NOTES

A Fibonacci-like Sequence of Composite Numbers

DONALD E. KNUTH*
Stanford University
Stanford, CA 94305

Ronald L. Graham [1] found relatively prime integers a and b such that the sequence $\langle A_0, A_1, A_2, \dots \rangle$ defined by

$$A_0 = a, \qquad A_1 = b, \qquad A_n = A_{n-1} + A_{n-2} \tag{1}$$

contains no prime numbers. His original method proved that the integers

$$\begin{aligned} a &= 331635635998274737472200656430763 \\ b &= 1510028911088401971189590305498785 \end{aligned} \tag{2}$$

have this property. The purpose of the present note is to show that the smaller pair of integers

$$\begin{aligned} a &= 62638280004239857 \\ b &= 49463435743205655 \end{aligned} \tag{3}$$

also defines such a sequence.

Let $\langle F_0, F_1, F_2, \dots \rangle$ be the Fibonacci sequence, defined by (1) with $a = 0$ and $b = 1$; and let $F_{-1} = 1$. Then

$$A_n = F_{n-1}a + F_n b. \tag{4}$$

Graham's idea was to find eighteen triples of numbers (p_k, m_k, r_k) with the properties that

- p_k is prime;
- F_n is divisible by p_k iff n is divisible by m_k;
- every integer n is congruent to r_k modulo m_k for some k.

He chose a and b so that

$$a \equiv F_{m_k - r_k}, \qquad b \equiv F_{m_k - r_k + 1} \pmod{p_k}. \tag{5}$$

It followed that

$$A_n \equiv 0 \pmod{p_k} \quad \Leftrightarrow \quad n \equiv r_k \pmod{m_k} \tag{6}$$

for all n and k. Each A_n was consequently divisible by some p_k; it could not be prime.

The eighteen triples in Graham's construction were

*This research and/or preparation was supported in part by the National Science Foundation under grant CCR-86-10181, and by the Office of Naval Research contract N00014-87-K-0502.

$$\begin{array}{lll}
(3,4,1) & (2,3,2) & (5,5,1)\\
(7,8,3) & (17,9,4) & (11,10,2)\\
(47,16,7) & (19,18,10) & (61,15,3)\\
(2207,32,15) & (53,27,16) & (31,30,24)\\
(1087,64,31) & (109,27,7) & (41,20,10)\\
(4481,64,63) & (5779,54,52) & (2521,60,60)
\end{array} \tag{7}$$

(It is easy to check that the second property above holds, because m_k is the first subscript such that F_{m_k} is divisible by p_k. The third property holds because the first column nicely "covers" all odd values of n; the middle column covers all even n that are not divisible by 6; the third column covers all multiples of 6.) It is not difficult to verify by computer that the values of a and b in (2) satisfy (5) for all eighteen triples (7); therefore, by the Chinese remainder theorem, these values are the smallest nonnegative integers that satisfy (5) for $1 \leqslant k \leqslant 18$. Moreover, these huge numbers are relatively prime, so they produce a sequence of the required type.

Incidentally, the values of a and b in (2) are not the same as the 34-digit values in Graham's original paper [1]. A minor slip caused his original numbers to be respectively congruent to F_{32} and F_{33} (mod 1087), not to F_{33} and F_{34}, although all the other conditions were satisfied. Therefore the sequences defined by his published starting values may contain a prime number A_{64n+31}. We are fortunate that calculations with large integers are now much simpler than they were in the early 60s when Graham originally investigated this problem.

But we need not use the full strength of (5) to deduce (6). For example, if we want

$$A_n \equiv 0 \pmod 3 \quad \Leftrightarrow \quad n \equiv 1 \pmod 4,$$

it is necessary and sufficient to choose $a \not\equiv 0 \pmod 3$ and $b \equiv 0 \pmod 3$; we need not stipulate that $a \equiv 2$ as required by (5). Similarly if we want

$$A_n \equiv 0 \pmod{17} \quad \Leftrightarrow \quad n \equiv 4 \pmod 9$$

it is necessary and sufficient to have

$$A_4 \equiv 0 \pmod{17} \quad \text{and} \quad A_5 \not\equiv 0 \pmod{17};$$

the sequence $\langle A_4, A_5, A_6, \ldots \rangle$ will then be, modulo 17, a nonzero multiple of the Fibonacci sequence $\langle F_0, F_1, F_2, \ldots \rangle$. The latter condition can also be rewritten in terms of a and b,

$$b \equiv 5a \pmod{17} \quad \text{and} \quad a \not\equiv 0 \pmod{17},$$

because $A_4 = 2a + 3b$ and $A_5 = 3a + 5b$. This pair of congruences has 16 times as many solutions as the corresponding relations $a \equiv 5$ and $b \equiv 8$ in (5).

Proceeding in this way, we can recast the congruence conditions (6) in an equivalent form

$$b \equiv d_k a \pmod{p_k} \quad \text{and} \quad a \not\equiv 0 \pmod{p_k}, \tag{8}$$

for each of the first seventeen values of k. We choose d_k so that

$$F_{r_k - 1} + d_k F_{r_k} \equiv 0 \pmod{p_k};$$

this can be done since $0 < r_k < m_k$, hence F_{r_k} is not a multiple of p_k. The following pairs (p_k, d_k) are obtained:

(3,0)	(2,1)	(5,0)
(7,3)	(17,5)	(11,10)
(47,3)	(19,17)	(61,30)
(2207,3)	(53,4)	(31,21)
(1087,3)	(109,100)	(41,21)
(4481,1)	(5779,2)	(2521, *)

In each case we have

$$F_{r_k} + d_k F_{r_k+1} \not\equiv 0 \pmod{p_k}.$$

(Otherwise it would follow that $F_n + d_k F_{n+1} \equiv 0$ for all n and we would have a contradiction when $n = 0$.)

The final case is different, because $r_{18} = m_{18}$. We want

$$a \equiv 0 \pmod{2521} \quad \text{and} \quad b \not\equiv 0 \pmod{2521} \tag{9}$$

in order to ensure that the numbers A_{60n} are divisible by 2521.

Let us therefore try to find "small" integers a and b that satisfy (8) and (9). The first step is to find an integer D such that

$$D \equiv d_k \pmod{p_k} \tag{10}$$

for $1 \leqslant k \leqslant 17$. Then (8) is equivalent to

$$b \equiv Da \pmod{P} \quad \text{and} \quad \gcd(a, P) = 1, \tag{11}$$

where

$$P = p_1 p_2 \cdots p_{17} = 975774869427437100143436645870. \tag{12}$$

Such an integer D can be found by using the Chinese remainder algorithm (see, for example, Knuth [2, Section 4.3.2]); it is

$$D = -254801980782455829118669488975, \tag{13}$$

uniquely determined modulo P.

Our goal is now to find reasonably small positive integers a and b such that

$$a = 2521n, \qquad b = aD \bmod P, \tag{14}$$

for some integer n. If a and b are also relatively prime, we will be done, because (8) and (9) will hold.

Let $C = 2521D \bmod P$. We can solve (14) in principle by trying the successive values $n = 1, 2, 3, \ldots$, looking for small remainders $b = nC \bmod P$ that occur before the value of $a = 2521n$ gets too large. In practice, we can go faster by using the fact that the smallest values of $nC \bmod P$ can be computed from the continued fraction for C/P (or equivalently from the quotients that arise when Euclid's algorithm is used to find the greatest common divisor of C and P).

Namely, suppose that Euclid's algorithm produces the quotients and remainders

$$\begin{aligned} P_0 &= q_1 P_1 + P_2, \\ P_1 &= q_2 P_2 + P_3, \\ P_2 &= q_3 P_3 + P_4, \ \ldots \end{aligned} \tag{15}$$

when $P_0 = P$ and $P_1 = C$. Let us construct the sequence

$$n_0 = 1, \qquad n_1 = q_1, \qquad n_j = q_j n_{j-1} + n_{j-2}. \tag{16}$$

Then it is well known (and not difficult to prove from scratch, see Knuth [3, exercise 6.4–8]) that the "record-breaking" smallest values of $nC \bmod P$ as n increases, starting at $n = 1$, are the following:

n	$nC \bmod P$	
$kn_1 + n_0$	$P_1 - kP_2$	for $0 \leqslant k \leqslant q_2$
$kn_3 + n_2$	$P_3 - kP_4$	for $0 \leqslant k \leqslant q_4$
$kn_5 + n_4$	$P_5 - kP_6$	for $0 \leqslant k \leqslant q_6$

and so on. (Notice that when, say, $k = q_4$, we have $kn_3 + n_2 = n_4$ and $P_3 - kP_4 = P_5$; so the second row of this table overlaps with the case $k = 0$ of the third row. The same overlap occurs between every pair of adjacent rows.) In our case we have

$$\langle q_1, q_2, q_3, \ldots \rangle = \langle 1,2,3,2,1,3,28,1,4,1,1,1,6,12626,1,195,4,7,1,1,2,\ldots \rangle \tag{17}$$

and it follows that

$$\langle n_1, n_2, n_3, \ldots \rangle = \langle 1,3,10,23,33,122,\ldots \rangle.$$

The record-breaking values of $nC \bmod P$ begin with

n	$nC \bmod P$
1	6798454001099037863589679223355
2	3839159307923704725744991988840
3	879864614748371587900304753325
13	560163765818153213756531777785
23	240462916887934839612758802455

These special values of n increase exponentially as the values of $nC \bmod P$ decrease exponentially.

The "best" choice of $a = 2521n$ and $b = nC \bmod P$, if we try to minimize $\max(a, b)$, is obtained when a and b are approximately equal. This crossing point occurs among the values $n = kn_{17} + n_{16}$, for $0 \leqslant k \leqslant q_{18} = 7$, when we have

$a = 2521n$	$b = nC \bmod P$	$\gcd(a, b)$
2502466953682069	237607917830996295	11
12525102462108367	206250504149697855	1
22547737970534665	174893090468399415	35
32570373478960963	143535676787100975	1
42593008987387261	112178263105802535	17
52615644495813559	80820849424504095	1
62638280004239857	49463435743205655	1
72660915512666155	18106022061907215	5

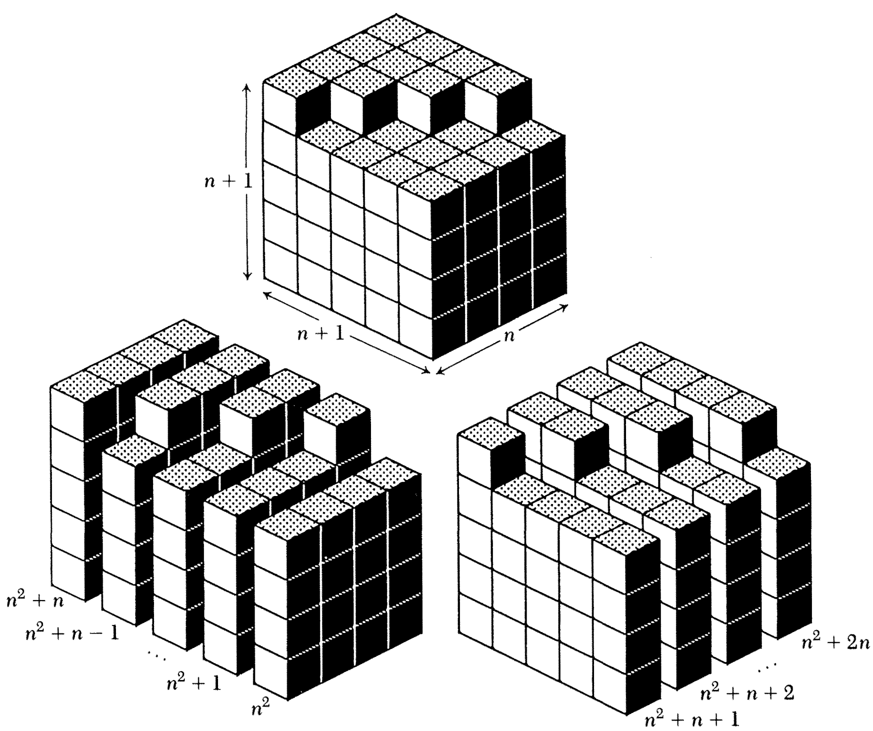
We must throw out cases with $\gcd(a, b) \neq 1$, but (luckily) this condition doesn't affect the two values that come nearest each other. The winning numbers are the 17-digit values quoted above in (3).

Slight changes in (7) will probably lead to starting pairs (a, b) that are slightly smaller than the 17-digit numbers in (3). But a proof applicable to substantially smaller starting values, with say fewer than ten digits each, would be quite remarkable.

REFERENCES

1. Ronald G. Graham, A Fibonacci-like sequence of composite numbers, this Magazine 37 (1964), 322–324.
2. Donald E. Knuth, *The Art of Computer Programming, Vol. 2: Seminumerical Algorithms*. Addison-Wesley, Reading, MA, 1969; second edition, 1981.
3. ______, *The Art of Computer Programming, Vol. 3: Sorting and Searching*. Addison-Wesley, Reading, MA, 1973.

Proof without Words: Consecutive sums of consecutive integers



$$1+2=3$$
$$4+5+6=7+8$$
$$9+10+11+12=13+14+15$$
$$16+17+18+19+20=21+22+23+24$$
$$\vdots$$
$$n^2+(n^2+1)+\cdots+(n^2+n)=(n^2+n+1)+\cdots+(n^2+2n)$$

—ROGER B. NELSEN
Lewis and Clark College
Portland, OR 97219