THE SUBTRACTIVE EUCLIDEAN ALGORITHM AND FIBONACCI NUMBERS

Leonard Chastkofsky
Department of Mathematics, University of Georgia, Athens, GA 30602
(*Submitted June 1999*)

1. INTRODUCTION

In an article in this journal, A. Knopfmacher [1] studied the subtractive Euclidean algorithm. He considered pairs (m, n) of subtractive length K and showed that there are 2^{K-2} coprime pairs with $m > n$ of length K. He also observed that various pairs consisting of Fibonacci and Lucas numbers occur among these pairs.

In this paper we present another approach to studying coprime pairs with subtractive length K. We show how to express the elements in every such pair in terms of Fibonacci numbers. The formula for the number of such pairs follows easily from this. In addition, we obtain the average size of the elements of pairs of length K.

2. ANALYSIS OF THE SUBTRACTIVE ALGORITHM

Let m and be positive integers with $m \geq n$. The subtractive algorithm for finding the greatest common divisor of m and n proceeds from the observation that the gcd of the pair $\{m, n\}$ is the same as that of $\{m-n, n\}$. We can continue this process until we get down to the pair $\{1, 0\}$, where 1 is the gcd of $\{m, n\}$. The number of steps needed is the subtractive length of $\{m, n\}$.

For example, starting with the pair $\{14, 9\}$ we have

$$\{14, 9\} \to \{9, 5\} \to \{5, 4\} \to \{4, 1\} \to \{3, 1\} \to \{2, 1\} \to \{1, 1\} \to \{1, 0\}.$$

The subtractive length of $\{14, 9\}$ is 7.

Let $A = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ and $B = \left(\begin{smallmatrix} 1 & 1 \\ 1 & 0 \end{smallmatrix}\right)$. The idea behind our method is that we obtain each pair in the algorithm from the preceding one by using either matrix A or B.

Theorem 1: Let $\{m, n\}$ be a coprime pair with $m > n$, $m \geq 2$. Then $\binom{m}{n}$ can be expressed uniquely as $M_1 M_2 \ldots M_{K-2} M_{K-1} M_K \binom{1}{0}$, where all M_i are equal to either A or B and $M_{K-1} = A$, $M_K = B$. The subtractive length of $\{m, n\}$ is equal to K in the above representation.

Proof: We prove this by induction on the larger element of the pair, m. The smallest such pair is $\{2, 1\}$ and $\binom{2}{1} = AB\binom{1}{0}$, so the result is true in this case. Suppose that it is true for smaller pairs than $\{m, n\}$. If $m-n > n$, then $\binom{m}{n} = A\binom{m-n}{n}$ and $\{m-n, n\}$ has a unique such representation of length $K-1$. If $n > m-n$, then $\binom{m}{n} = B\binom{n}{m-n}$ and $\{n, m-n\}$ has a unique such representation of length $K-1$. In either case, $\binom{m}{n}$ has a unique such representation of length K.

Corollary: Let $K \geq 2$. The number of coprime pairs $\{m, n\}$ with $m > n$ and subtractive length K is equal to 2^{K-2}.

Proof: In the above representation, there are 2^{K-2} choices for the M_i, $1 \leq i \leq K-2$.

3. AVERAGE SIZE OF PAIRS WITH GIVEN LENGTH

We now obtain a formula for the average size of coprime pairs $\{m, n\}$ with subtractive length K.

Theorem 2: The sum of $\binom{m}{n}$ over all coprime pairs $\{m, n\}$ with $m > n$ and subtractive length K is

$$\begin{pmatrix} 2\cdot 3^{K-2} \\ 3^{K-2} \end{pmatrix} \text{ for } K \geq 2.$$

Proof: We get all such pairs by applying a product $M_1 M_2 \ldots M_{K-2}$ to $\binom{2}{1}$, where M_i is either A or B. We get all such products by expanding $(A+B)^{K-2}$. But $A+B = \left(\begin{smallmatrix} 2 & 2 \\ 1 & 1 \end{smallmatrix}\right)$, so

$$(A+B)^{K-2} = \begin{pmatrix} 2\cdot 3^{K-3} & 2\cdot 3^{K-3} \\ 3^{K-3} & 3^{K-3} \end{pmatrix}.$$

Thus, the required sum is

$$(A+B)^{K-2}\begin{pmatrix} 2 \\ 1 \end{pmatrix} = \begin{pmatrix} 2\cdot 3^{K-2} \\ 3^{K-2} \end{pmatrix}$$

as stated.

Combining this with the Corollary to Theorem 1, we obtain the following corollary.

Corollary: The average size of m over all pairs $\{m, n\}$ as above is $2\cdot\left(\frac{3}{2}\right)^{K-2}$, while that of n is $\left(\frac{3}{2}\right)^{K-2}$.

Knuth and Yao [2] have studied the inverse of this question: Given m, what is the average length of the subtractive algorithm as n varies? The analysis is deep and the answer approximate. On the other hand, the answer to the question as to the average size of m and n given K is exact and the analysis simple.

4. FORMULAS IN TERMS OF FIBONACCI NUMBERS

We can combine equal matrices in the above representation of $\{m, n\}$ to write

$$\begin{pmatrix} m \\ n \end{pmatrix} = A^{a_1}B^{b_1}A^{a_2}B^{b_2}\ldots A^{a_r}B^{b_r}\begin{pmatrix} 1 \\ 0 \end{pmatrix},$$

where all a_i and b_i are positive integers equal to or greater than 1, except perhaps for a_1 which can be 0, while b_r must be 1. The subtractive length of $\{m, n\}$ is $\sum a_i + \sum b_i$.

Remark: Knopfmacher uses a different association of pairs of subtractive length K with sequences that sum to K. Our approach gives an alternative way of seeing that the number of sequences summing to K is 2^{K-1}. (Since b_r must be 1, the rest of the terms in the sequence $a_1, b_1, a_2, b_2, \ldots$ sum to $K-1$, and we have seen that there are 2^{K-2} possibilities.)

Note that

$$A^a = \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix},$$

while B is the matrix generating Fibonacci numbers, so that

$$B^b = \begin{pmatrix} F_{b+1} & F_b \\ F_b & F_{b-1} \end{pmatrix}.$$

We will use the following notation. Let $\{a_1, b_1, a_2, b_2, \ldots, a_r, b_r\}$ be a sequence of integers and let $I_r = \{1, \ldots, r\}$. Let J be a subset of I_r. Define $a_J = \prod_{i \in J} a_i$. Define B_j to be the sequence obtained as follows: First, drop all a_i for which $i \in J$ from the original sequence. Add together consecutive b_i in the remaining sequence. Then B_j is the sequence obtained from the b_i combined this way.

Example 1: Suppose $r = 10$ and $J = \{2, 3, 7, 8, 10\}$. Then

$$B_J = \{b_1 + b_2 + b_3, b_4, b_5, b_6 + b_7 + b_8, b_9 + b_{10}\}.$$

Define B'_J to be the sequence obtained from B_J by adding 1 to its first element.

Example 2: In Example 1,

$$B'_J = \{b_1 + b_2 + b_3 + 1, b_4, b_5, b_6 + b_7 + b_8, b_9 + b_{10}\}.$$

If S is a finite sequence of positive integers, let $F(S) = \prod_{s \in S} F_s$.

Theorem 3: There is a 1-1 correspondence between coprime pairs $\{m, n\}$ with $m > n$ and subtractive length $K \geq 2$ and sequences of integers $\{a_1, b_1, a_2, b_2, \ldots, a_r, b_r\}$ with all a_i and b_i positive integers, except perhaps for a_1 which can be 0, and with $b_r = 1$ and $\sum a_i + \sum b_i = K$. If $\{m, n\}$ corresponds to the sequence $\{a_1, \ldots, b_r\}$, then

$$n = \sum_{\substack{J \subset I_r \\ 1 \notin J}} a_J F(B_J) \quad \text{and} \quad m = a_1 n + \sum_{\substack{J \subset I_r \\ 1 \notin J}} a_J F(B'_J).$$

Proof: The correspondence is $\{m, n\} \leftrightarrow \{a_1, \ldots, b_r\}$ where

$$\begin{pmatrix} m \\ n \end{pmatrix} = A^{a_1} B^{b_1} A^{a_2} B^{b_2} \ldots A^{a_r} B^{b_r} \begin{pmatrix} 1 \\ 0 \end{pmatrix}.$$

Using the formulas for A^{a_i} and B^{b_i} given above, and multiplying out the product, we get expressions for m and n in terms of the a_i and b_i. We consider such an expression as a polynomial in the a_i, with every power of a_i being 0 or 1. For $J \subset I_r$, we get the coefficient of $\prod_{i \in J} a_i$ by setting $a_i = 0$ for $i \notin J$ in the expression for $\binom{m}{n}$. It is thus sufficient to consider the cases $J = I_r$ and $J = \{2, \ldots, r\}$. We need to show that the coefficient of $a_2 \ldots a_r$ in n is $F(b_1) \ldots F(b_r)$, while in m it is $F(b_1 + 1) \ldots F(b_r)$, and that the coefficient of $a_1 \ldots a_r$ in m is $F(b_1) \ldots F(b_r)$.

We prove this by induction on r. It is easy to check the formula for $r = 1$. Suppose it holds for $r - 1$. Then it holds for

$$\begin{pmatrix} m' \\ n' \end{pmatrix} = A^{a_2} B^{b_2} \ldots A^{a_r} B^{b_r} \begin{pmatrix} 1 \\ 0 \end{pmatrix}.$$

We have $n = F_{b_1} m' + F_{b_1 - 1} n'$ and $m = (F_{b_1 + 1} + a_1 F_{b_1}) m' + (F_{b_1} + a_1 F_{b_1 - 1}) n'$. The coefficient of $a_2 \ldots a_r$ in m' is $\prod_{i=2}^{r} F_{b_i}$, so this gives the coefficient of n in $a_2 \ldots a_r$ and that of m in $a_2 \ldots a_r$ and $a_1 \ldots a_r$ as stated.

Example 3: We determine all coprime pairs $\{m, n\}$ as above with $r = 2$. Using the theorem, we get $m = F_{b_1 + 2} + a_1 F_{b_1 + 1} + a_2 F_{b_1 + 1} + a_1 a_2 F_{b_1}$ and $n = F_{b_1 + 1} + a_2 F_{b_1}$, since $b_2 = 1$. We have $a_1 + a_2 + b_1 = K - 1$. Specializing a_1 and a_2 to certain small values gives rise to pairs consisting of Fibonacci and Lucas numbers as shown in the following table.

a_1	a_2	m	n
0	1	F_{K+1}	F_K
1	1	F_{K+1}	F_{K-1}
2	1	L_{K-1}	F_{K-2}
0	2	L_{K-1}	L_{K-2}
1	2	L_{K-1}	L_{K-3}

We get more such pairs by considering the case $r = 3$.

Thus, we see how the theorem accounts for the occurrence of Fibonacci and Lucas numbers as coprime pairs of a given length.

It is now easy to account for an observation in [1].

Corollary: For given K, the largest coprime pair $\{m, n\}$ with $m > n$ and subtractive length K is $\{m = F_{K+1}, n = F_K\}$.

Proof: We obtain the largest value by taking as many $M_i = B$ as possible in the product $\prod M_i\binom{1}{0}$, and this gives the stated pair.

5. CONCLUSION

This study was chanced upon while studying decomposition numbers of the finite Chevalley groups. In particular, products of matrices such as those occurring in Theorem 3 arise in the study of decomposition numbers of $SL_3(P^K)$. Their traces give some of the decomposition numbers. Details will be given elsewhere.

REFERENCES

1. A. Knopfmacher. "Elementary Properties of the Subtractive Euclidean Algorithm." *The Fibonacci Quarterly* **30.1** (1992):80-83.
2. D. E. Knuth & A. C. C. Yao. "Analysis of the Subtractive Algorithm for Greatest Common Divisors." *Proc. Nat. Acad. Sci. U.S.A.* **72.12** (1975):4720-22.

AMS Classification Numbers: 11A05, 11B39

❖❖❖