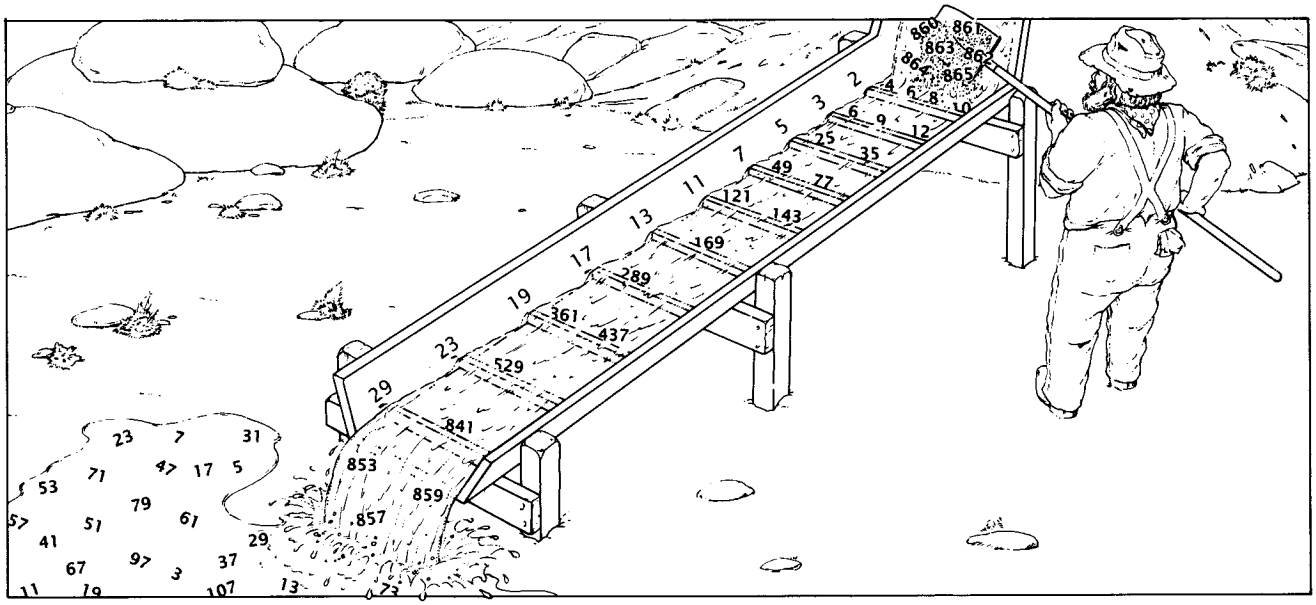
TYRO: Don't tell me that p is prime!

YUKE: Sure is. Prime as all get-out. Look. You can't divide it by 2 because there's 1 left over. You can't divide it by 3 because there's 1 left over. There's always 1 left over, right up to n. There's just no getting around it.

TYRO: Gosh, I guess that's what keeps you going.

YUKE: Yup. Well, don't just stand there yammering. Help me with this sluice box here.

Even if there is no largest prime, there is certainly a largest known prime. The distinction confuses some readers and even a few journalists. The fault lies with those back-page



A sluice box mines primes

259 (1)

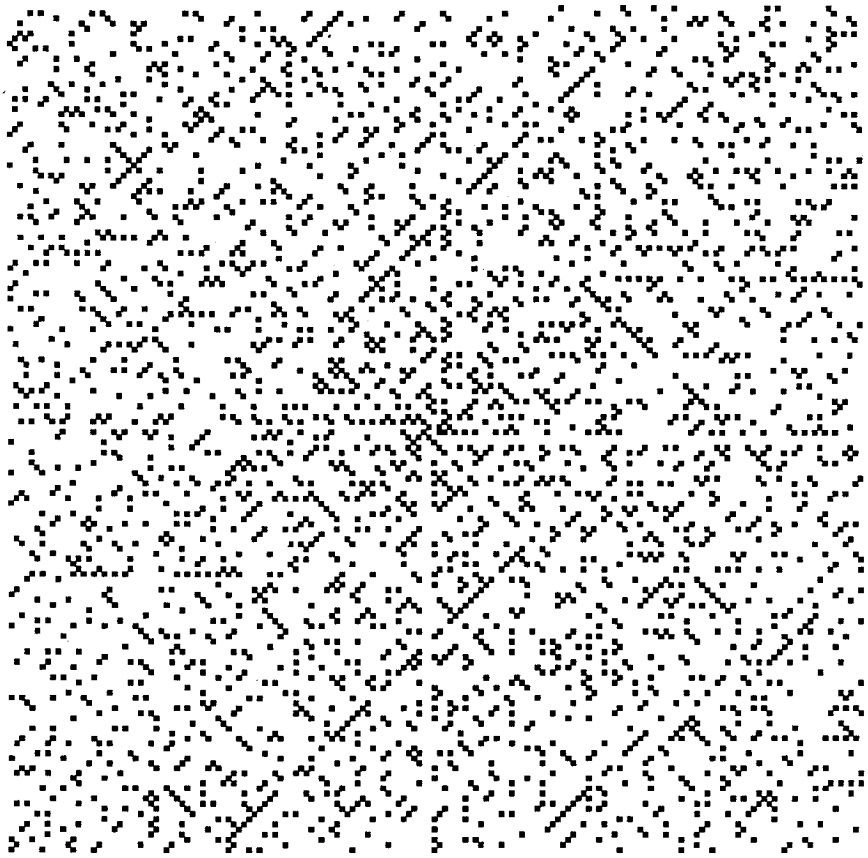
headlines: LARGEST PRIME FOUND. The confusion sometimes continues into the story. We learn that a new supercomputer has just shown that the 7,067-digit number $5 \times 2^{23,473} + 1$ is prime. It has no divisors except 1 and, of course, itself. The story might well omit (or the reader might miss) the fact that this is merely the largest known prime; soon a new, larger prime may well be found.

I hesitate to mention the largest prime number currently known. It may no longer be current by the time these words appear in print. As of this writing, the largest known prime is a 65,050-digit number found by David Slowinski of Cray Research, Inc., in 1985: $2^{216,091} - 1$. Prime numbers that have the form $2^m - 1$ are called Mersenne primes after the preeminent French mathematical amateur Marin Mersenne. All known primes greater than 1,000 are collected by another amateur, Samuel D. Yates of Delray Beach, Fla. The Yates collection is definitive. He has generously offered it to readers who send the cost of copying and postage ($3) to 157 Capri-D, Kings Point, Delray Beach, Fla. 33445.

How quickly do prime numbers thin out along the banks of the continuum? Within the first 10 numbers, four, or 40 percent, are prime. Within the first 100, the percentage drops to 25 percent. The percentage continues to drop more or less progressively. In general, the number of primes less than or equal to a number n is approximately $n/\log n$. (In this context the approximation is asymptotic. In other words, if the number of primes less than or equal to n is represented by the symbol $p(n)$, the ratio of $p(n)$ to $n/\log n$ approaches 1 as n gets larger. To quote old Yuke: "Downstream the primes thin out by the factor of a natural log.")

A few trials give some feeling for the rule. How many primes are there, according to the formula, between 1 and 100? Between 1 and 1,000? In the first case the formula yields an approximate value of 22. In the second case the formula predicts something like 145 primes.

Not surprisingly, the phenomenon of thinning-out produces more and longer stretches of numbers where there are no primes at all. To find a stretch of a million consecutive nonprimes, for example, one need only travel downstream, as Martin Gardner once did, to the number 1,000,001!. The exclamation mark does not indicate admiration but elaboration: it stands for $1 \times 2 \times 3 \times \ldots \times 1{,}000{,}001$. Teen-age terminology applies, namely humongous. But with ease we detect the prime-free stretch. If n runs from 2 to 1,000,001 in the simple formula $1{,}000{,}001! + n$, each of the resulting numbers happens to be composite. After all, in each case n divides both 1,000,001! as well as itself. Thus it divides the sum.



Stanislaw Ulam's spiral reveals a number of prime lodes

I stated above that there is no formula for prime numbers, no combination of algebraic operations on n that will produce, with a fixed number of crank turns, the nth prime. Many people have fallen prey to vain imaginings brought about by initial success. A well-known joke among mathematics undergraduates illustrates the point. It involves three ways of showing that all odd numbers are prime:

Mathematician: "Three is a prime, 5 is a prime, 7 is a prime... The result follows by induction."

Physicist: "Three is a prime, 5 is a prime, 7 is a prime, 9—experimental error, 11 is a prime..."

Engineer: "Three is a prime, 5 is a prime, 7 is a prime, 9 is a prime..."

Engineers may have the last laugh, since mathematicians depend increasingly on computers to probe for large primes.

Would it be enough to produce a formula that itself produces only primes? Pierre de Fermat, the famous 17th-century French mathematician, thought he had such a formula when he wrote $2^{2^n} + 1$. Plug in any value of n, he believed, and a prime number would emerge. Fermat's bubble was burst after his death when the Swiss mathematician Leonhard Euler found factors for the fifth Fermat "prime": $4{,}294{,}967{,}297 = 641 \times 6{,}700{,}417$.

As old Yuke might remark, "There's more than one way to skin a cat." Sometimes a visual pattern suggests a formula. Such a pattern was doodled one day by Stanislaw Ulam, the Polish-American mathematician. Attending a boring lecture, he began absentmindedly to draw a grid of horizontal and vertical lines. He numbered one of the resulting squares 1 and proceeded to number succeeding squares in a spiral around the first one:

```
5  4  3
6  1  2
7
```

When the spiral of numbers had wrapped around itself several times, Ulam began to circle the primes with no particular purpose in mind. He sat

up rather quickly, however, when he noticed an odd pattern developing. Straight lines had begun to appear out of nowhere! Ulam was immediately aware, of course, that such lines hinted at formulas for primes. The computer plot on the preceding page duplicates Ulam's pencil-and-paper experiment by replacing nonprimes with small white squares and primes with black ones.

The prominent diagonal lines correspond to prime lodes. How could one express this geology symbolically? Near the center of the diagram one such deposit proceeds down and to the left. It consists of the number sequence 7, 23, 47, 79,... The formula for this sequence happens to be quadratic: $4x^2 + 4x - 1$.

Those with some memory of high school algebra can develop the formula for virtually any line in the diagram. It may be that the formula is rich in primes well beyond the limits of the plot. Euler (rhymes with "spoiler"—and he ruined a number of careers by anticipating so many mathematical results) had stumbled on a similar formula in the 18th century: $x^2 + x + 41$. The formula does not show up on Ulam's spiral unless one uses a different central number. A spiral that starts at 41 reveals a vein that contains 40 consecutive prime numbers before it peters out!

Perhaps it is only city slickers who mine primes by formulaic methods. Those who work the banks of the Continuum River prefer pans or, better yet, sluice boxes. In these devices, also known as number sieves, numbers are shoveled in at one end; only primes emerge from the other end. Wood ribs catch the composite numbers by a divisibility test [*see illustration on page 120*]. Sluice boxes work perfectly well inside computers, naturally.

The simplest sluice box separates primes by dividing by 2, 3, 4 and so on. If one inputs the number n at one end, the sluice box tests whether n is divisible by 2, by 3, by 4 and continues until one of the tests succeeds or the count reaches n. In the first case the number is not prime. In the second case it is. An algorithm for this model of sluice box provides the simplest framework for home-computer programs. It is called SLUICE1:

```
input n
f ← 1
for k ← 2 to n − 1
    test ← rem(n/k)
    if test = 0 then f ← 0
if f = 1 then output "prime"
```

The program accepts a number n that is typed in (input) by the human user. Then the program sets the variable f (which acts as a flag) to 1; if f still has the value 1 when the program reaches its last line, the number n must be prime. A single *if* statement is executed repeatedly inside a loop. The index k runs from 2 to $n - 1$. For each such value SLUICE1 performs the division n/k, takes the remainder (rem) of the division n/k and stores the result under the name *test*. Usually *test* will be nonzero at the end of the loop. In other words, the number k does not divide n evenly. But if the division ever results in a zero remainder, SLUICE1 will immediately set the flag f to the value 0, holding it there until the loop has been completed. If the second *if* statement has a positive outcome, the program will print "prime." If f has been set to 0 somewhere along the line, only a grim silence will follow.

Although it is easy to understand, the foregoing program is too slow, particularly if it is adapted to produce a sequence of primes. The adaptation would merely involve replacing the first input statement by a loop statement, such as "for $n \leftarrow 3$ to 1,000." The final statement would be modified to print not "prime" but the value of n that made it all the way through the sluice box without being divided evenly. One by one all the prime numbers from 3 to 997 will come tumbling out, but very slowly!

Things move much more swiftly after SLUICE1 has been subjected to some tinkering. First, there is no point in testing whether the number n is prime by the division n/k if k happens to be larger than the square root of n; at least one of n's factors does not exceed its square root. The famous "fundamental theorem of arithmetic" also tells us that every whole number is the product of a unique set of prime numbers. It is not composite unless it can be divided evenly by a prime less than itself. Putting the two facts together results in a much shorter loop that uses only prime values for the index k and only those primes that are less than the square root of n.

The new algorithm, called SLUICE2, differs enough from its simpleminded counterpart to require a relisting:

```
r ← 1
p(1) ← 2
for n ← 3 to 1,000
    k ← 1
    f ← 1
while f = 1 and p(k) ≤ sqrt(n)
    test ← rem(n/p(k))
    if test = 0 then f ← 0
    k ← k + 1
if f = 1 then r ← r + 1
    p(r) ← n
```

Because SLUICE2 needs a list of primes in order to function properly, it stores these as it generates them in an array called p. The variable r keeps track of the index for the last entry of p. That way SLUICE2 always knows where to put the next prime it generates. The first line of the algorithm sets the index to 1. The next line specifies that the first member of the prime array will be 2. Then comes the loop command discussed above. It controls the testing of all numbers from 3 to 1,000. The variable k keeps track of which array element is currently being tested against n. Inside the main loop is a common kind of loop that uses the word "while"; as long as the flag is 1 and the current prime to be tested does not exceed the square root of n, the inner loop keeps chugging through successive values of k. Outside this loop f will equal either 1 or 0. In the first case a prime has been found. SLUICE2 adds the prime to its list. In the second case the main loop will simply go on to the next value of n.

Readers programming this kind of sluice box have two choices for structuring the program to print out all the primes found. SLUICE2 may print the array p all at once when the main

67	1	43
13	37	61
31	73	7

3	61	19	37
43	31	5	41
7	11	73	29
67	17	23	13

Henry Ernest Dudeney's prime square **(left)** ***and that of Allan W. Johnson, Jr.*** **(right)**

3	1	3	9	9	1
9	8	3	9	2	9
1	6	4	3	1	2
5	1	7	4	7	1
7	1	5	9	7	1
9	3	7	3	3	9

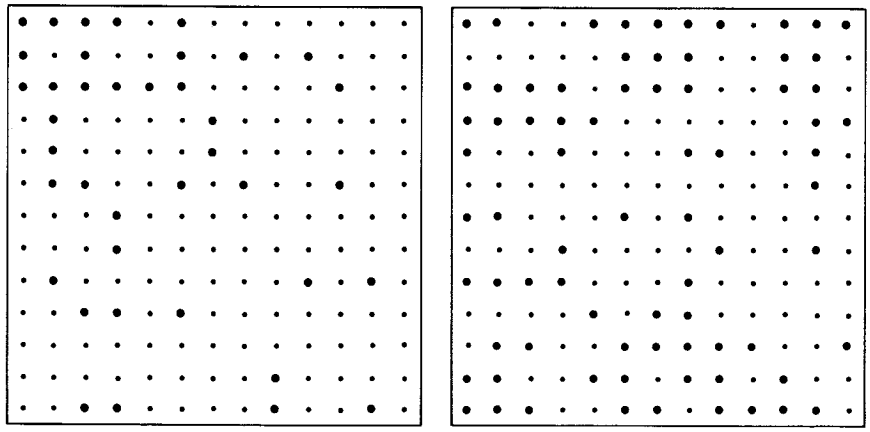
Gordon Lee's 6-by-6 prime grid

algorithm is complete. The experience is akin to opening a poke full of nuggets. It is more adventurous, some would say, to place a print command right after the line $p(r) \leftarrow n$. Then the user watches individual nuggets appear as soon as they are found.

I have been unadventurous in suggesting an iteration limit of a mere 1,000 numbers to test. There is no reason the limit should not be increased to 100,000 or even one million. Or is there? It all depends on how large an array one's system allows. The size of the array hinges on the number of primes one expects to generate. Here the prime-ratio formula comes in handy. The formula suggests that approximately 72,382 of the numbers less than 1,000,000 are prime. A computer that has only 64K of memory will not make the grade.

Prime numbers have figured in countless mathematical recreations. To continue the theme of primes in square arrays, two diversions come to mind. The first originates with Henry Ernest Dudeney, the distinguished English puzzle creator. Magic squares will be familiar to many readers as square arrays of numbers whose entries have the same sum along each row, each column and the two main diagonals. Are there magic squares consisting only of primes? The answer is yes. The 3-by-3 magic square shown on the opposite page sums to 111 (which happens to be prime) along all rows, columns and the diagonals. The 3-by-3 square is accompanied by a 4-by-4 companion. Squares of orders higher than 4 have been found. Readers who discover such squares for themselves are invited to send them in. The best example will appear in a future column; larger squares are superior to smaller ones and, for the same size, smaller sums are better than larger ones.

Another British purveyor of puzzles has issued a challenge to readers. Gordon Lee, who writes a column called "Winners and Losers" in a computer publication titled *Dragon User*, has constructed a 6-by-6 square of digits that conceals a great many prime numbers, 170 to be exact [*see illustration at right on opposite page*]. To find a prime number on Lee's grid scan along any row, column or diagonal in any direction. It may happen that a sequence of digits thus encountered is a prime number, one of the 170 counted by Lee. No more than 616 numbers (prime or otherwise) can be found in a 6-by-6 grid of digits. Repeated primes are only counted once. Lee counts 1 as a prime.



David H. Fax's blown matrix **(left)** ***and Patrick E. Kane's*** **(right)**

Can readers come up with a 6-by-6 square of digits that contains more than 170 primes? Those who write and run SLUICE1 or SLUICE2 will have a slight edge on the task. Lee suggests a strategy of seeding the square with the digits 1, 3, 7 and 9, since a prime must end with one of them. On the other hand, a square composed of only those digits would be relatively poor in primes. A judicious scattering of even numbers, including 0, might improve one's chances of meeting Lee's challenge. I shall publish the best solution sent to me (as long as it contains more than 170 primes).

In March this department dealt with a home-computer laboratory in which simulated gas molecules bounced within a closed vessel to mimic the effects of pressure. Molecules also diffused digitally from one side of a container to the other. Finally, make-believe atoms of the dangerously unstable substance I called gridium were gathered into a critical mass. A number of readers developed their own pressure vessels and diffusion chambers, but most found gridium too hard to resist. From all over North America and later from other parts of the world, reports of "computer explosions" crossed my desk.

By specifying the track of an escaping neutron with a linear equation, I inadvertently implied that two neutrons travel in opposite directions from the splitting atom. Most readers chose one of the two directions. In either case, it was not easy to get all the atoms in a plane n-by-n grid to blow up.

By plotting the results of numerous experiments, Robert Castle of Webster, Tex., found that 90 percent of the atoms usually fissioned in a 16-by-16 grid. By the time n reached a value of 32, 99 percent of the atoms were atomized. Robert M. Martin, a professor of philosophy at Dalhousie University in Nova Scotia, found a 90 percent criticality when n was equal to 19, and 99 percent of the gridium disappeared when n was equal to 39. Most other nuclear experimenters found values somewhere between these. Of those people sticking to the double-neutron burn in the original recipe, Richard W. Smith of Ann Arbor, Mich., was typical in finding lower critical masses. He reports a 98 percent burn when the grid measured 15 by 15.

Few readers developed a system as sophisticated as the program called SHAKEY. Developed by Robert B. Merkin of Northampton, Mass., SHAKEY not only can handle very large grids but also incorporates a great many time-saving techniques to speed up the essential boom. SHAKEY's home reactor allows different grid spacings to be tried and emits clicks at every decay like a Geiger counter. Merkin says he will be glad to share SHAKEY with readers who write to him at 55 Milton Street, Northampton, Mass. 01060.

Dramatic samples of blown matrixes were sent by David H. Fax of Pittsburgh, Pa., and Patrick E. Kane of Champaign, Ill. Their productions are shown above.

FURTHER READING

THE QUEEN OF MATHEMATICS. Eric Temple Bell in *The World of Mathematics*, edited by James R. Newman. Simon and Schuster, Inc., 1956.

AMUSEMENTS IN MATHEMATICS. Henry Ernest Dudeney. Dover Publications, Inc., 1970.

THE SEARCH FOR PRIME NUMBERS. Carl Pomerance in *Scientific American*, Vol. 247, No. 6, pages 135-147; December, 1982.

ONE MILLION PRIMES THROUGH THE SIEVE. T. A. Peng in *Byte*, Vol. 10, No. 11, pages 243-244; Fall, 1985.