A5265 Scan Guy a Nowahowshi all to 6 segs

£91

THE UNIVERSITY OF CALGARY

Department of Mathematics Statistics and Computing Science 5265

DISCOVERING PRIMES WITH EUCLID

Richard Guy and Richard Nowakowski

Research Paper No. 260

November 1974

DISCOVERING PRIMES WITH EUCLID

Richard Guy and Richard Nowakowski

If we "discover" primes by Euclid's process,

$$a_0 = 1 + 1 = 2,$$
 $a_1 = 2 + 1 = 3,$
 $a_2 = 2.3 + 1 = 7,$
 $a_3 = 2.3.7 + 1 = 43,$

 $a_{4} = 2.3.7.43 + 1 = 1807 = 13.139,$

 $a_5 = 2.3.7.13.43.139 + 1 = 3263443$ (prime),

 $\alpha_6 = 2.3.7.13.43.139.3263443 + 1 = 10650056950807 = 547.607.1033.31051,$ $\alpha_7 = 2.3.7.13.43.139.547.607.1033.31051.3263443 + 1 = 113423713055421844361000443$ = 29881.67003.9119521.6212157481

where each term is one more than the product of the primes we have so far discovered, starting from the empty product 1, and continuing

$$a_n = \prod_{i=0}^{n-1} a_i + 1,$$

(1)
$$a_{n+1} = a_n (a_n - 1) + 1,$$

then we may wonder if, for example, we will ever discover the prime 5. The answer is "No", as may be seen by looking at the residues of α_n , modulo 5: 2,3,2,3,2,3,...; in fact, from α_4 on, the final three decimal digits of α_n are ...807 or ...443, according as n is even or odd.

More generally, if a prime p>3 divides a_{n+1} , then (1) tells us that

$$a_n^2 - a_n + 1 \equiv 0, \mod p,$$

$$(2a_n-1)^2 \equiv -3, \mod p$$
.

Now -3 is a quadratic residue only for primes 6k+1, [3, Theorem 96] so no primes of the form 6k-1 will occur. Note that we now have a proof that there are infinitely many primes of the form 12k-5, since each α_n (n>1) is of this form and no α_n can contain only factors of the form 12k+1. So there are infinitely many primes of the form 6k+1. This complements the result concerning primes 6k-1 [3, Theorem 12], just as the results concerning primes $4k\pm1$ [3, Theorems 11 and 14] complement each other.

Will all the primes 6k+1 occur? The answer is still "No", but it seems difficult to characterize the ones which do. The candidates are

7,13,19,31,37,43,61,67,73,79,97,103,109,127,139,151,157,...

of which we have already seen 7,13,43,139,547,607,...

We calculated the residues of a_n ($n=0,1,2,\ldots$), mod p, for each prime $p\equiv 1$, mod 6, p<1120. The least values of n and k for which $a_n\equiv a_{n+k}$, mod p are called the preperiod and the period. Table 1

lists the preperiod and period for each of these primes. It seems unlikely that there is any simple relationship between the entries. A prime will appear as a factor of one of the a_n just if the period is 1, for if $p \mid a_k$ for some k, then $a_{k+1} = a_k(a_k-1) + 1 \equiv 1$, mod p, and, by induction, $a_{k+r} \equiv 1$, mod p, for all $r \geqslant 1$ and the period is 1. Conversely, if the period is 1, $a_{k+r} \equiv a$ for some k and all $r \geqslant 1$; $a_{k+2} = a_{k+1}(a_{k+1}-1) + 1 \equiv a_{k+1}$, mod p; $(a_{k+1}-1)^2 \equiv 0$ and a = 1, i.e. $a_{k+r} \equiv 1$ for $r \geqslant 1$. Now suppose $a_k \not\equiv 1$, mod p (there is such a k, since $a_0 = 2$). Then $a_k(a_k-1) + 1 \equiv 1$, $a_k(a_k-1) \equiv 0$ and $p \mid a_k$. So the only primes to appear, apart from 2 and 3, are

7,13,43,73,139,181,547,607,1033,...

which occur in a_n for n = 2,4,3,11,4,9,6,6,6,... respectively.

prime preperiod period		9 31 37 0 0 3 4 9 2	4 9		73 79 .2 3 1 14	5	103 2 11	109 20 5	127 7 8	139 5 1	151 5 5	157 2 14	163 2 8	181 10 1	193 1 11	199 2 20
prime preperiod period	211 22 3 18 24	2 2	41 271 8 6 9 23	277 9 27	283 12 7	307 10 8	313 25 2	331 1 21	337 3 19	349 6 5	367 3 10	373 41 4	379 17 18	397 11 6	409 0 18	421 3 37
prime preperiod period	433 439 2 12 47 18	2 3	63 487 7 22 22 6	499 2 12	523 28 32	541 14 21	547 7 1	571 34 8	577 9 27	601 16 8	607 7 1	613 28 2	619 20 3	631 41 10	643 4 13	661 0 33
prime preperiod period	673 693 37 6 12 38	5 23	27 733 9 17 10 39	739 7 4	751 2 16	757 6 4	769 24 6	787 56 10	811 13 23	823 28 23	829 14 14	853 4 12	859 19 3	871 64 2	883 8 44	907 8 18
prime preperiod period	919 93 1 21 16 2	7 24	91 997 39 55 10 10	1009 0 17		5)33] 7 1	L039 18 18	1051 12 10	2	3 4)69 42 25	L087 1 35	1093 25	5 2	L7 20 46

Table 1

In correspondence, Prof. D.H. Lehmer has pointed out to us that in order that

$$a_{n+2} = (a_n^2 - a_n)^2 + (a_n^2 - a_n) + 1$$

should be divisible by p, we must have $x^2+x+1\equiv 0$, mod p, where $x=a_n^2-a_n$. So $a_n^2-a_n\equiv \omega$ or ω^2 where ω , ω^2 are the cube roots of unity other than 1. That is, $1+4\omega$ or $1+4\omega^2$ must be a quadratic residue of p. More generally, the condition for p to appear as a factor of a member of the sequence is that the continued radical

$$-1 \pm 2\sqrt{-1 \pm 2\sqrt{-1 \pm 2\sqrt{-1}}}$$

(where there are n radicals) should be a quadratic residue of p for some choice of signs. That is, if each of these expressions becomes a non-residue of p for all choices of sign, p will never be discovered after n steps. We have a binary tree with root -3. Each residue produces a dicotyledon (outvalence 2); each non-residue is sterile (outvalence 0) and zero is a monocotyledon (outvalence 1). If the height of the tree for the prime p is h, then p occurs in $a_0, a_1, a_2, \ldots, a_h$ or does not occur at all.

Some trees are shown in Figures 1 and 2; we thank D.H. Lehmer for the tree for 1033. The number of non-residues exceeds the number of residues by 1; zero, when it occurs, is not counted as a residue. At first it seems that if p occurs, then zero appears in its tree, but this is not true for p=139, 547, 607 or 1033. Zero can occur in the trees of primes which do not occur, e.g. p=31 and 103. Some data concerning the trees is given in Tables 2 and 3.

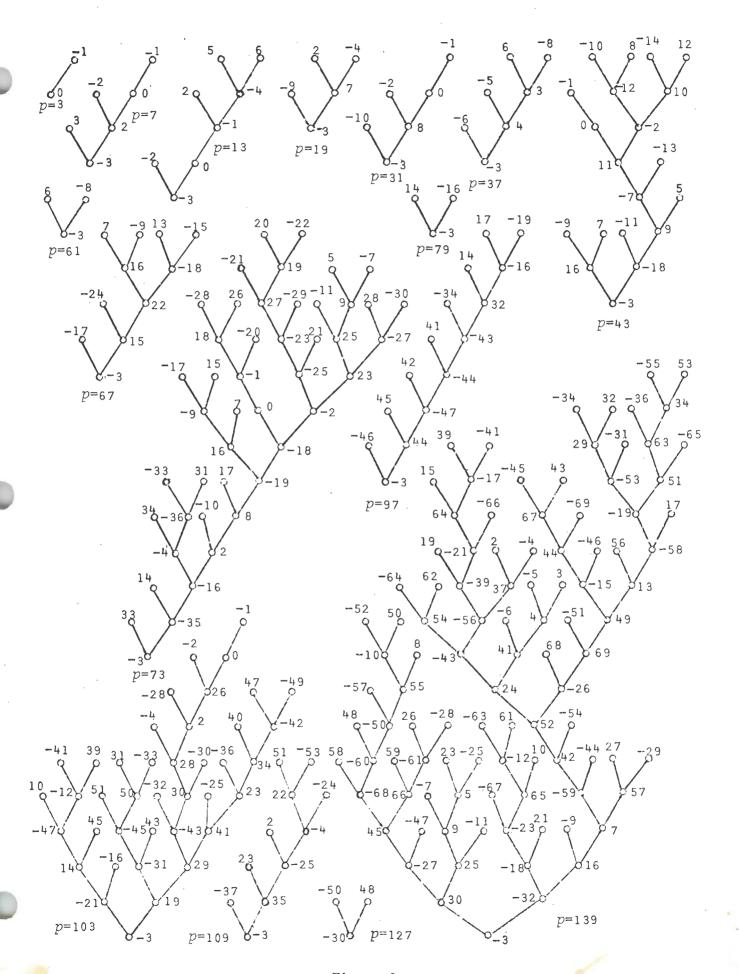


Figure 1

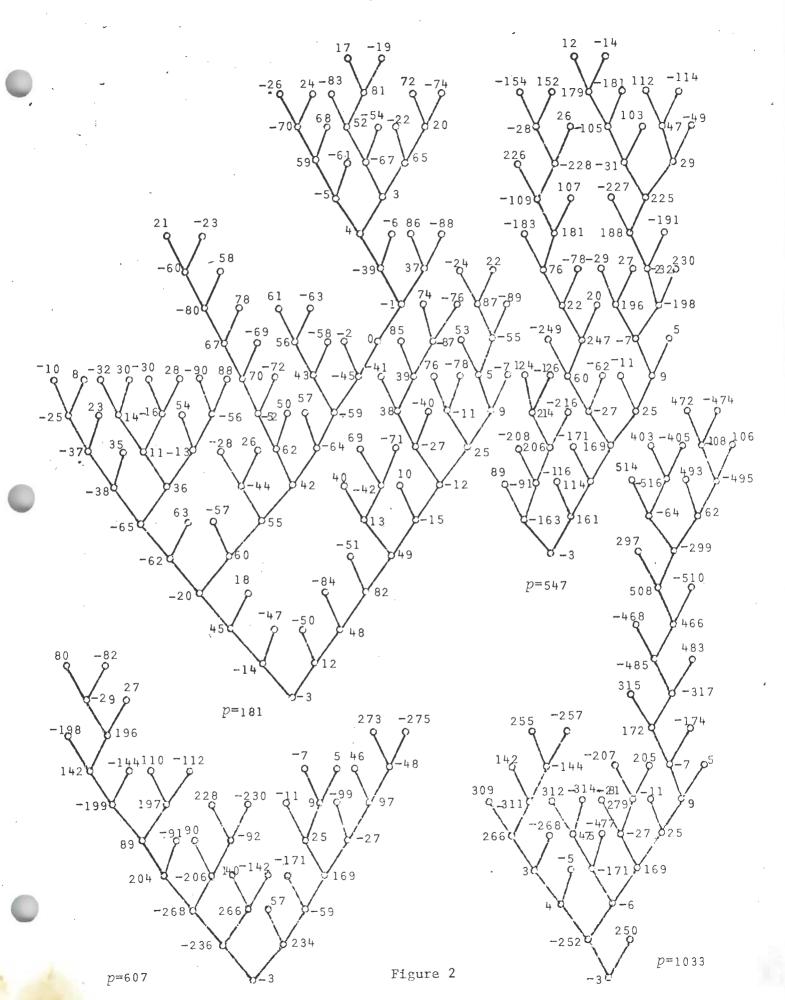
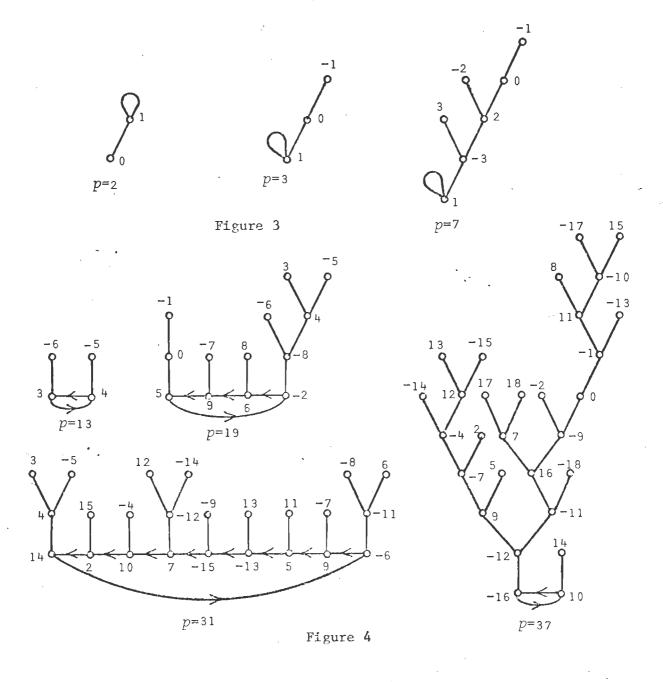


Table 2. Primes which occur

prime	rank of apparition	height of tree	height of zero in tree	number of residues	period	preperiod
(2)	0	(0)	_		1	1
(3)	1	1	0	1	1	2
7	2	3	2	2	1	- 3
13	4	4	1	3	1	5
43	3	7	5	9	1	4
73	11	12	7	22	1	12
139	4	16	_	50	1	5
181	9	18	10	61	1	10
547	6	14	_	29	1	7
607	6	9	_	21	1	7
1033	6	16	_	27	1	7

Table 3. Primes which do not occur

prime	height of tree	height of zero in tree	number of residues	period	preperiod
19	2	_	2	4	0
31-	3	2	2	9	0
37	3	-	3	2	3
61	1	_	1	8	9
67	4		5	3	2
79	1	-	1	14	3
97	7	- · ·	7	3	5
103	9	8	19	11	2
109	5	_	5	5	20
127	1	_	1	8	7
151	9	_	17	5	5
157	3	-	4	14	2



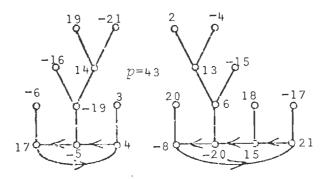


Figure 5

Investigation of the residues and non-residues which do not appear in the tree leads to a structure consisting of a tree with an additional edge, i.e. a circuit with a tree attached to each vertex. The root, -3, of the trees we have already seen springs from the vertex 1 which has a loop attached to it. The "augmented trees" for 2, 3 and 7 are shown in Figure 3. They each contain a complete set of residues. The augmented tree for 5, or for any prime of the form 6k-1, consists only of the vertex 1 with a loop and the vertex -3, which is terminal, being a non-residue. The *complement* is the graph whose vertices do not appear in the augmented tree. The complement for p=5 consists of the circuit 0 and -1 with -2 attached to -1. The complements for p=3 and 7 are empty; those for p=13, 19, 31 and 37 are shown in Figure 4. The complement may break into more than one component, as is shown by p=43 in Figure 5.

Mullin [5] has posed problems concerning similar sequences in which only the least, or only the greatest, of the primes discovered at each stage is included in the next product. Define $p_0^b = a_0^b = 2$ and p_n^b as the least prime factor in

$$a_n^b = 1 + \prod_{i=0}^{n-1} p_i^b,$$

then the sequence $\{p_n^b\}$ is

and appears as number 329 in Sloane's Handbook [6].

A multiprecise routine for prime testing on the Olivetti 101, written by Michael Morrison, enabled us to complete the factorization of a_9^{\slash} . This sequence and the others mentioned in this paper were

945

pursued by J.L. Selfridge and M.C. Wunderlich. For the two known sequences a_8 is composite with no factor less than 10^7 ; no larger terms were calculated. The remaining sequences were calculated as far as possible, completely factoring all numbers of less than 35 digits and searching to 10^7 on larger numbers $(a_{14}^b, a_9^{\#}, b_{20}^b, b_{11}^{\#})$.

$$a_{9}^{b} = 139.25621.420743244646304724409$$
 $a_{10}^{b} = 2801.2897.489241.119812279.437881957$
 $a_{11}^{b} = 11.1009.241139351.217973650939627698919$
 $a_{12}^{b} = 17.1949.193681376161759185018665262907$
 $a_{13}^{b} = 5471.19940260577270817092450816057441$

so that the next five members of the sequence $\{p_n^b\}$ are 139, 2801, 11, 17 and 5471. It is not known if all primes occur in this sequence; but a probability argument suggests that they do.

The sequence $\{p_n^\#\}$ where $p_n^\#$ is the greatest prime factor in

$$a_n^{\#} = 1 + \prod_{i=1}^{n-1} p_i^{\#},$$

is Sloane's number 330, but this is taken from an erroneous calculation [4] and should read

The error was also copied by Cox and van der Poorten [1], who show that no prime less than 53 occurs in the sequence, except for those which comprise the first four terms. The sequence is monotonic so far, but it seems very unlikely that this property will persist.

946

The sequence $\{a_n\}$ is denoted by $\{b_n^{(1)}\}$ in a paper of Golomb [2], but he is concerned with aspects other than primality.

One can pose analogous problems in which (1) is replaced by

$$b_{n+1} = b_n(b_n+1) - 1 \quad (n>1),$$

where each term is one less than the product of all previous ones. If we start with $b_1 = b_1^{\rlap/b} = b_1^{\rlap/t} = 3$, we obtain $b_2 = 2$, $b_3 = 5$, $b_4 = 29$, $b_5 = 869 = 11.79$, $b_6 = 756029 = 19.39791$,

 $b_7 = 571580604869 = 151.3785302019$

 $b_8 = 326704387862983487112029 = 162897238039.2005585802411$

 $b_9 = 106735757048926752040856495274871386126283608869$

= 3889.27445553368199216261469913930283205483744821

where the last factor is a pseudoprime which has not been tested for primality. The primes, other than 3, 2 and 5, which occur must have 5 as a quadratic residue, i.e. they are of the form $10k\pm1$. Not all of these occur; for example $b_n \equiv 1$, mod 31, for n > 4.

If, instead of all the primes which appear at each stage we select only the least, or the greatest, we obtain the sequences

$$\{q_n^b\}$$
 3,2,5,29,11,7,13,37,32222189,131,136013303998782209, 5265
31,197,19,157,17,8609,1831129,35977,...;
 $\{q_n^{\sharp}\}$ 3,2,5,29,79,68729,3739,6221191,157170297801581, 5266

neither of which is monotonic. It is an open question whether all primes occur in the former sequence, but the same probability argument suggests that they do. Selfridge observes that considerations modulo 3739 and 68729 show that 7, 11, 13, 17, 19 and 23 do not occur in the latter.

Since we wrote this, we have received a letter dated 75:ii:27 in which H.J.Jacte Riele reports that he has pursued the preperiods and periods for primes $p \equiv 1$, mod 6; for p < 10000. This has enabled us to correct some errors in Table 1:enIt also extends the sequence of discovered primes, which now reads

7,13,43,73,139,181,547,607,1033,1171,1459,1861,1987,2029,2287,2437, 4219,4519,6469,7603,8221,9829,...

It is tempting to compare the density of this sequence with that of the primes p which give Mersenne primes 2^p-1 . te Riele also observes that only primes $\equiv \pm 1$, mod 10, can have preperiod 0.

REFERENCES

- C.D. Cox and A.J. Van der Poorten, On a sequence of prime numbers, J. Austral. Math. Soc., 8(1968) 571-574; M.R. 37 #3998.
- 2. Solomon W. Golomb, On certain nonlinear recurring sequences, Amer. Math. Monthly, 70(1963) 403-405; M.R. 26 #6112.
- 3. G.H. Hardy and E.M. Wright, An introduction to the theory of numbers, Oxford University Press, 4th edition, 1960.
- 4. Robert R. Korfhage, On a sequence of prime numbers, Bull. Amer. Math. Soc., 70(1964) 341-342; correction, 747.
- 5. Albert A. Mullin, Recursive function theory (a modern look at a Euclidean idea), Bull. Amer. Math. Soc., 69(1963) 737.
- 6. N.J.A. Sloane, A handbook of integer sequences, Academic Press, 1973.