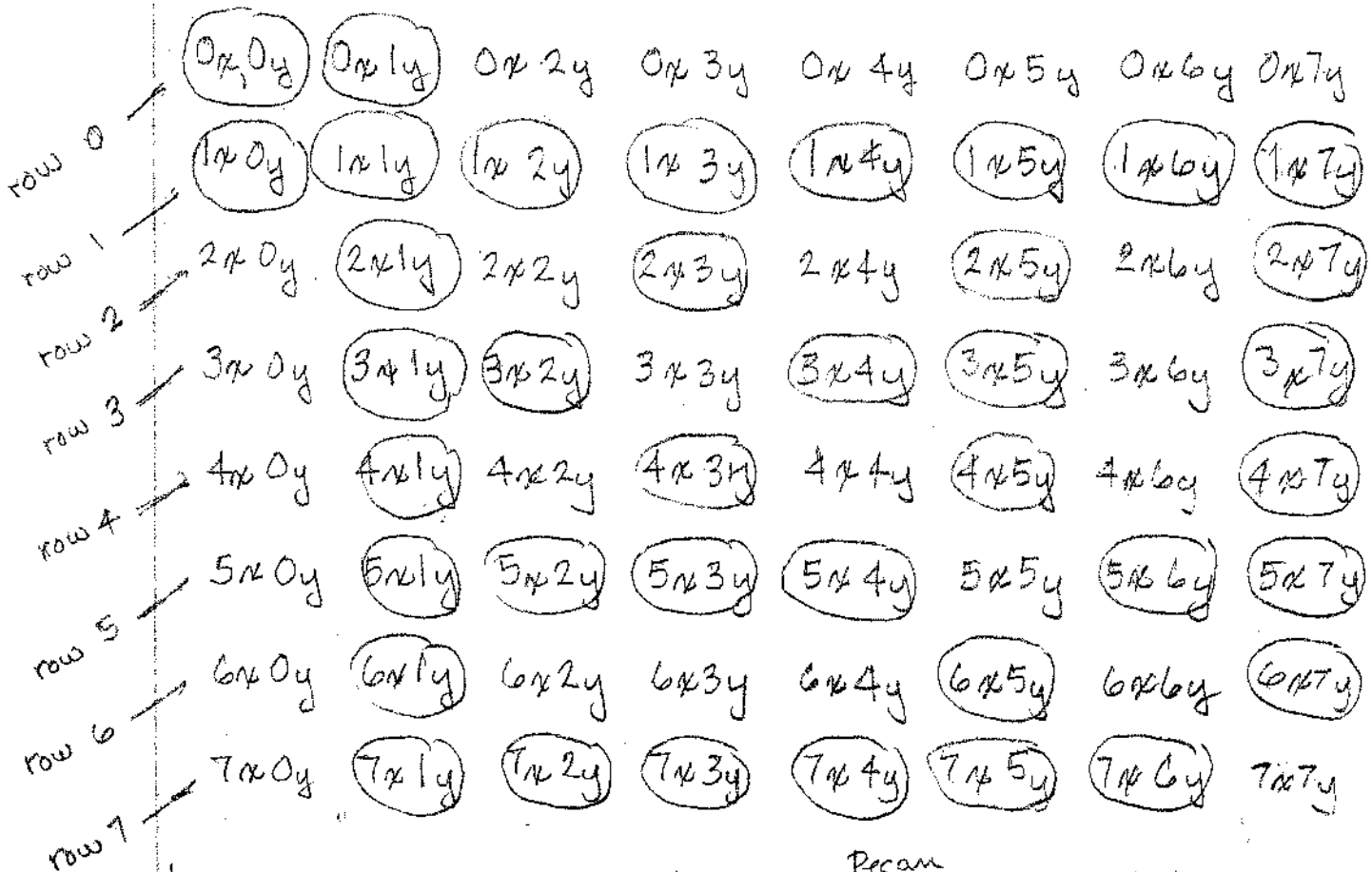


# Pecan-Tree Patterns, In a Nut-Shell

①

©2000 by Ervin M. Wilson, (work in progress)  
all proprietary rights reserved

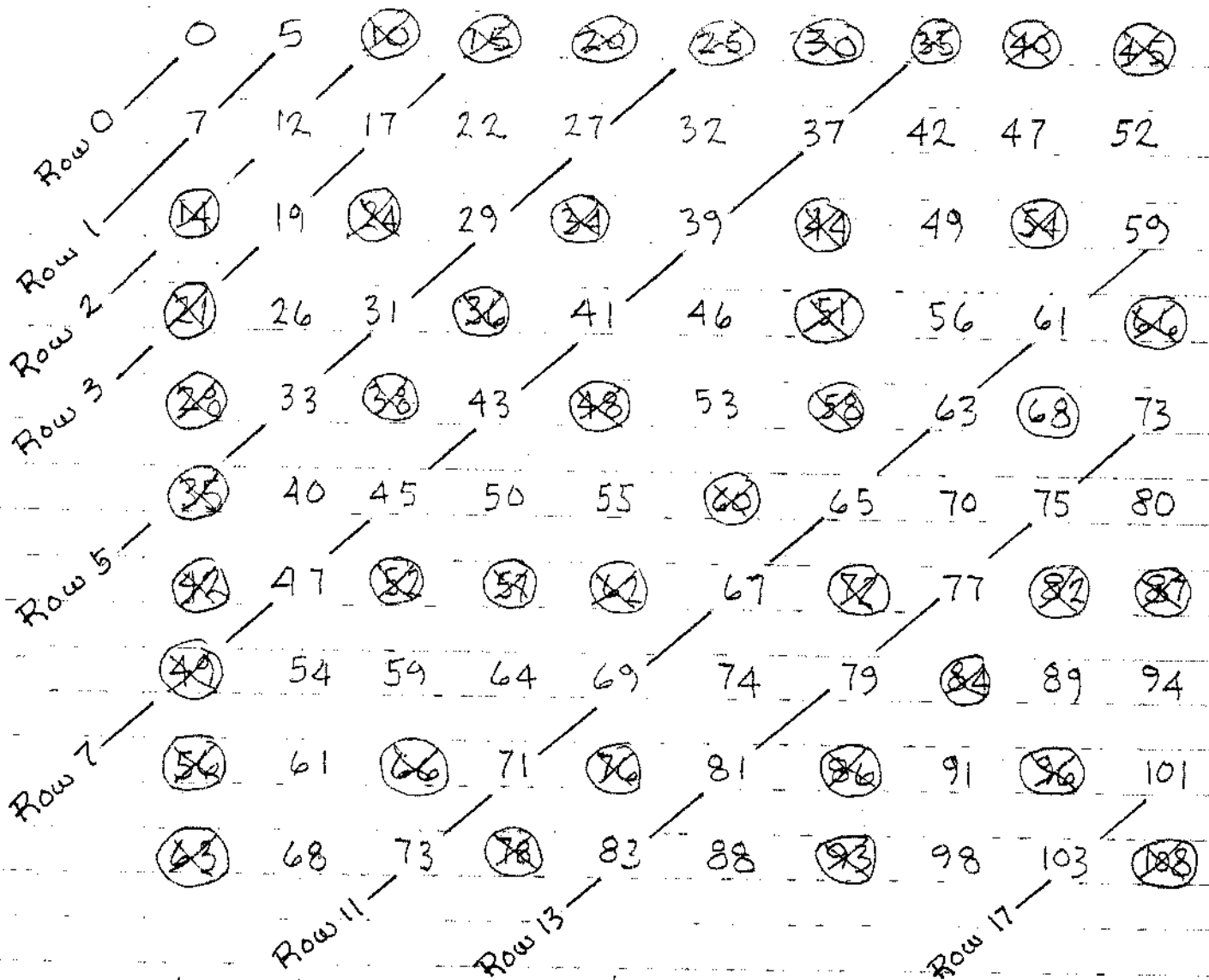
Fig. 1 Biaxial Co-prime Pattern



If we are in an orchard of  $64^{\text{Pecan}}$  trees planted  $8 \times 8$  as shown and we stand at Tree " $0 \times 0_y$ " and sight through the orchard, the trees we can actually see are shown in the circles. They form the co-prime pattern, which extended endlessly never exactly repeats itself, but is nonetheless precisely determined. This pattern is described in the Scale Tree/Peirce Series/Stern-Brocot Series, as it is likewise found in the Lambdoma/Farey Series. Variations on this pattern are found throught nature, the arts, the sciences, and in many surprisingly unexpected places. Interesting and diverse applications are found in musical scales and their associated keyboards. 22 June 2000EW

# Co-prime Moves, on a 5+7 Cross-Grid

© 1999 by Erv Wilson



I was doing something like this at BYU circa 1950, after reading Joseph Yasser's A Theory of Evolving Tonality. At the time I did not see the co-prime moves pattern from "0".

# Co-prime Moves, on the cap 9 Lambda

© 1999 by Erv Wilson, all rights reserved



The reducible rationals are struck out. The remaining, irreducible rationals form a co-prime moves pattern from " $\frac{0}{0}$ ". Compare this with Yasserian Keyboard Guide, by Erv Wilson 1994.

# How to Construct a Co-Prime Grid

22 NOV 99, 5:10

©1999 by Ervin M. Wilson, all proprietary rights reserved

fig 1. assuming roots

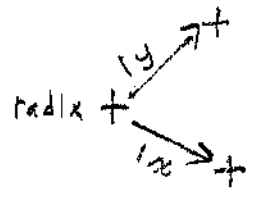
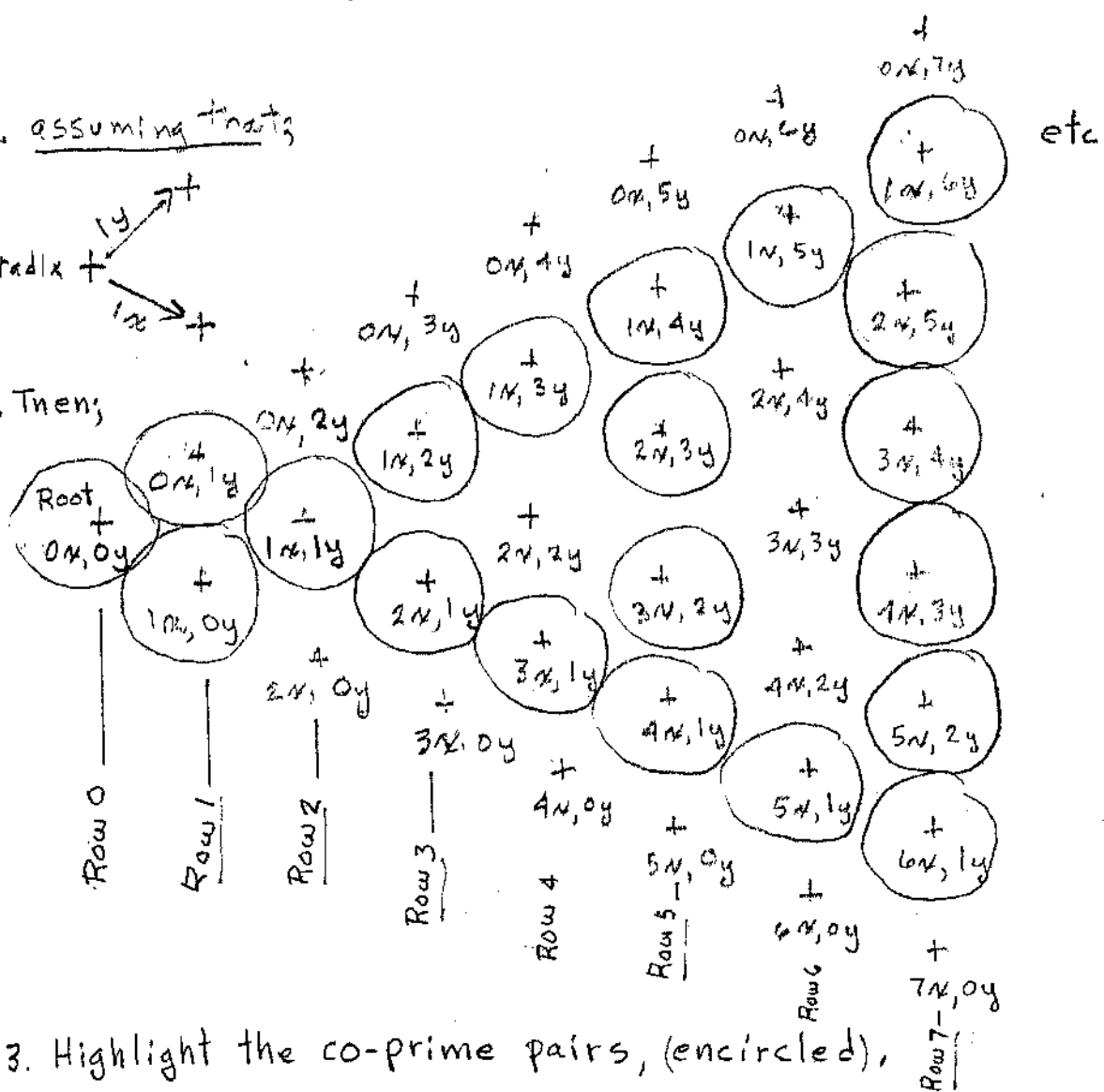


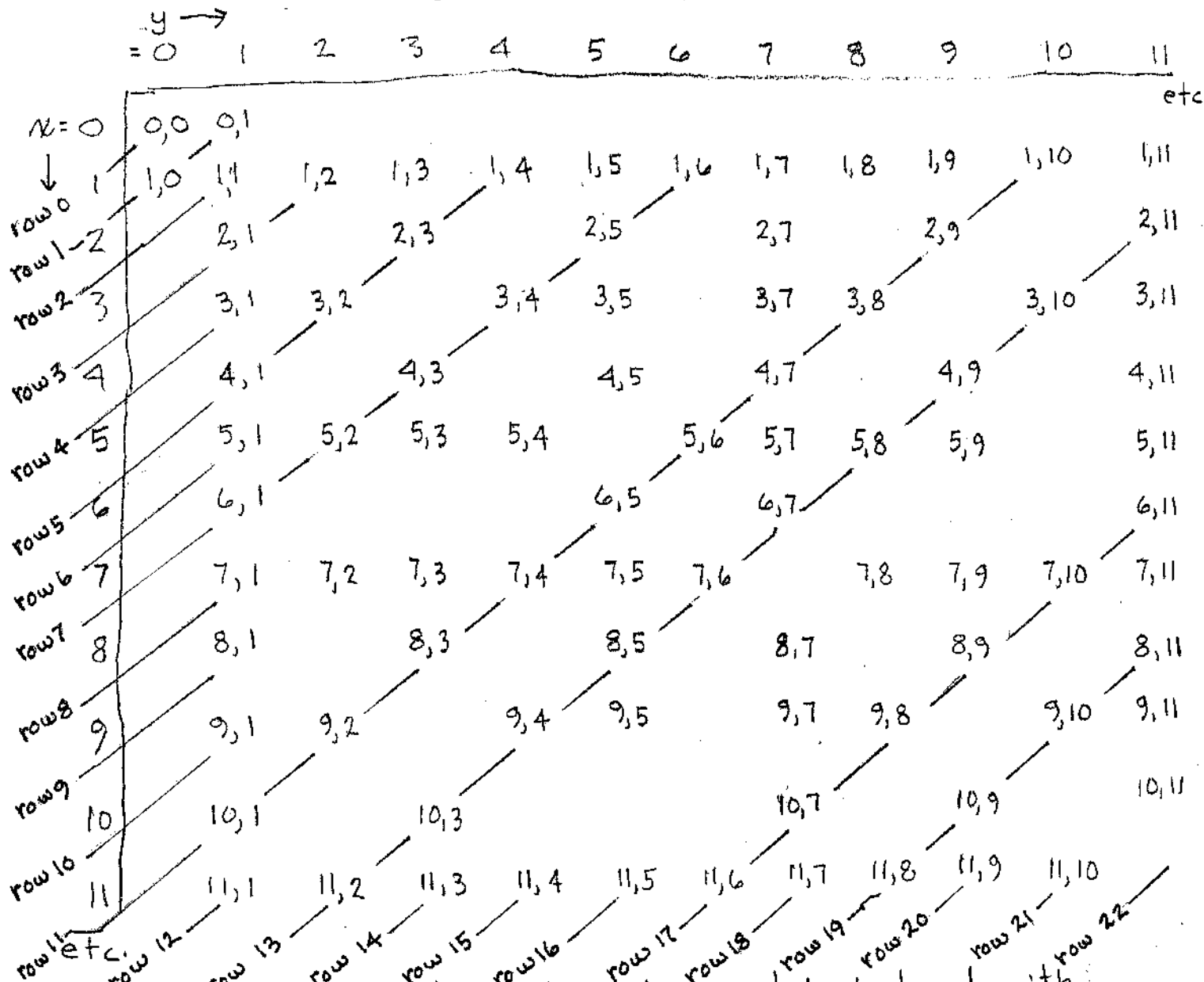
Fig 2. Then;



3. Highlight the co-prime pairs, (encircled),
4. Neglect or suppress the reducible pairs, (not encircled)

Comments; The above fig 2 shows, from the Root  $(0x, 0y)$ , all generalized Octave sites and their respective Generator sites, out to row 7. The grid extends endlessly.

Co-Prime Logic Diagram, (to cap 11) 23 Nov 99 EW  
 © 1999 by Ervin M. Wilson, all proprietary rights reserved

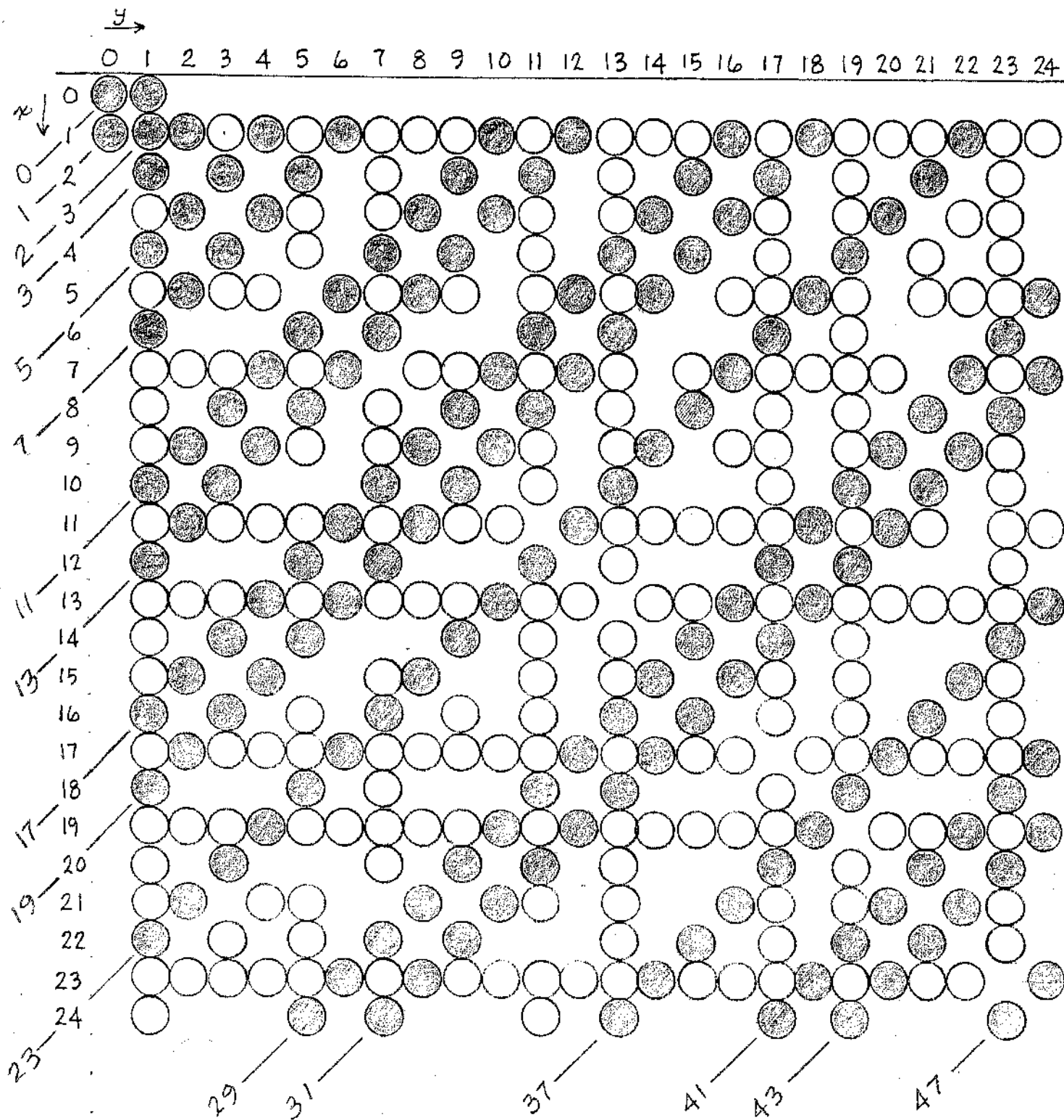


This diagram extends endlessly, and is imbued with Properties applicable to musical scales and generalized musical keyboards. It contains the essential elements of the Peirce Series (Scale-Tree), the Farey Series (Lambdoma) and the gamut of Fibonacci Series. It gives the  $x, y$  coordinates of the Co-Prime Grid.

# Co-PRIME LOGIC Diagram, to Cap 24

23 NOV 99. EW

© 1999 by Ervin Wilson, all proprietary rights reserved



coprime 362  
 25 ~ 25 403  
 reducible 263

$$263/362 = .726519337$$

11  
7

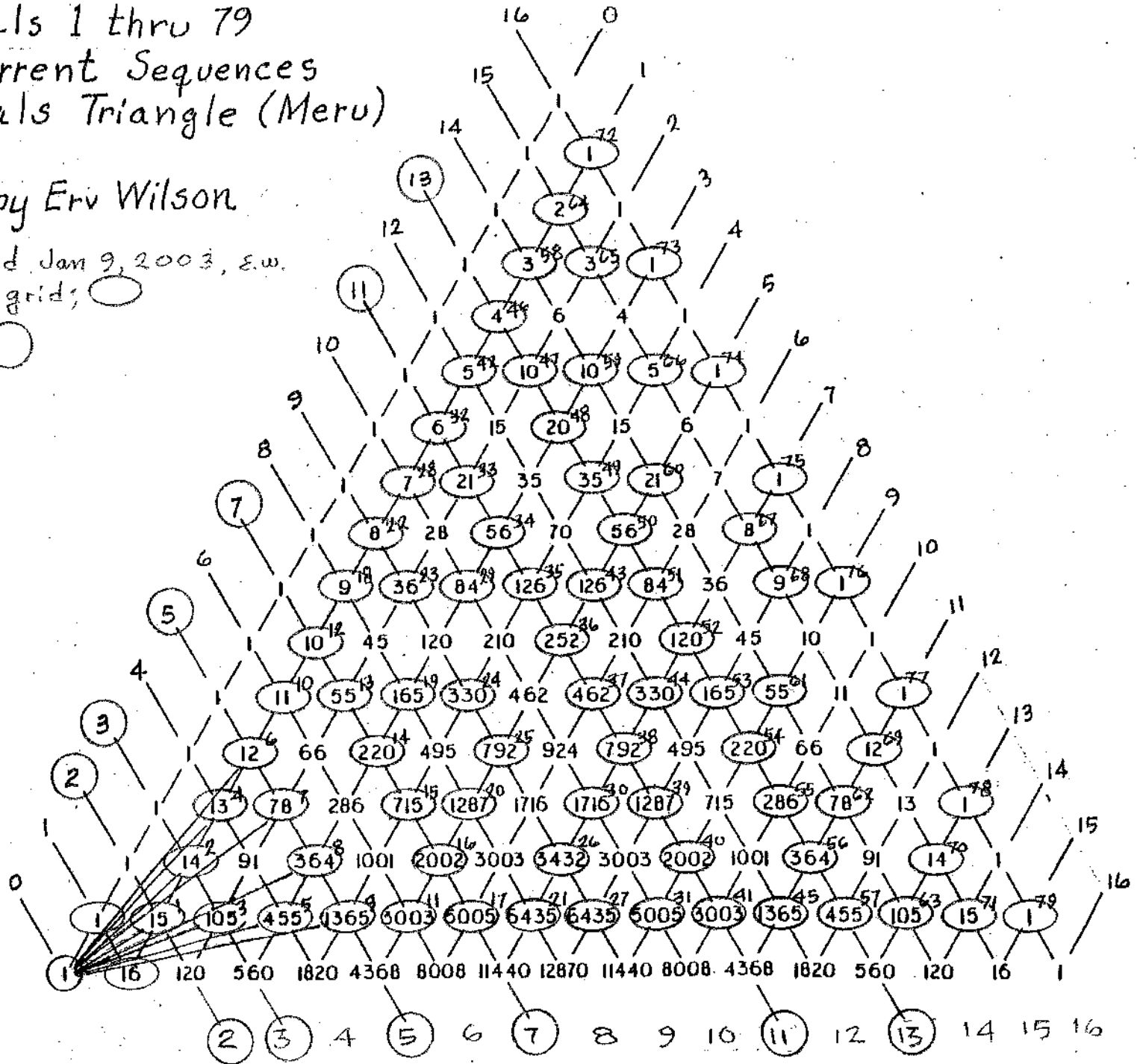
Figure 10, from "Scales of Mt. Meru"

Diagonals 1 thru 79  
 Of Recurrent Sequences  
 In Pascals Triangle (Meru)

© 1996 by Erv Wilson

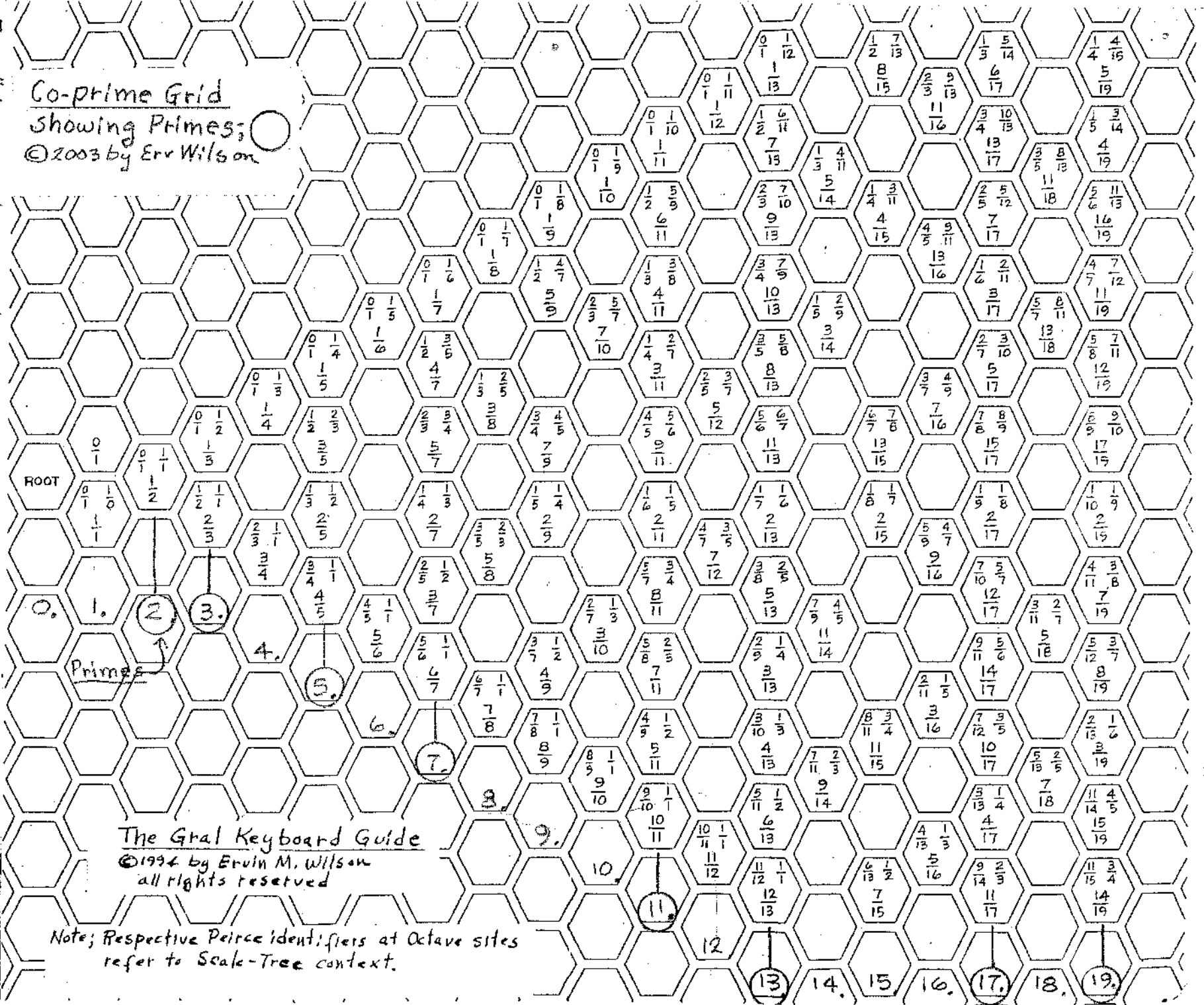
annotated Jan 9, 2003, e.w.  
 co-prime grid; ○

Primes; ○



Ref. "Jumping Champions", Ian Stewart, Scientific American Dec 2000.  
 "Prime Pursuit", Vars Peterson, Science News Oct 26, 2002.

Co-prime Grid  
 showing Primes; ○  
 ©2003 by Err Wilson



The Gral Keyboard Guide  
 ©1994 by Ervin M. Wilson  
 all rights reserved

Note; Respective Peirce identifiers at Octave sites refer to Scale-Tree context.

# PRIME PURSUIT

## Constructing an efficient prime number detector

BY IVARS PETERSON

**P** rime numbers lie at the core of some of the oldest and most perplexing questions in mathematics. Evenly divisible only by themselves and 1, they are the building blocks of integers. In recent decades, prime numbers have emerged from their starring roles in mathematical research (*SN*: 5/25/02, p. 324) by becoming prized commodities—as elements in a cryptographic scheme widely used to keep digital messages secret (*SN*: 2/6/99, p. 95).

Although there are infinitely many primes, they are also relatively scarce and rather haphazardly scattered among the integers. Indeed, of the first 25 billion whole numbers, only 1,091,987,405—or about 4 percent—are primes, and the proportion of primes decreases as the numbers get bigger.

The absence of any readily discernible pattern in their distribution makes identifying primes a tricky proposition. Is 687,532,127 a prime? There's no way to tell simply by looking. Clearly, the number isn't evenly divisible by two, nor by any other even number. Is it divisible by 3? 5? 7? By 26,203? In fact, 687,532,127 has no divisors other than one and itself, so it's a prime.

This process of elimination by trial division is the idea behind the prime-detecting sieve of Eratosthenes, named for a Greek mathematician who lived in the third century B.C. The sieve of Eratosthenes represents a systematic way of checking whether a number is a prime by dividing into the given number all smaller primes, starting with two and going up to the square root of the target number. If none of the integers divides evenly into the given number, the target is a prime. In the case of huge numbers, however, trial division is both tedious and time-consuming.

Even so, the need to undertake such primal analysis has mushroomed because of the increasing importance of cryptography. One widely used cryptographic scheme is based on the notion that, whereas it's relatively easy to multiply together large primes, it's considerably more difficult to factor the resulting number and retrieve the original primes. Yet that operation is just the one required for decoding the encrypted messages. This scheme requires a ready-to-use supply of large primes, so it has encouraged mathematicians and computer scientists to seek increasingly efficient ways of identifying prime numbers.

Now, a team from the Indian Institute of Technology (IIT) in Kanpur, India, has devised a novel approach for detecting primes. The new technique solves a long-standing problem in number

theory and computer science, providing a long-sought improvement in the theoretical efficiency of prime-detecting algorithms.

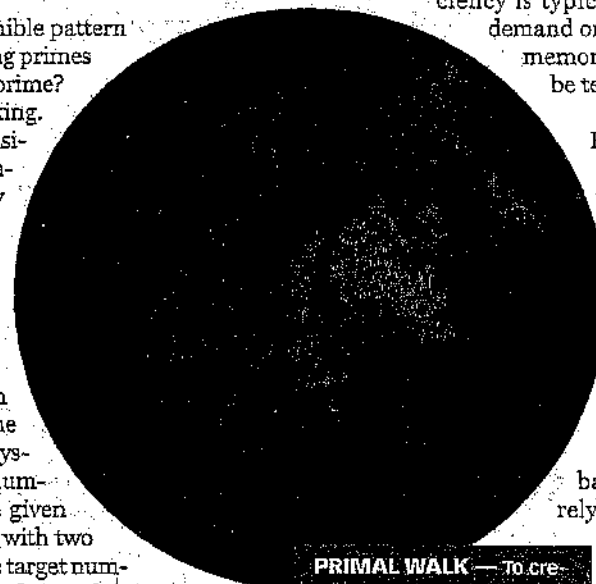
"It is a lovely result and gives the field of algorithmic number theory a shot in the arm," says number theorist Carl Pomerance of Bell Laboratories in Murray Hill, N.J. "I was surprised, especially with the simplicity of the method. My hat is off to them."

The IIT team of Manindra Agrawal, Neeraj Kayal, and Nitin Saxena announced its findings in August. Mathematicians quickly confirmed the validity of the results, and some researchers have already made improvements, offering hope that this novel approach eventually may be turned into a practical, speedy method for finding primes.

**TIME TRIALS** With computers now doing all the heavy lifting in testing for primes, much recent research has focused on the efficiency of competing sets of instructions, or algorithms. This efficiency is typically measured in terms of how the demand on computer resources, such as time or memory, goes up as the size of the number to be tested increases.

The efficiency of the venerable sieve of Eratosthenes, for example, is related to the number of trial divisions required to test a given integer for primality. The trouble is that the number of trial divisions grows exponentially with the number of digits in the target integer. So, although it's a practical way to test integers smaller than 10 billion, which have nine digits, it fails miserably for integers of 25 digits or more.

Today's heavily used, computer-based procedures for detecting primes rely instead on a mathematical shortcut discovered in the 17th century by jurist and mathematician Pierre de Fermat. His so-called little theorem expresses a remarkable relationship involving primes: If an integer  $p$  is a prime number, then for all integers  $a$ , dividing both  $a^p$  and  $a$  by  $p$  gives a result with the same remainder. For example, if  $p = 7$  (a prime) and  $a = 9$ , dividing  $9^7$  by 7 gives a remainder of 2, as does dividing 9 by



**PRIMAL WALK** — To create this nebular image, a plotter moved up, down, left, or right, depending on the value of each of 100 million primes. The plotter changed the color it laid down every time it hit a previously visited spot.

7. Any integer  $p$  that fails this test isn't a prime; it's a composite number with factors other than 1 and itself. However, a few composite numbers also pass the test, so further steps are needed to weed them out to ensure that the target truly is a prime (*SN*: 3/6/82, p. 158).

For practical purposes, it isn't usually necessary to check specifically for these fake primes. The idea behind today's most effi-

cient Fermat-based algorithms is to test the integer in question using a randomly chosen value for  $a$ . If the integer passes the Fermat test, there's only a small probability that it's actually not a prime. If the target integer is tested again with another randomly chosen value of  $a$  and still passes, the probability is even smaller that it's not a prime. The more times it passes, the more likely it is to be an authentic prime. By repeating the test enough times, it's possible to reduce the probability of error to nearly zero. That's good enough for the sorts of primes needed for a prime-based cryptographic system.

**ELUSIVE EFFICIENCY** What had eluded researchers until now, however, was a prime-detecting method that not only always yields a correct answer but also meets another important criterion: efficiency of calculation. Instead of an algorithm requiring an amount of computer time that grows exponentially with the target number's size, computer scientists wanted one that grows more slowly, say, at a rate that's only proportional to the number size or, more likely, a straightforward power of the number size.

For example, suppose that the number of digits in a target integer is  $N$  and the number of digits is doubled to  $2N$ . With exponential growth, the time required to test the number would increase from  $b^N$  to  $b^{2N}$ , where  $b$  is some constant related to the prime-testing algorithm. If, instead, the rate grows as a power of number size, the time would increase at a more sedate pace from  $N^c$  to  $(2N)^c$ , where the exponent  $c$  is a constant. In the latter case, researchers describe the algorithm as taking no more than polynomial time. A polynomial is an algebraic expression containing powers of one or more variables.

To find a prime-detecting algorithm that could do the job in polynomial time, researchers had explored a variety of approaches—some based on highly sophisticated mathematics—but with limited success. In 1999, Agrawal decided to try a relatively simple approach that he noticed had been overlooked by others. He enlisted the aid of Kayal and Saxena, who were undergraduate students at the time. Early computer simulations were encouraging, but only this past summer did the team finally work out the complete method and the mathematical proof establishing its theoretical efficiency.

In effect, the IIT team found a new, generalized version of Fermat's little theorem—one in which the integers  $a^p$  and  $a$  are replaced by polynomial expressions:  $(x - a)^p$  and  $(x^p - a)$ . Using this foundation, they formulated an algorithm that they could

prove had a polynomial running time proportional to  $N^{12}$ .

Primality-testing methods had been getting quicker, but the algorithms had been getting more complex, says Chris K. Caldwell of the University of Tennessee at Martin. "In contrast, [the Agrawal-Kayal-Saxena algorithm] has a shocking simplicity. It's an algorithm that most any programmer can follow," he says.

## PRACTICAL CONCERNS

Achieving a theoretical breakthrough is one thing. Putting it into practice for everyday use is another matter entirely. With a running time proportional to the 12th power of the number of digits, the new algorithm is still painfully slow for relatively small numbers. As it turns out, Caldwell says, "it is far slower than trial division in practice."

However, "one has to be extremely careful when pronouncing something practical or not," warns Richard E. Crandall of the Center for Advanced Computation at Reed College in Portland, Ore.

Indeed, experts who have carefully studied the Agrawal-Kayal-Saxena algorithm have already made improvements. One such variant was developed by Hendrik W. Lenstra of the University of California, Berkeley. Crandall recently demonstrated that a computer programmed with this variant could crack a 30-digit prime in about a day instead of the several years required for the original IIT algorithm.

That's a significant improvement in performance but still far from the speed required to identify, say, 1,000-digit primes.

There's hope, however. A crucial step in Lenstra's variant algorithm can be readily divided up among a large number of computers. A project in which volunteers' computers around the world shared in the calculations could easily handle a 1,000-decimal-digit potential prime in about a year, Crandall estimates. The SETI@home project, in which more than a million computers worldwide have participated in sifting through radio-telescope signals for signs of extraterrestrial life, is one well-known example of such an effort (SN: 3/4/00, p. 152).

Additional improvements in the Agrawal-Kayal-Saxena prime-detecting algorithm may be ahead. "Give number theorists a year with this algorithm, and it should be much clearer what its future is," Caldwell says.

Whatever happens on the practical front, the IIT work stands as a major theoretical advance. Moreover, because the team solved the problem in such an elegant, unexpected manner, mathematicians are now wondering what else they may have overlooked in other mathematical ventures. ■

101	100	99	98	97	96	95	94	93	92	91
102	65	64	63	62	61	60	59	58	57	90
103	66	37	36	35	34	33	32	31	56	89
104	67	38	17	16	15	14	13	30	55	88
105	68	39	18	5	4	3	12	29	54	87
106	69	40	19	6	1	2	11	28	53	86
107	70	41	20	7	8	9	10	27	52	85
108	71	42	21	22	23	24	25	26	51	84
109	72	43	44	45	46	47	48	49	50	83
110	73	74	75	76	77	78	79	80	81	82
111	112	113	114	115	116	117	118	119	120	121

**PRIMAL WALK**— One way to visualize the distribution of prime numbers is to arrange the integers in a square spiral, starting with 1 at the center of a grid, and then color the squares containing primes. Top grid shows primes (red squares) among integers from 1 to 121, and bottom grid shows primes (white or red squares) among integers from 1 to about 65,000. For more: <http://www.sciencenews.org/20020504/mathtrk.asp>

301 300 299 298 297 296 295 294 **293** 292 291

302 244 243 242 241 240 **239** 238 237 236 235 290

303 245 193 192 191 190 189 188 187 186 185 234 289

304 246 194 148 147 146 145 144 143 142 141 184 233 288

305 247 195 **149** **109** 108 107 106 105 104 **103** 140 183 232 287

306 248 196 150 110 76 75 74 **73** 72 71 102 139 182 231 286

**307** 249 **197** 151 111 77 49 48 **47** 46 45 70 101 138 181 230 285

308 250 198 152 112 78 50 28 17 26 25 44 69 100 137 180 229 284

309 **251** 199 153 **113** **79** 51 **29** **13** 12 11 24 43 68 99 126 179 228 **283**

310 252 200 154 114 80 52 30 14 4 **3** 10 23 42 **67** 98 135 178 227 282

**311** 253 201 155 115 81 **53** **31** 10 5 1 2 9 22 41 66 97 134 177 226 **281**

312 254 202 156 116 82 54 32 16 6 7 8 31 40 65 96 133 176 225 280

313 255 203 **157** 117 **83** 55 33 17 18 19 20 29 64 95 132 175 224 279

314 256 204 158 118 84 56 34 35 36 **37** 38 63 94 131 174 223 278

315 257 205 159 119 85 57 35 58 **59** 60 61 62 93 130 173 222 **277**

316 258 206 160 120 86 58 38 **89** 90 91 92 129 172 221 276

**317** 259 207 161 121 122 123 124 125 126 **127** 128 171 220 275

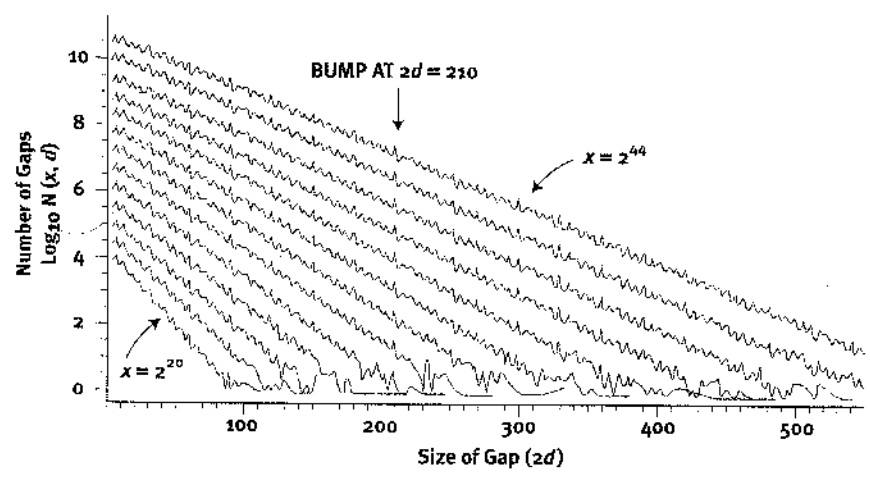
318 260 208 162 163 164 165 **166** 167 168 169 170 219 274

319 261 209 210 211 212 213 214 215 216 217 218 273

320 262 **263** 264 265 266 267 268 **269** 270 271 272

321 322 323 324 325 326 327 328 329 330 **331**





**LOGARITHMIC PLOT** shows how the number of gaps between successive primes less than  $x$  varies with the size of the gap ( $2d$ ). The plot suggests that 210 may be a jumping champion.

persists up to numbers in the trillions may well change as the numbers get still bigger. And that's where the surprise comes in. Odlyzko and his colleagues provide a persuasive argument that somewhere near  $x = 1.7427 \times 10^{35}$  the jumping champion changes from 6 to 30. They also suggest that it changes again, to 210, near  $x = 10^{425}$ .

Except for 4, the conjectured jumping champions fit into an elegant pattern, which becomes obvious if we factor them into primes:

$$\begin{aligned} 2 &= 2 \\ 6 &= 2 \times 3 \\ 30 &= 2 \times 3 \times 5 \\ 210 &= 2 \times 3 \times 5 \times 7 \end{aligned}$$

Each number is obtained by multiplying successive primes together. These numbers are called primorials—like factorials, but using primes—and the next few are 2,310, 30,030 and 510,510. In their article, Odlyzko and his co-authors propose the Jumping Champions Conjecture: the jumping champions are precisely the primorials, together with 4.

Here's a brief explanation of their analysis. Anyone who looks at the sequence of primes notices that every so often two consecutive odd numbers are prime: 5 and 7, 11 and 13, 17 and 19. The Twin Prime Conjecture states that there are infinitely many such pairs. It is based on the idea that primes occur "at random" among the odd numbers, with a probability based on the Prime Number Theorem. Of course, this sounds like nonsense—a number is either prime or not; there isn't any probability involved—but it is reasonable nonsense for this kind of problem. According to a calculation of

probabilities, there is no chance that the list of twin primes is finite.

What about three consecutive odd numbers being prime? There is only one example: 3, 5, 7. Given any three consecutive odd numbers, one must be a multiple of 3, and that number is therefore not prime unless it happens to equal 3. Yet the patterns  $p, p+2, p+6$  and  $p, p+4, p+6$  cannot be ruled out by such arguments, and they seem to be quite common. For example, the first type of pattern occurs for 11, 13, 17 and again for 41, 43, 47. The second type of pattern occurs for 7, 11, 13 and again for 37, 41, 43.

About 80 years ago English mathematicians Godfrey Harold Hardy and John Edensor Littlewood analyzed patterns of this kind involving larger numbers of primes. Using the same kind of probabilistic calculation that I described for the twin primes, they deduced a precise formula for the number of sequences of primes with a given pattern of gaps. The formula is complicated, so I won't show it here; see the article in *Experimental Mathematics* and the references therein.

From the Hardy-Littlewood work, Od-

lyzko and his colleagues extracted a formula for  $N(x, d)$ , which is the number of gaps between consecutive primes when the gap is of size  $2d$  and the primes are less than  $x$ . (We use  $2d$  rather than  $d$  because the size of the gap has to be even.) The formula is expected to be valid only when  $2d$  is large and  $x$  is much larger. The illustration at the left shows how  $\log N(x, d)$  varies with  $2d$  for 13 values of  $x$  ranging from  $2^{20}$  to  $2^{44}$  (in this graph,  $\log$  denotes a base 10 logarithm). Each plot line is approximately straight but has lots of bumps. A particularly prominent bump occurs at  $2d = 210$ , the conjectured jumping champion for very large  $x$ . (It would look even more prominent if the logarithmic graphing didn't flatten it out.) This kind of information suggests that the  $N(x, d)$  formula is not too wide off the mark.

Now, if  $2d$  is going to be a jumping champion, the value of  $N(x, d)$  has to be pretty big. The best way to achieve this is if  $2d$  has many distinct prime factors. Also,  $2d$  should be as small as possible subject to this condition, so the most plausible choices for  $2d$  are the primorials. The known jumping champion 4 is presumably an exception. It occurs at a size where the  $N(x, d)$  formula isn't a good approximation anyway. The formula also lets us work out roughly when a given primorial takes over from the previous one as the new jumping champion.

What's left for recreational mathematicians to do? Prove the Jumping Champions Conjecture, of course—or disprove it. If you can't do either, try searching for other interesting properties of the gaps between primes. For example, what is the least common gap (that actually occurs) between consecutive primes less than  $x$ ? And which gap occurs closest to the average number of times? As far as I know, these questions are wide open, even for relatively small values of  $x$ .

### READER FEEDBACK

In a recent column on logical paradoxes ["Paradox Lost," June], I argued that the Surprise Test paradox rests on an inconsistent interpretation of the word "surprise" and isn't really a paradox at all.

Several readers drew my attention to an article entitled "Surprise Maximization" in *American Mathematical Monthly* (Vol. 107, No. 6, June–July 2000). The authors define a measure of surprise and ask what strategy the teacher should follow to maximize the students' surprise. They conclude that in choosing the day of the week for the test, the teacher should use a probability distribution that remains roughly constant through the early part of the week but increases rapidly in the last few days. Under this strategy, Friday would be chosen most often. —I.S.

ALL ILLUSTRATIONS BY DE PAUL LINDSEY