THE SEARCH FOR AURIFEUILLIAN-LIKE FACTORIZATIONS

S. S. Wagstaff, Jr.[1]
Department of Computer Science, Purdue University, West Lafayette, IN 47097, USA
ssw@cerias.purdue.edu

Received: , Revised: , Accepted: , Published:

Abstract

We searched the Cunningham tables for new algebraic factorizations similar to those discovered by Aurifeuille. A naive search would have been too slow. We accelerated it enough to make it feasible. Many interesting results were found.

Dedicated to the memory of John Selfridge, who loved the integers.

1. Introduction

The Cunningham Project, started more than a century ago by Cunningham and Woodall, summarized in their 1925 book [7] and continued to this day by many others [4], studies the factorization of numbers of the form $b^n \pm 1$ with small integers $b > 1$. John Selfridge was one of the leaders of the Cunningham Project from the 1960s until his death in 2010.

Let $\Phi_d(x) \in \mathbb{Z}[x]$ denote the dth *cyclotomic polynomial*, the monic, irreducible polynomial whose roots are the primitive dth roots of unity. The degree of $\Phi_d(x)$ is given by Euler's totient function $\phi(d)$. Let $n > 1$ be an integer. An important property of cyclotomic polynomials is the product $x^n - 1 = \prod_{d|n} \Phi_d(x)$. Substituting $x = b$ into this formula gives a (partial) factorization of the integer $b^n - 1$. The factorization is nontrivial except when $b = 2$ and n is prime. Likewise, $x^n + 1$ can be partially factored as $\prod \Phi_d(x)$ where the product extends over integers d dividing $2n$ but not n (because $x^n + 1 = (x^{2n} - 1)/(x^n - 1)$). This gives a factorization of $b^n + 1$ which is nontrivial when n is not a power of 2. We call these product formulas the *cyclotomic factorizations* of $b^n - 1$ and $b^n + 1$.

Aurifeuillian factorizations are algebraic factorizations of $b^n \pm 1$ (or more generally $a^n \pm b^n$) which go beyond the cyclotomic factorization of some of these numbers.

[1]The author was supported by the Center for Education and Research in Information Assurance and Security at Purdue University.

The simplest one is the identity

$$2^{4k-2}+1=(2^{2k-1}-2^k+1)(2^{2k-1}+2^k+1), \tag{1}$$

which factors the number 2^n+1, with $n=4k-2$, in a different way from the cyclotomic factorization of this number. The number $3^{3m}+1$ always has the cyclotomic factorization $(3^m+1)(3^{2m}-3^m+1)$, but the second factor could be prime. However, when $m=2k-1$ is odd, the second factor splits into two nearly equal parts:

$$3^{6k-3}+1=(3^{2k-1}+1)(3^{2k-1}-3^k+1)(3^{2k-1}+3^k+1). \tag{2}$$

In the Cunningham notation, the trinomial factor with -3^k is called "L" while the one with $+3^k$ is called "M". Thus, "3,27L" is $3^9-3^5+1=19441$ and "3,27M" is $3^9+3^5+1=19927$.

A *primitive factor* of b^n-1 is one which does not divide b^i-1 for any $i<n$. A *primitive factor* of b^n+1 is one which does not divide b^i+1 for any $i<n$. When Aurifeuillian factorizations occur, they cut across the cyclotomic factorizations and may be used to show that certain $b^n\pm1$ have at least two primitive prime factors. (For example, $3^{27}+1$ has the two primitive prime factors 19441 and 19927.) A corollary of this statement is that there are infinitely many composite pseudoprimes to any base $b>1$. (See Theorem 1 of [13].) Another important application of Aurifeuillian factorizations is to assist in factoring Cunningham numbers. Knuth [11], Section 4.5.4, page 376, gives an example of factoring $2^{214}+1$, a 65-digit number easy with today's factoring methods, but quite hard in 1981. His first step was to use the formula (1). Wagstaff [20] factored

$$\frac{173^{173}-1}{173-1}=347\cdot 685081\cdot 161297590410850151\cdot P176\cdot P184,$$

where $Pxxx$ denotes a prime with xxx decimal digits. If one began naively to factor this number, it would be easy to discover the three small prime factors, but no algorithm known at this time could split the product of the two large prime factors. However, this number admits an Aurifeuillian factorization that breaks it into two nearly equal pieces, each of which is easy to factor. See Table 24, page 455, of Riesel [14] for the coefficients of the Aurifeuillian factorization of $173^{173}-1$ (which were computed by Brent).

Aurifeuille (see Lucas [12]) proved Aurifeuillian factorizations exist for infinitely many b. Schinzel [15] proved the existence of Aurifeuillian factorizations for a^n-b^n in many cases. See [4] for a description of the cyclotomic and Aurifeuillian factorizations and their relation. See [16], [3], [2] and [14] for ways to compute formulas for Aurifeuillian factorizations. Because of their beauty and usefulness, some mathematicians have sought other algebraic identities similar to those Schinzel found. See [9], [18], [17], [5], for example. Granville and Pleasants [8] showed that Schinzel found all such identities, provided one accepts their (reasonable) definition

of "such identities." However, they noted that some numerical examples from the Cunningham tables suggest that other such identities might exist. For example,

$$6^{106}+1 = 37 \cdot 26713 \cdot 1754369260046476588102446137364791189 17 \cdot 175787157418305877173455355755546870641,$$

with two nearly equal (prime) factors. The number $12^{193}-1$ has these two 77-digit (prime) factors:

$$45217442809188335376258573027831301630813739280371078165650059881162723213257$$
$$46575681210815057292336472816642998460431175135914483032447698371111751624211.$$

These two examples do not come from either cyclotomic or Aurifeuillian factorizations.

Whenever examples like these were discovered, John Selfridge would study them for a long time, muttering to himself, "There is something algebraic going on here."

In this note, we describe a systematic empirical search of the Cunningham tables for new algebraic identities beyond those discovered by Schinzel.

2. How the Cunningham Tables Were Searched

It is easy to discover the cyclotomic factorizations in a table of numbers $b^n \pm 1$ in which each number is factored. Look for primes that appear in multiple lines. Aurifeuillian factorizations are slightly harder to find by inspecting tables of factored numbers. It helps if the factors of $b^n \pm 1$ are grouped to form nearly equal products. Here is an example. We have

$$\begin{aligned} N := 5^{35}-1 &= 2 \cdot 2 \cdot 11 \cdot 71 \cdot 211 \cdot 631 \cdot 4201 \cdot 19531 \cdot 85280581 \\ &= (2 \cdot 2 \cdot 19531)\,(71 \cdot 85280581)\,(11 \cdot 211 \cdot 631 \cdot 4201) \\ &= 78124 \cdot 6054921251 \cdot 6152578751 \\ &= (5^7-1) \cdot 6054921251 \cdot 6152578751. \end{aligned}$$

Note that $78124^2 = 6103359376$, so that the three factors in the last line are close to $N^{1/5}$, $N^{2/5}$, $N^{2/5}$, respectively. The two 10-digit factors in the last line give the Aurifeuillian factorization.

We will seek new algebraic identities by grouping primes to form nearly equal products. ("Nearly equal" means that one product equals $1+\varepsilon$ times the other product for some small real number ε.) Suppose $p_1, \ldots, p_k$ are the prime factors in one line of the Cunningham table, or perhaps all the prime factors of b^n-1 or of b^n+1 for particular b and n. We seek subsets $T \subset \{1, \ldots, k\}$ so that

$$\prod_{i \in T} p_i \approx \prod_{i \notin T} p_i.$$

In the example of $5^{35}-1$ above, the algebraic factor 5^7-1 would have to be have to be removed first. Then we would partition the set of primes $\{71, 85280581, 11, 211, 631, 4201\}$ into two subsets with nearly equal products. Later we will explain a way to do this which does not require noticing that 5^7-1 must be removed.

The first observation is that one need not do much arithmetic with multiprecise integers. Rather, it is easier to take logarithms of all the primes, say, $a_i = \log p_i$, and convert the problem to this one involving only sums of real numbers. Given positive real numbers a_1, ..., a_k, find subsets $T \subset \{1, \ldots, k\}$ so that

$$\sum_{i \in T} a_i \approx \sum_{i \notin T} a_i.$$

Some cases are easy. If the largest prime p_k is greater than the product of the other prime factors, then there is at most one useful subset T. If the number k of prime factors (or addends in the equivalent real number problem) is small, then we can examine all 2^{k-1} subsets T containing 1. But in the interesting part of the Cunningham tables, k may be more than 40, too large for a brute force search. For example,

$$3^{1155}+1 = 2\cdot 2\cdot 7\cdot 7\cdot 31\cdot 43\cdot 61\cdot 67\cdot 211\cdot 271\cdot 331\cdot 463\cdot 547\cdot 661\cdot 991\cdots P96\cdot P100 \quad (3)$$

has 44 prime factors, which may be seen at `factordb.com`.

We will actually solve a slightly more general problem. Let $c = \sum_{i=1}^{k} a_i$. Let α be a real number between 0 and 1. We will find subsets $T \subset \{1, \ldots, k\}$ so that $\sum_{i \in T} a_i \approx \alpha c$. The original problem had $\alpha = 1/2$. If we set $\alpha = 1/3$, then we will be seeking a partition of the prime factors of $b^n \pm 1$ into two sets so that the product of the primes in one set is approximately equal to the square of the product of the primes in the other set. One might choose $\alpha = 2/5$ to discover the Aurifeuillian factorization of $5^{35}-1$ in the example above. (Using this α, one need not remove the factor 5^7-1.) With no loss of generality we may assume $0 < \alpha \le 1/2$. When investigating possible factorizations of $b^n \pm 1$, one might use some α for which $n\alpha$ is an integer. In the known Aurifeuillian factorizations of $b^n \pm 1$, the $\alpha = a/b$, where $0 < a \le b/2$ is an integer. We decided to examine these values of α and a few others.

Our method for handling large k was to replace the real numbers by small positive integers. Choose a positive integer K_1 of convenient size. Define integers b_1, ..., b_k by $b_i = \lfloor a_i K_1/c + 0.5 \rfloor$, that is, b_i is $a_i K_1/c$ rounded off to the nearest integer. Since $0 < a_i \le c$ we have $0 \le b_i \le K_1$. Let $K = \sum_{i=1}^{k} b_i$. Then

$$K = \sum_{i=1}^{k} b_i \approx \sum_{i=1}^{k} a_i K_1/c = \frac{K_1}{c} \sum_{i=1}^{k} a_i = \frac{K_1}{c} c = K_1.$$

Also,

$$\sum_{i \in T} b_i \approx \alpha K \quad \Leftrightarrow \quad \sum_{i \in T} a_i \approx \alpha c. \quad (4)$$

We handled the approximate equalities as percentage errors. For example, allowing a 1% error means

$$0.99\alpha c \le \sum_{i\in T} a_i \le 1.01\alpha c.$$

The problem for $b_1, \ldots, b_k$ with $\alpha = 1/2$ is called the *partition problem* in computer science. The general problem with arbitrary α is known as the *subset sum problem*. Wikipedia has articles on both problems. See Section 37.3 of [6], first edition, or Section 35.5 of the second edition of that book, for a discussion of the subset sum problem. Both problems are NP-complete, but heuristics solve the problems quickly in many cases.

We decided to use a variation of the polynomial time approximation algorithm in the Wikipedia article on the subset sum problem. Our algorithm uses a $k \times (K+1)$ matrix $X_{r,j}$ of linked lists of pairs (i, b) of integers with $i + b = j$. The pairs contain information needed to recursively express j as a sum of input numbers b. The pair $(0, b)$ in $X_{0,b}$ represents the number b in the input. When $r > 0$, the pair (i, b) in $X_{r,(i+b)}$ represents the sum of the input number b and the number i whose representation as a sum of input numbers is given in the entry $X_{(r-1),i}$ in the previous row. Here is the algorithm we used.

for $r = 1$ to k { insert $(0, b_r)$ onto X_{1,b_r} }
for $r = 2$ to k {
    for $j = 0$ to K {
        if $X_{(r-1),j} \neq \emptyset$ {
            b_n = least b of $(\cdot, b)$ on $X_{(r-1),j}$
            for $\ell = n + 1$ to $k - 1$ { insert (j, b_ℓ) onto $X_{r,(j+b_\ell)}$ }
        }
    }
}
for $r = 1$ to k {
    for $j \approx \alpha K$ {
        for each entry in $X_{r,j}$ {
            follow the pointers back to construct sets T
            if $\sum_{i\in T} b_i \approx \alpha K$, check whether $\sum_{i\in T} a_i \approx \alpha c$ and print T if so.
        }
    }
}

In the algorithm, the condition $j \approx \alpha K$ means that j is one of the 1, 2 or 3 integers within 1 of the real number αK, unless the percentage error is very large. We may ignore the columns $X_{r,j}$ of the matrix with $j > \alpha K$ (or $j > \alpha K + 1$) because these columns do not matter since their ordered pairs represent sums greater than αK of input numbers.

Here is an example of the algorithm. Suppose $k = 5$ and the input integers b_i are 2, 2, 6, 7, 9. Then $K = 26$. Assume that $\alpha = 0.5$ and the percentage error is so small that only the column with $j = \alpha K = 13$ gives acceptable equal sums. Here is the matrix of linked lists $X_{r,j}$. Rows 4 and 5 are not relevant.

Row	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
1			$(0,2)$ $(0,2)$				$(0,6)$	$(0,7)$		$(0,9)$					
2					$(2,2)$				$(2,6)$	$(2,7)$		$(2,9)$		$(6,7)$	
3											$(4,6)$	$(4,7)$		$(4,9)$	

The only linked list with more than one entry in the matrix is $X_{1,2}$, with two entries. The entry $(4,6)$ in $X_{3,10}$ means that one can express $10 = 4 + 6$, where 6 is an input number and 4 can be expressed by looking at an entry in $X_{2,4}$. In that linked list one finds the pair $(2,2)$, which means that one can express 4 as the sum of the input number 2 plus a 2 from an entry of $X_{1,2}$. There one finds an entry $(0,2)$, meaning that 2 is an input number. By following these links we have expressed $10 = 6 + 2 + 2$, a sum of input numbers.

In the second part of the algorithm one searches the column with $j = 13$. The entry $(4,9)$ in $X_{3,13}$ leads to $13 = 2 + 2 + 9$ and the entry $(6,7)$ in $X_{2,13}$ leads to $13 = 6 + 7$. The result is the partition of the set of input numbers into two equal sums $2 + 2 + 9 = 6 + 7$. In this case, there is only one partition.

Theorem 1 *The algorithm takes $O(k^2K + S)$ steps, where S is the number of solutions to the approximate equality* (4).

Proof. The three nested **for** loops in the first part of the algorithm clearly take $O(k^2K)$ steps. In the second part of the algorithm, the two **for** loops search through all solutions to the approximate equality (4).

Sometimes there are many solutions to (4). The number $3^{1155} + 1$ in (3) has an Aurifeuillian factorization given by (2) and there are many ways that primes can be swapped between the L and M factors to produce other approximate equalities. Thus, there are cases in which the algorithm runs for a long time because there are so many answers to the problem it solves. Perhaps one of the answers is an instance of a new algebraic factorization with infinitely many cases. This slowness cannot be avoided.

3. The Results

We searched the Cunningham tables of June 21, 2011, for new algebraic factorizations. When we used a percentage error of 1% or 0.1%, the program found too many approximate solutions to examine. Therefore, we processed the tables with

a percentage error of 0.01%. However, this choice gave too many solutions in the 2LM table, so we sharpened the percentage error to 0.001% for this table.

We did the computations for the primitive parts only, for the full factorization of $b^n \pm 1$, and for the L and M parts of Aurifeuillian factorizations separately. We also combined the sides of the Aurifeuillian factorizations and rediscovered them as a way of testing the program. It found all of them when n was large enough so that the difference $|\log L - \log M|$ was within the percentage error of $\log L$.

Isolated approximate splits are interesting curiosities, but our goal was to find new identities having infinitely many cases. Hence we searched for partitions of the factors of $b^n \pm 1$ with fixed α, b and $\pm$ with exponents n in an arithmetic progression or the start of another infinite series. We took special notice of identities in which the approximation was much better than the allowed percentage error. One clue that an approximate split is new was that the factors from an earlier referenced line were not all on the same side of the partition. When all prime factors from each earlier referenced line were on the same side of the partition, there was usually an algebraic explanation.

Here are the results for each base. Some numbers, like $3^{1155} + 1$ mentioned in (3), have many small factors that partition nicely in many ways for every α. We offer an explanation for this phenomena in Section 3.9.

3.1. Base 2

We tried $\alpha = 1/4$ and $1/2$. The base 2 tables are longer than those of other bases and contain many numbers with lots of factors. The numbers $2^{1155} \pm 1$ and $2^{2310} + 1$ each gave tens of thousands of solutions. The numbers $2^3 + 1 = 3 \cdot 3$ and 2,10L $= 2^5 - 2^3 + 1 = 5 \cdot 5$ each had a perfect partition.

Many numbers in the 2LM table split in non-Aurifeuillian ways into two factors nearly as close as their Aurifeuillian factorizations. As one example, consider $2^{534} + 1$. The number 2,534L contains factors from 2,2M (written 2,2+ in the Cunningham table) and 2,178M. The number 2,534M contains factors from 2,6M (written 2,6+ in the Cunningham table) and 2,178L. Each of 2,534L, 2,534M also has three primitive factors. However, the product of 2,178L and the three primitive factors of 2,534L is almost as close to the product of 2,2+, 2,6+, 2,178M and the three primitive factors of 2,534M as are the two factors of the Aurifeuillian factorization of $2^{534} + 1$. Similar examples exist for $2^n + 1$ with $n = 582$, 594, 618, 678, 702, 714, 726, etc.

3.2. Base 3

We tried $\alpha = 1/4$, $1/3$ and $1/2$. The primitive parts of $3^5 - 1$ and $3^1 + 1$ have perfect partitions of $11 \cdot 11$ and $2 \cdot 2$, respectively.

With $\alpha = 1/2$ there were good approximate splits for $3^n - 1$ for $n = 165$, 225, 315, 375, 405, 525, 555, 585 and 615. These numbers all have many prime factors and

the splits appeared to be coincidences even though these n are all $\equiv 15 \pmod{30}$. There are many ways to swap L and M factors between the Aurifeuillian factors of $3^{6k-3}+1$ to produce good approximate splits different from the Aurifeuillian factorizations.

3.3. Base 5

We tried $\alpha = 1/5$, $1/4$, $2/5$ and $1/2$. The number $5^{315}+1$, which has 27 prime factors, including three 3s and two 7s, had many approximate solutions.

The number $5^1 - 1 = 2 \cdot 2$ has a perfect partition for $\alpha = 1/2$.

With the value $\alpha = 1/2$, we found an interesting split of the number 5,575M into two nearly equal pieces. One piece included the 64-digit prime factor and the factors 1069501 and 26135496851. The other piece contained the other five prime factors, one of which comes from 5,25L.

Also with $\alpha = 1/2$, we found splits of $5^n - 1$ with each n in the arithmetic progression with first term 225 and common difference 30. All of these numbers have Aurifeuillian factorizations, but the factorizations we found were not Aurifeuillian. Many of these factorizations are just Aurifeuillian factorizations with a few factors swapped between the L and M sides. For example, 5,375L includes 5,125M and 5,375M includes 5,125L. If one swaps the factors from 5,125M and 5,125L between these two numbers, the new products are very close.

With $\alpha = 2/5$, we found good approximate splits of $5^n + 1$ for each n in the arithmetic progression with first term 105 and common difference 15. All were cyclotomic factorizations. One example is $(5^{120}-1)^{2/5} \approx 5^{48} \approx \Phi_{24}(5)\Phi_{40}(5)$.

3.4. Base 6

We tried $\alpha = 1/6$, $1/4$, $1/3$ and $1/2$. The number $6^{315}-1$, which has 28 prime factors, including two 5s, had many approximate solutions.

The value $\alpha = 1/3$ found the cyclotomic factorization $6^{3k}+1 = (6^k+1)(6^{2k}-6^k+1)$ for $3k = 36$, 48, 108, 192, 240, 288 and 336.

3.5. Base 7

We tried $\alpha = 1/7$, $2/7$, $3/7$, $1/2$ and $1/4$. The number $7^{330}+1$, which has 26 prime factors, including three 5s, had many approximate solutions.

Several striking approximate solutions had $\alpha = 2/7$. All were cyclotomic factorizations. Here are two examples:

$$(7^{105}-1)^{2/7} \approx 7^{30} \approx \Phi_7(7)\Phi_{35}(7)$$

and

$$(7^{147}-1)^{2/7} \approx 7^{42} \approx \Phi_{49}(7).$$

These occur because $\frac{2}{7} \cdot 105 = 30 = \phi(7) + \phi(35)$ and $\frac{2}{7} \cdot 147 = 42 = \phi(49)$. Other examples like these occur with $n = 189$, 231, 245, 273, 315, 357 and 385.

These examples lead me to the following question. Given a rational number α, which positive integers n have one or more distinct divisors d_i so that $\sum_i \phi(d_i) = \alpha n$? For $\alpha = 2/7$, there are solutions for $n = 105$ ($d_1 = 7$, $d_2 = 35$) and $n = 147$ ($d_1 = 49$). The program found no solutions for $\alpha = 1/7$ or $3/7$.

Similar examples were found for $\alpha = 2/7$ and $7^n + 1$ with $n = 126$, 168, 210, 252, 280, 294, 336, 350, 378 and 441.

3.6. Base 10

We tried $\alpha = 1/10$, $1/5$, $3/10$, $2/5$, $1/2$ and $1/4$. The number $10^{315} - 1$, which has 31 prime factors, counting four 3s, had many approximate solutions.

The number $10^1 - 1 = 3 \cdot 3$ has a perfect partition for $\alpha = 1/2$.

With $\alpha = 1/2$ there were many non-Aurifeuillian factorizations of $10^n + 1$ for $n = 330$, 390, 450, 510, 570, 630, 690 and 750. Note that these exponents form an arithmetic progression. Some of these factorizations are just Aurifeuillian factorizations with a few factors swapped between the L and M sides. For example, 10,750L includes 10,250L and 10,750M includes 10,250M. If one swaps the pieces from 10,250L and 10,250M between these two numbers, the new products are even closer than the Aurifeuillian factorizations.

With $\alpha = 0.4$, we found cyclotomic factorizations similar to those for $7^{105} - 1$. Here is an example:

$$(10^{75} - 1)^{0.4} \approx 10^{30} \approx \Phi_3(10)\Phi_{15}(10)\Phi_{25}(10).$$

There are other similar examples for $10^n - 1$ with n in the arithmetic progression 105, 135, 165, ... and for $10^n + 1$ with $n = 120$, 135, 180, 225, 300, 315 and 360. The other values of α that we tried did not give such examples in base 10.

3.7. Base 11

We tried $\alpha = 1/11$, $2/11$, $3/11$, $4/11$, $5/11$, $1/2$ and $1/4$. We found this interesting example with $\alpha = 1/4$ and only 18 prime factors. The product of the nine prime factors 73, 2521, 7321, 10657, 20113, 40177, 3262393, 77001139434480073 and 139032641114575020289 of $11^{252} + 1$ is approximately $405233 \cdot 10^{60}$ and $11^{252/4} = 11^{63} \approx 405265 \cdot 10^{60}$.

3.8. Base 12

We tried $\alpha = 1/12$, $1/6$, $1/4$, $1/3$, $5/12$ and $1/2$. The number $12^{231} - 1$ has 21 prime factors (counting two 11s). The product of the prime factors 157, 4621, 793717, 886381, 661269577, 191199728567, 50565974802015289 and P71 is very

close to the product of the other 13 prime factors. Furthermore, the product of the prime factors 11, 23, 4621, 5999137, 379101493, 191199728567, 8177824843189 and 50565974802015289 is very close to $12^{231/4}$ while the product of the other 13 prime factors is very close to $12^{3\cdot 231/4}$. The number $12^{255}-1$ also has 21 prime factors. The product of the prime factors 61, 661, 1021, 22621, 79561, 31144681, 5383015065849288291601 and 50540765443957214580241 is very close to $12^{255/4}$ while the product of the other 13 prime factors is very close to $12^{3\cdot 255/4}$. These are the only two examples of such a split in the 12− table.

There is one remarkable example in the 12+ table. The number $12^{369}+1$ has eleven primitive prime factors. The Aurifeuillian factorization of this number splits these factors into two groups whose products are near 12^{120}, since $\phi(369)/2 = 120$. However, the product of 1423355095922941, 105843637766088877609 and 37407215337032784045769872298 3, namely $56355\cdot 10^{60}$, is very close to $12^{60} = 56347\cdot 10^{60}$, while the product of the other eight factors is very close to 12^{180}. This is the only example of a good approximate split with $\alpha = 1/4$ in the 12+ table.

When the program was run with $\alpha = 1/3$, many cyclotomic factorizations, like $12^{48}+1 = (12^{16}+1)(12^{32}-12^{16}+1)$, were discovered. Here is an example of an approximate split with $\alpha = 1/3$ that was not cyclotomic. The number $N = (12^{183}+1)/(12^{61}+1)$ has 14 prime factors. The product of the factors 367, 1278439, 13154655247, 563215815517 and 22163333263957 is very close to $N^{1/3}$ while the product of the other nine factors is very close to $N^{2/3}$.

The other values of α (1/12, 1/6 and 5/12) produced no interesting results. The number $12^{525}+1$ has 28 prime factors, and they can be arranged to fit all of the αs we tried.

3.9. Are these results just coincidences?

Any real number $0 < \alpha < 1$ may be approximated within 2^{-k} by a sum of distinct powers of 2: 2^{-i} with $0 \le i < k$ using the binary representation of α. Likewise, if we are given k positive real numbers $a_1, \ldots, a_k$, with $a_i \le a_{i+1} \le 2a_i$ for $1 \le i < k$, then any positive real number less than their sum $c = \sum_{i=1}^{k} a_i$ may be approximated within a_1 by a sum of a_i with distinct i. Even when the inequalities are not satisfied for every $i < k$, many real numbers less than c can be approximated. When a_i and a_{i+1} are even closer together than $a_i \le a_{i+1} \le 2a_i$ for many i, there will be many approximations of some real numbers less than c.

When the real numbers a_i are the logarithms of the prime factors of a typical integer N, they might satisfy the inequality $a_i \le a_{i+1} \le 2a_i$ for several i. See Bach [1] for an algorithm to construct random factored integers N. For a typical random N, the a_i will roughly form a geometric progression. When N has many prime factors, the average common ratio will be smaller than 2, so that $a_i \le a_{i+1} \le 2a_i$ for many i. A more precise statement is given in Theorem 3 of Vershik [19], which says that the ratios $\log q/\log p$ of logarithms of consecutive large prime divisors $q < p$ of

large random integers are asymptotically independent and uniformly distributed in the unit interval $(0, 1)$. Of course, Cunningham numbers $b^n \pm 1$ are not random.

A typical random integer N has about $\ln \ln N$ prime factors. (See Hardy and Ramanujan [10].) Cunningham numbers have more than the typical number of prime factors due to the cyclotomic and Aurifeuillian factorizations. If a Cunningham number $N = b^n \pm 1$ has j prime factors, then it will be possible to find subsets of the set of prime factors whose product is within a factor of $1 + 2^{-j}$ of N^α for many $0 < \alpha < 1$.

Some Cunningham numbers have more than fifteen prime factors. For these numbers and for any $0 < \alpha < 1$, there are many partitions of the set of prime factors in which the product of the primes in one piece is within a factor of $1 + 2^{-15}$ of N^α. These partitions produced many splits within 0.01% that were coincidences.

4. Conclusion

This research has been a treasure hunt. As I read through the lists of approximate products, many times I thought I had found a new algebraic factorization. In all cases where there was any sort of regularity, as with exponents in an arithmetic progression, it always turned out that the approximate equality could be explained by known cyclotomic or Aurifeuillian factorization formulas. I believe now that Schinzel [15] really did find all algebraic factorizations of the Cunningham numbers and that Granville and Pleasants [8] adequately captured the notion of "such identities" and showed that there are no others.

The Cunningham Project has been in existence for more than a century. It now lists the factorizations of thousands of integers $b^n \pm 1$. It has spurred the development of many new factoring algorithms. Millions of hours of computer time have been devoted to the project. But there has been surprisingly little analysis of the results. The present paper is one of the few studies of the tables. In it we have "data-mined" the Cunningham tables for algebraic factorizations like those discovered by Aurifeuille and generalized by Schinzel. One might argue that this search was futile because Granville and Pleasants proved there are no more identities beyond those given by Schinzel. However, it is possible that their definition of "such identities" somehow missed some actual identities. In this paper, we searched for and found no new ones having infinitely many cases. We have made an empirical confirmation of the conclusions of Granville and Pleasants. We hope this paper inspires others to analyze the Cunningham tables in different ways and discover new truths.

All of the lists of approximate equalities are available on the web site
`http://homes.cerias.purdue.edu/~ssw/cun/aurifeuillian/index.html`
so that readers may learn more details of the approximate equalities reported above and make their own search for treasure.

The author is grateful to Mikhail Atallah for valuable discussions of the accelerated algorithm. He thanks Paul M. Kuliniewicz and Usman Latif for writing the program for the subset sum algorithm. He is indebted to the referee for clarifying several obscure points in the first draft of this paper.

References

[1] E. Bach. *Analytic Methods in the Analysis and Design of Number-Theoretic Algorithms*. The MIT Press, Cambridge, Massachusetts, 1985.

[2] R. P. Brent. On computing factors of cyclotomic polynomials. *Math. Comp.*, 61:131–149, 1993.

[3] R. P. Brent. Computing Aurifeuillian factors. In *Computational Algebra and Number Theory (Sydney, 1992)*, volume 325 of *Math. Appl.*, pages 201–212, Dordrecht, 1995. Kluwer Acad. Publ.

[4] John Brillhart, D. H. Lehmer, J. L. Selfridge, Bryant Tuckerman, and S. S. Wagstaff, Jr. *Factorizations of* $b^n \pm 1$, $b = 2, 3, 5, 6, 7, 10, 11, 12$ *up to high powers*. Amer. Math. Soc., Providence, Rhode Island, Third edition, 2002. Electronic book available at `http://www.ams.org/publications/ebooks`.

[5] M. Chamberland. Binary BBP-formulae for logarithms and generalized Gaussian-Mersenne primes. *J. Integer Seq.*, 6, 2003. Article 03.3.7, 10 pp. (electronic).

[6] T. H. Cormen, C. E. Leiserson, and R. L. Rivest. *Introduction to Algorithms*. MIT Press/McGraw-Hill, Cambridge, Massachusetts and New York, First edition, 1990; second edition, 2001.

[7] A. J. C. Cunningham and H. J. Woodall. *Factorisation of* $y^n \mp 1$, $y = 2, 3, 5, 6, 7, 10, 11, 12$ *Up to High Powers* (n). Francis Hodgson, London, 1925.

[8] A. Granville and P. Pleasants. Aurifeuillian factorization. *Math. Comp.*, 75:497–508, 2007.

[9] S. G. Hahn. A remark on Aurifeuillian factorizations. *Math. Japon.*, 39:501–502, 1994.

[10] G. H. Hardy and S. Ramanujan. The normal number of prime factors of a number n. *Quart. J. Math.*, 48:76–92, 1917.

[11] D. E. Knuth. *The Art of Computer Programming, Volume 2, Seminumerical Algorithms*. Addison-Wesley, Reading, Massachusetts, Second edition, 1981.

[12] É. Lucas. Théorèmes d'arithmétique. *Atti. Roy. Acad. Sci. Torino*, 13:271–284, 1878.

[13] C. Pomerance, J. L. Selfridge, and S. S. Wagstaff, Jr. The pseudoprimes to $25 \cdot 10^9$. *Math. Comp.*, 35:1003–1026, 1980.

[14] H. Riesel. *Prime Numbers and Computer Methods of Factorization*. Birkhäuser, Boston, Massachusetts, Second edition, 1994.

[15] A. Schinzel. On primitive prime factors of $a^n - b^n$. *Proc. Cambridge Philos. Soc.*, 58:555–562, 1962.

[16] P. Stevenhagen. On Aurifeuillian factorizations. *Indag. Math.*, 49:451–468, 1987.

[17] Q. Sun, D. Ren, S. Hong, P. Yuan, and Q. Hahn. A new class of Aurifeuillian factorizations of $M^n \pm 1$. *Sci. Math.*, 2:353–360, 1999.

[18] Q. Sun, P. Yuan, and Q. Hahn. A question about Aurifeuillian factorizations. *Chinese Sci. Bull.*, 40:1681–1683, 1995.

[19] A. M. Vershik. Asymptotic distribution of decompositions of natural numbers into prime divisors. *Dokl. Akad. Nauk SSSR*, 289:269–272, 1986. English translation: *Soviet Math. Dokl.* 34:57–61, 1986.

[20] S. S. Wagstaff, Jr. Aurifeuillian factorizations and the period of the Bell numbers modulo a prime. *Math. Comp.*, 65:383–391, 1996.