Fields Institute Communications
Volume **00**, 0000

# The Cunningham Project

**Samuel S. Wagstaff, Jr.**
Center for Education and Research in Information Assurance and Security
and Department of Computer Sciences, Purdue University
West Lafayette, IN 47907-1398 USA
ssw@cerias.purdue.edu

**Abstract.** The goal of the Cunningham Project is to factor numbers of the form $b^n \pm 1$ for small $b$. We explain why people factor these particular numbers, tell about those who have factored them, list some methods they used and describe some of their outstanding successes.

## 1 Introduction

The goal of the Cunningham Project is to factor numbers of the form $b^n \pm 1$ for integers $2 \le b \le 12$. The factors of these numbers are important ingredients in solving many problems in number theory. We will mention some of these problems in the next section.

Then we will tell the stories of some of the people who have factored these numbers over the past two centuries. Naturally, one of them was named Cunningham; we will say a great deal about him.

The fourth section explains some of the methods used to factor these numbers. In order to know whether a factorization is complete, we must be able to determine whether a large number is prime or composite. For a long time, primality testing was about as hard as factoring. However, in the past quarter century primality testing has become much easier than factoring. We will discuss the new advances as well as the older methods. Computers and other devices have aided the Cunningham Project immeasurably. We will mention some of their achievements and also tell how people factored before computers.

In the final section we will mention some of the greatest accomplishments the Cunningham Project has seen.

## 2 Why are these numbers interesting?

In elementary school, we learn how to convert fractions into repeating decimals. For example, $1/37 = 0.027027027027\ldots$. The length of the period of the decimal

2000 *Mathematics Subject Classification.* Primary 11Y05; Secondary 11A41, 11A51, 11Y11.
This work was supported in part by grants from the CERIAS Center at Purdue University and from the Lilly Endowment Inc.

fraction for $1/p$, where $p$ is a prime other than 2 or 5, is the smallest positive integer $n$ for which $p$ divides $10^n - 1$. The prime 37 divides 999 but not 99 or 9, so the period of the decimal fraction for $1/37$ is $n = 3$. The *primitive* prime factors of $10^n - 1$, that is, the ones which do not divide $10^i - 1$ for any $1 \le i < n$, are the primes $p$ for which the period of the decimal fraction $1/p$ is $n$. In 1801 Gauss (see Articles 308–318 of [12]) solved the general problem of determining the period of the decimal fraction for the rational number $a/b$.

Since the ancient Greeks, people have called numbers like 6 and 28, which equal the sum of their proper divisors, "perfect." Euclid knew that if $2^p - 1$ is prime, then $2^{p-1}(2^p - 1)$ is perfect. Thus, $2^{2-1}(2^2 - 1) = 6$ and $2^{3-1}(2^3 - 1) = 28$ are perfect. Euler proved that all even perfect numbers have this form. The study of perfect numbers led Mersenne to assert which numbers $2^p - 1$ are prime. The search for Mersenne primes $M_p = 2^p - 1$ continues today. For most of the past few hundred years, the largest known prime has been a Mersenne prime. We still don't know whether there are any odd perfect numbers. Many theorems restrict putative odd perfect numbers in some way. For example, Brent, Cohen and te Riele [5] showed that any odd perfect number must exceed $10^{300}$. Furthermore, such a number must have at least 29 prime factors, at least 8 of which are distinct, and one of which exceeds $1,000,000$. The proofs of these theorems have many cases and require knowledge of factors of numbers of the form $b^n \pm 1$. See Williams [46] for more about the history of perfect numbers and Mersenne primes.

Fermat thought that $F_m = 2^{2^m} + 1$ is prime for every non-negative integer $m$. The first five of these numbers, $F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$ and $F_4 = 65537$, are all prime. If Fermat tried to factor $F_5 = 4294967297$, either he didn't try many divisors or else he made a mistake. Euler showed that $F_5 = 641 \cdot 6700417$, proving Fermat wrong. Further study of the factorization of numbers $2^n + 1$ suggests that it is most unlikely that there is another prime in the sequence $\{F_m\}$ after $F_4$.

If $N$ is a large odd number and the factorization of $N - 1$ or $N + 1$ is known, then it is easy to decide whether $N$ is prime. One can use a theorem like this one due to Kraitchik [16] and D. H. Lehmer [18] when the factors of $N - 1$ are known.

**Theorem 2.1** *Let $N > 1$ and $a$ be integers such that $a^{N-1} \equiv 1 \pmod N$. If $a^{(N-1)/p} \not\equiv 1 \pmod N$ holds for every prime $p$ dividing $N - 1$, then $N$ is prime.*

The numbers $N = b^n \pm 1$, with small $b$, are ideal for primality testing via these theorems because we know the prime factors of $N \mp 1 = b^n$. For most $b$ and $n$ it is evident that $b^n \pm 1$ is composite because of an algebraic identity. For example, if $n = cd$ is composite, then $b^n - 1$ is divisible by both $b^c - 1$ and $b^d - 1$. It turns out that when $b \ge 2$ the numbers $b^n \pm 1$ can be prime only in the cases $2^p - 1$, with prime $p$, and $b^{2^m} + 1$. Otherwise, one can exhibit an algebraic factorization of $b^n \pm 1$. The former numbers are called Mersenne numbers and the latter are generalized Fermat numbers.

The factorization of the numbers $b^n \pm 1$ is determined partly by the factorization of the polynomial $x^n - 1$. If we let $\Phi_d(x)$ denote the $d$-th cyclotomic polynomial, then we have

$$x^n - 1 = \prod_{d|n} \Phi_d(x) \tag{2.1}$$

for $n \ge 1$. Although the cyclotomic polynomials are irreducible over the integers, formula (2.1), with $x = b$, does not give the complete factorization of $b^n - 1$ since any

factor $\Phi_d(b)$ might be composite. When $N = \Phi_d(b)$ is prime, one can often prove its primality via Theorem 2.1 because the constant term of $\Phi_d(x)$ is 1 for $d > 1$, and $N - 1$ is frequently divisible by a few powers of $b$. For example, let $b = 12$ and $d = 109$ (a prime). Then $\Phi_{109}(x) = (x^{109} - 1)/(x - 1)$ and $N = \Phi_{109}(12) = (12^{109} - 1)/11$ happens to be prime. The number $N - 1 = 12(12^{108} - 1)/11$ is easy to factor because $x^{108} - 1$ splits into many factors over the integers, so it is easy to apply Theorem 2.1. Hugh Williams found this proof in time for the 1983 first edition of [7]. We may factor $b^n + 1$ in a similar fashion using the identity

$$x^n + 1 = (x^{2n} - 1)/(x^n - 1) = \prod_{d|2n} \Phi_d(x) \Big/ \prod_{d|n} \Phi_d(x) = \prod_{d|m} \Phi_{2^t d}(x),$$

where $2n = 2^t m$ with $m$ odd.

Sometimes tables of factored integers can lead us to new algebraic identities. As a simple example, consider this table excerpted from a table of factorizations of numbers $2^n + 1$.

| $n$ | $2^n + 1$ | $2^n + 1$ factored | $2^n + 1$ factored again | $2^{n/2} + 1$ |
|---|---|---|---|---|
| 2 | 5 | 5 | $1 \cdot 5$ | 3 |
| 6 | 65 | $5 \cdot 13$ | $5 \cdot 13$ | 9 |
| 10 | 1025 | $5^2 \cdot 41$ | $25 \cdot 41$ | 33 |
| 14 | 16385 | $5 \cdot 29 \cdot 113$ | $113 \cdot 145$ | 129 |

It is easy to observe that the average of the two factors shown in the penultimate column equals the number in the last column. This leads to the identity

$$2^{4k-2} + 1 = (2^{2k-1} - 2^k + 1)(2^{2k-1} + 2^k + 1), \tag{2.2}$$

which is easy to prove once it is noticed. There is an identity like (2.2) for each $b$ that is not a power. It algebraically factors either $b^n - 1$ or $b^n + 1$, depending on $b$, for all $n$ in a certain arithmetic progression. The two factors are labeled "L" and "M" in [9] and [7]. These identities are named after Aurifeuille, who discovered some of them. (See page v of [9].) In terms of the binary representation of integers, Equation (2.2) shows that there exist integers with arbitrarily many 1 bits which can be multiplied times a number with exactly three 1 bits to give a product with exactly two 1 bits.

A polynomial $t(x)$ of degree $n > 1$ in $\mathbf{F}_2[x]$ is called *primitive* if it is irreducible and it does not divide $x^d + 1$ for any divisor $d$ of $2^n - 1$. See Golomb [15] for important applications of primitive polynomials in cryptography. The nondivisibility condition in the definition is not hard to check, even when $n$ is in the thousands, if one knows the complete prime factorization of $2^n - 1$.

The numbers $b^n \pm 1$ are among the most interesting large numbers and provide exciting test cases for new factoring algorithms.

## 3 The people who have factored the numbers

The Cunningham Project takes its name from the book [9] of Cunningham and Woodall.

Allan Joseph Champneys Cunningham was born in 1842 in Delhi [43] and educated at King's College, London and at the Military Seminary in Addiscombe. As a military engineer he saw action in Bhutan in 1865–66. The British annexation of Assam State in eastern India in 1826 heightened border tensions with Bhutan. The

situation simmered until 1863, when Sir Ashley Eden went to Bhutan to demand reparations for border raids into Assam. The government of Bhutan responded by holding him hostage until he signed a truce. Britain voided the truce upon Eden's release and attacked Bhutan. It was this battle in which Cunningham participated. He taught mathematics at the Thomason Civil Engineering College in Roorkee during 1871–1881. While there he conducted hydraulic experiments in the Ganges Canal. This college became the Department of Civil Engineering at the Indian Institute of Technology, Roorkee, in 1949, soon after India became independent. Today it is the oldest and largest civil engineering department in India. The Ganges Canal was built by the British in 1854 and used for irrigation. The water in the canal comes from behind the Haridwar dam on the Ganges in the foothills of the Himalayas near Roorkee. The canal must have been an interesting testbed for Cunningham's hydraulic experiments as it carries 7000 cubic feet of water per second, is ten feet deep, 170 feet wide and 900 miles long. The United States Army Corps of Engineers [30] studied the Ganges Canal and other large irrigation systems of the world as it planned irrigation canals in California in the 1870's. Cunningham returned to England in 1881. After he retired from the army as a Lieutenant-Colonel in 1891, he devoted the rest of his life to the theory of numbers. He was skilled as a computer and best known for his work on factoring numbers of the form $a^n \pm b^n$. He died in London in 1928.

The Cunningham-Woodall book [9] is a little book (xx + 24 pp.) that compiles the work of the authors and many others in factoring numbers of the form $y^n \pm 1$ for $2 \le y \le 12$. Actually, the others contributed mostly to the tables for bases $y = 2$ and $y = 10$. Factors for the other six bases are the authors' original work. The base 2 tables run up to the exponent $n = 500$, while the other tables extend to exponent $n = 100$. Most earlier tables listed all the prime factors of $y^n \pm 1$ for each $n$, resulting in much repetition of previously stated factors. The Cunningham-Woodall tables [9] was the first work to list essentially only the primitive factors. For each $n$ it listed just the factors of the "maximal algebraic primitive factor" (M. A. P. F.) of $y^n \pm 1$, that is, $\Phi_n(y)$ for $y^n - 1$ and odd $n$, and $\Phi_{2n}(y)$ for $y^n + 1$. The Introduction to [9] explains this economy and also presents a hard-to-understand explanation of the Aurifeuillian factorizations. If a prime $p$ divides $\Phi_n(y)$ and also $\Phi_d(y)$ for some proper divisor $d$ of $n$, then $p$ is called an *intrinsic* prime factor of $\Phi_n(y)$. An intrinsic prime factor $p$ of $\Phi_n(y)$ must divide $n$, and may divide $\Phi_n(y)$ only once if $n > 2$.

Most of the factors given in [9] were discovered by trial division. This effort by many people found all factors of $2^n \pm 1$ below $300,000$ and all factors below $100,000$ for higher bases. In 1925, it took much labor to discover whether a large odd number was prime or composite. Large prime cofactors were written in full in [9], composite cofactors were generally omitted and cofactors of undecided primality sometimes were listed and followed by a question mark. The blank spaces and question marks signaled unexplored territory. They and the credit given to the discoverers of notable prime factors inspired later researchers to try to complete the unfinished work.

Many researchers before Cunningham contributed to factoring $b^n \pm 1$. Marin Mersenne asserted which numbers $2^p - 1$ were prime. Fermat thought that the numbers $F_n$ were all prime. Euler showed that $F_5$ is composite because 641 divides it. Legendre [17] showed that every primitive prime divisor of $b^n \pm 1$ must have the form $2nx + 1$, which accelerates trial division by a factor of about $n$. In a

famous quotation, Gauss (in Article 329 of [12]) stated that the problem of factoring integers was important. He also introduced the congruence notation and produced some ideas for factoring integers. W. Looff [25] published a table of known factors of $10^n - 1$ for $1 \leq n \leq 60$. C. G. Reuschle [38] published a table of known factors of $b^n - 1$ for $b = 2, 3, 5, 7, 10$ and $n \leq 42$. Landry gave a simple proof that $2^{31} - 1$ is prime (Euler had done this with a tedious calculation) and factored $F_6$ in several months when he was 82 years old.

Lucas [26] supplied important ideas for deciding whether a large number is prime, including a special, fast test for Mersenne numbers $2^p - 1$. His tests used ideas which in modern terms would be described as properties of the finite fields $\mathbf{F}_p$ and $\mathbf{F}_{p^2}$. Pepin [31] developed a swift test for the primality of $F_n$ that is still used today. Proth [37] and Pocklington [32] invented new and faster tests for primality.

A few contemporaries of Cunningham also concerned themselves with factoring numbers. Maurice Kraitchik was born in Minsk in 1882 and lived in Belgium after obtaining a doctorate from the University of Liége in 1910. He wrote several books on number theory and was an expert in factoring and primality testing. He died in 1957. D. N. Lehmer was born in Indiana in 1867, earned a doctorate from the University of Chicago in 1900, and was a professor of mathematics at the University of California, Berkeley, from 1904 until he died in 1938. He published a table of prime numbers and a table of factors up to about $10^7$. He also created a set of stencils for factoring large numbers manually and wrote a review [20] of [9].

D. H. Lehmer (or Dick Lehmer), the son of D. N. Lehmer, was born in Berkeley in 1905 and obtained a Ph. D. at Brown University in 1930. While still an undergraduate student at Berkeley he sent new factors of $b^n \pm 1$ to Cunningham. He developed new factoring and primality testing methods and was a coauthor of [7]. Dick Lehmer died in 1991.

Dick Lehmer, whose wife Emma always helped him with his research, was joined by Selfridge and Brillhart and others in continuing the Cunningham Project through the 1950's, 1960's, 1970's and 1980's. In the 1960's, Tuckerman searched for factors below $10^8$ of $b^n \pm 1$ and also sought new Mersenne primes, finding $M_{19937}$. Morrison and Brillhart [28] developed the continued fraction factoring method, the first general factoring algorithm with a subexponential running time, in the early 1970's. Wagstaff joined this group in the late 1970's, checking the on-line Cunningham tables and then finding new factors of the numbers, first by trial division and then by many other methods. Their efforts resulted in the publication of updated Cunningham tables [7] as a book in 1983, 1988 and 2002. Yates published a book [50] about "repunits" which gave known factors of $10^n - 1$.

In the late 1970's, the invention of the RSA cryptosystem [39], whose security relies on the intractability of factoring large integers, made factoring suddenly fashionable, important and worthy of funding as a research area. Modern cryptography turned number theory into applied mathematics. As the Cunningham numbers are the most interesting sequence of numbers to factor, many people joined the factoring bandwagon in the 1980's. Davis, Holdridge and Simmons [10] of Sandia Labs implemented the quadratic sieve and factored all of the "Ten Most Wanted" numbers of the first edition of [7]. Bob Silverman wrote programs for the latest factoring algorithms, starting with the continued fraction factoring algorithm and methods invented by Pollard in the 1970's, and found many new Cunningham factors with them. Peter Montgomery implemented the same algorithms and found

faster ways to compute with large integers. He was the first to write a good program for H. W. Lenstra's [24] elliptic curve factoring method, ECM, invented in 1985. Suyama advanced ECM and factored many Cunningham numbers on a tiny personal computer (PC). Hugh Williams contributed new ideas for proving primality and supplied many prime proofs for the first edition of [7]. Mike Morrison and Brillhart [28] wrote the first continued fraction factoring program and Marvin Wunderlich automated it. Selfridge and Wunderlich wrote an automatic prime proving program based on the ideas of Brillhart, Lehmer and Selfridge [6].

Beginning in the middle 1980's the number of people helping the Cunningham Project exploded. I can only list the names of the most important contributors and hope I haven't missed anyone. In addition to those mentioned above, those who contributed something to the Cunningham Project include Guy, Robinson, Brent, te Riele, Kida, Pomerance, Gerver, Schnorr, A. K. Lenstra, Alford, Buell, Atkin, Morain, Cohen, Odlyzko, Adleman, Rumely, Keller, McCurdy, Niebuhr, Rickert, Smith, Gostin, Manasse, Lioen, Winter, Dixon, Granlund, Peralta, Leyland, Franke, Golliver, McCurley, Couveignes, Riesel, Bosma, van der Hulst, Shallit, Woltman, Seah, Crandall, Doenias, Norrie, Young, Mayer, Papadopoulos, Taura, McLaughlin, Elkenbracht-Huizing, Dilcher, Cavallar, Bernstein, Contini, Durman, Gallot, Kuwakado, Daminelli, Curry, Kleinjung, Lodin, Sassoon, Buhler, Harley, Kruppa, Muffett, Murphy, Ruby, Samidoost, Stevens, Wackerbarth, Wambach, Zimmermann and an anonymous factorer whose calls himself (or herself) "Marin Mersenne."

## 4 The methods used to factor the numbers

Most of the facts in this section come from [7] or [46]. We mention some of the algorithms and machines used to factor Cunningham numbers and also tell how to determine when a large number is prime.

**4.1 Prime testing.** When one factors large integers, one must be able to tell when one has finished. This requires the ability to recognize primes so that one does not try to factor them.

One naive way of proving $p$ prime is to show that it has no prime factor $\le \sqrt{p}$. This process may be accelerated if one can restrict the possible divisors, as explained in the next section. One advantage of this method is that it factors $p$ if $p$ turns out not to be prime.

Fermat's little theorem provides a simple test for compositeness. If $p$ is odd and for some $a$ not a multiple of $p$ we have $a^{p-1} \not\equiv 1 \pmod{p}$, then $p$ is composite. In applying this test to a divisor $p$ of $b^n \pm 1$ one must avoid choosing $a = b$ because usually $b^{p-1} \equiv 1 \pmod{p}$ whether $p$ is prime or composite. When this caution is observed, the test is quite reliable. In case $a^{p-1} \equiv 1 \pmod{p}$, and $a \ne b$, it is quite likely that $p$ is prime, but this statement has not been proved; $p$ is merely a *probable prime*. This test is quick because $a^{p-1} \bmod p$ may be computed by fast exponentiation.

Much effort has been placed in seeking ways to prove that a probable prime $p$ really is prime. Theorem 2.1 gives one answer but it requires factoring $p-1$. Much earlier Euler showed that if an integer $p$ can be written as the sum of two relatively prime squares in only one way, apart from sign changes and swapping the squares, then $p$ is a prime power. (It is easy to distinguish the first power of a prime from its higher powers.) Gauss generalized this approach to other binary quadratic forms.

Theorem 2.1 is one possible converse to Fermat's little theorem. Many other theorems that conclude, "then $p$ is prime," may be viewed as converses to Fermat's little theorem. They include the theorem of Pepin [31] that the Fermat number $F_n$ is prime if and only if $3^{(F_n-1)/2} \equiv -1 \pmod{F_n}$, the Lucas-Lehmer test for primality of the Mersenne number $M_p$, and many theorems that apply to general numbers. The latter were proved by Lucas [26], Proth [37], Pocklington [32], Brillhart, Lehmer, and Selfridge [6], and Morrison [29]. Some of these theorems allowed factors of $p+1$, in place of or in addition to factors of $p-1$, to contribute to the proof that $p$ is prime.

Note that $p-1$ and $p+1$ are the first two cyclotomic polynomials evaluated at $x = p$. Williams and his associates [48], [49], [47], [44] generalized the theorems mentioned above to some higher cyclotomic polynomials, proving that one can rigorously decide in polynomial time whether $p$ is prime, given a sufficiently large completely factored divisor of

$$(p-1)(p+1)(p^2+1)(p^2-p+1)(p^2+p+1).$$

Adleman, Pomerance and Rumely [1] invented a new prime proving method that generalizes Williams' results to even higher cyclotomic polynomials and correctly decides whether $p$ is prime in $< (\ln p)^{c \ln\ln\ln p}$ steps for some constant $c$. This nearly achieves the long-sought polynomial-time primality test since, although $\ln\ln\ln p \to \infty$ as $p \to \infty$, it has never been observed doing so. Cohen and Lenstra [23], [8] and Mihăilescu [27] improved this algorithm, making it faster and more practical. Odlyzko used this method to prove primality of many large primes from the second edition of [7].

Goldwasser and Killian [14] invented an elliptic curve analogue of a primality testing theorem of Pocklington [32] and Lehmer. It runs in probabilistic polynomial time. Atkin and Morain [3] turned it into a practical algorithm that works well for numbers up to a thousand decimal digits or more. It was used for the difficult prime proofs of the third edition of [7]. In August, 2002, Manindra Agrawal, Neeraj Kayal and Nitin Saxena announced a deterministic polynomial-time primality testing algorithm. It uses fairly simple mathematics but has not been used to prove primality of any Cunningham number.

**4.2 Factoring.** The earliest and simplest method of factoring an integer $N$ was trial division. Each number, usually a prime, in a sequence is divided into $N$ to see if it divides exactly. Sometimes many trial divisors can be ignored because one can prove they cannot divide $N$. Gauss observed that if $r$ is a quadratic residue modulo $N$, then it must be a quadratic residue modulo every prime factor $p$ of $N$ and so the Law of Quadratic Reciprocity restricts $p$ to lie in only one-half of the possible residue classes modulo $4r$. If one knows $t$ (independent) quadratic residues modulo $N$, then only one out of $2^t$ residue classes is allowed for $p$. (A set of quadratic residues is independent if no non-empty subset of them has a square product.) In addition to these restrictions, if one is trying to factor $b^n \pm 1$, then one can use a valuable theorem of Legendre: Every prime factor of the primitive part of $b^n \pm 1$ is $\equiv 1 \pmod{2n}$. Thus, only about one out of every $n$ possible divisors of $N$ need be tried.

Fermat invented a difference-of-squares factoring algorithm in which one tries to express $N$ as $x^2 - y^2$. The algorithm works well when $N$ has a divisor very near

$\sqrt{N}$, but runs slowly otherwise. Mersenne may have used this method to find that 233 divides $2^{29}-1$. (See page 37 of [46].)

Pollard invented two factoring methods in the 1970's that discovered many Cunningham factors. His rho or Monte Carlo method [34] discovers a prime factor $p$ of a larger number $N$ in about $O(\sqrt{p})$ arithmetic operations modulo $N$. His $p-1$ method [33] finds a prime factor $p$ provided $p-1$ has only small prime factors. Note that if $p$ is a primitive divisor of $b^n \pm 1$, then $2n$ divides $p-1$ by Legendre's theorem. This factor makes the $p-1$ method well-suited for application to Cunningham numbers. Williams [45] created a $p+1$ analogue that finds $p$ if $p+1$ has only small prime factors. Later H. W. Lenstra, Jr. [24] invented an elliptic curve analogue of Pollard's $p-1$ method. These four methods have found hundreds of Cunningham factors in the past 25 years.

The fastest known factoring methods today combine congruences modulo $N$ to construct a congruence $x^2 \equiv y^2 \pmod{N}$, which will factor $N$ provided that $x \not\equiv \pm y \pmod{N}$, a condition that holds at least half of the time. The earliest use of congruences to factor $N$ goes back to Legendre [17], who used them to find quadratic residues modulo $N$ and accelerate trial division. The first use of congruences to construct a congruence $x^2 \equiv y^2 \pmod{N}$, and factor $N$ directly, seems to have been done by Kraitchik [16], who obtained congruences by *ad hoc* means and factored some Cunningham numbers. Fifty years later, Morrison and Brillhart [28] used the continued fraction expansion for $\sqrt{N}$ to generate many congruences $x^2 \equiv q \pmod{N}$ with small $|q|$. They matched up the prime factors of $|q|$ to construct $x^2 \equiv y^2 \pmod{N}$. They called this algorithm the continued fraction factoring algorithm and factored many Cunningham numbers, beginning with $F_7$. Pomerance [35] discussed the quadratic sieve algorithm which replaces the slow trial division of the continued fraction factoring algorithm with a fast sieve to factor quadratic residues. Gerver [13], Davis and Holdridge [10], Silverman [41], Montgomery, Lenstra [22] and others implemented versions of this algorithm and factored many Cunningham numbers. Pollard created the cubic sieve which reduces the size of the numbers that need to be factored in the quadratic sieve. He refactored $F_7$ on a small computer to test his new method. He, the Lenstra brothers and Pomerance [21] extended this method to higher degree polynomials (and even smaller numbers to factor) and invented the number field sieve, NFS, the current fastest known factoring method. Curiously, this method favors Cunningham numbers. The first task of the NFS is to find a polynomial with certain properties. When the number to factor has the form $b^n \pm 1$ it is trivial to find an excellent polynomial for the NFS. It requires much more work to find a good polynomial for numbers not of these forms.

**4.3 Devices.** The earliest factorizations of $b^n \pm 1$ were done by hand. This is how Euler factored the 10-digit $F_5$, Landry factored the 19-digit $F_6$ and Cole factored the 21-digit $M_{67}$. The first devices to aid computation were mechanical calculators. These were used by Cunningham, Kraitchik, the Lehmers and many others. About 100 years ago, paper strips and stencils were used in sieving. Over the years, Dick Lehmer built sieve devices of bicycle chains, gears, electronic delay lines and shift registers and used all of them to factor $b^n \pm 1$. See [19] for a description of one of them.

Nearly every type of electronic computer has been used for the Cunningham Project. Dick Lehmer used one of the earliest ones, the ENIAC (Electronic Numerical Integrator and Computer), to find 85 new factors of $2^n \pm 1$ for $n \le 500$

"during a holiday weekend" in 1949. Emma Lehmer and John Selfridge factored Fermat numbers and other numbers on the SWAC ([National Bureau of] Standards Western Automatic Computer) at UCLA in the early 1950's. Raphael Robinson [40] programmed the Lucas-Lehmer primality test for $M_p$ on the SWAC and immediately found the Mersenne primes with $p = 521$, 607, 1279, 2203 and 2281. Much factoring of $b^n \pm 1$ was done on the IBM 701, 704, 709, 7090, 7094, 1130, 4341, 360 and 370 computers by many researchers. Wagstaff used a DEC 10/KI to perform trial division to $2^{35}$ on the tables of [7]. Baillie found many new factors with Pollard's $p-1$ method on a CDC 6500. Hiromi Suyama found many factors on an 8-bit microcomputer. H. Williams factored some hard numbers on an Amdahl 470 and completed many prime proofs on that machine.

Many supercomputers contributed to the Cunningham Project. Dick Lehmer factored many numbers on the Illiac IV supercomputer. Davis and Holdridge [10] used a Cray-1 and Cray X-MP to factor all of the "Ten Most Wanted" numbers from the first edition of [7]. McCurdy and Wunderlich factored $5^{171}+1$ via the continued fraction algorithm on an MPP (Massively Parallel Processor). H. te Riele et al. factored $(7^{104}+1)/(7^8+1)$ on a Cyber 205. Later they factored more Cunningham numbers with the quadratic sieve on a NEC SX-2 and on a Cray Y-MP4. Using a MasPar computer, A. K. Lenstra factored many Cunningham numbers with programs for the quadratic sieve, the number field sieve and his brother's elliptic curve method. Young and Buell used a Cray-2 to show that $F_{20}$ is composite.

Several special computing devices other than Lehmer's sieves were used to factor Cunningham numbers. Smith and Wagstaff [42] fabricated the EPOC (Extended Precision Operand Computer), with a 128-bit word length and a bank of parallel remaindering units, at the University of Georgia and used it to factor $3^{204}+1$ with the continued fraction algorithm. Dubner and Dubner [11] fabricated a special card, which plugs in to a PC, for rapidly performing arithmetic with large integers. They ran Pollard's rho method and the elliptic curve method on it and found many new factors. This machine also contributed to the primality proof of the "repunit" $(10^{1031}-1)/9$.

In the past fifteen years, networks of small computers have cooperated to achieve results that previously could only be done on supercomputers. At first, local area networks were used. For example, Alford and Pomerance [2] ran the quadratic sieve, a highly parallelizable algorithm, on several hundred PC's in a student laboratory at the University of Georgia. Y. Kida had similar success using many small computers in Japan, as did G. Sassoon with all the PC's on the Isle of Mull in Scotland. Silverman [41] ran the quadratic sieve on many SUN workstations at the MITRE Corporation and contributed many important factorizations to the Cunningham Project. More recently, large groups of computers of various types around the world have cooperated to achieve astounding factorizations. Groups of researchers with names like ECMNET and NFSNET have set record after record factoring harder and harder Cunningham numbers.

## 5 Records, Champions and Accomplishments

Here we mention some of the great advances that have promoted the Cunningham Project.

First of all, the invention of the electronic digital computer has removed most of the tedium and inaccuracy of hand calculation. It has relieved humans of some of the disappointment of failure to factor a number after many hours of hard work.

Rigorously deciding primality has made the greatest advance in algorithms. In Cunningham's time, the primality of many twenty-digit numbers could not be decided. Until about 25 years ago, deciding the primality of $N$ often was as difficult as factoring a hard composite number about the same size as $N$. Now we can decide whether a thousand-digit number is probably prime in a few seconds, and give a rigorous proof in an hour if it is prime. The primality of a thirty-digit integer can be decided rigorously in less than a second.

Even the quick probable prime test of $N$ has improved beyond simply checking whether $a^{N-1} \equiv 1 \pmod{N}$. The combination of a strong probable prime test and a Lucas probable prime test proposed by Baillie, Pomerance, Selfridge and Wagstaff [4], [36] has no known failure. Its first extensive use was in checking all the probable primes in the first and second editions of [7]. The test is considered so reliable that the American National Standards Institute has just adopted it as ANSI Standard X9-80, the official recommended method for choosing "industrial-grade primes" to use in cryptography.

There have been great advances in factoring methods, too, but we still don't know a polynomial-time algorithm for this problem. It was not until the 1988 second edition of [7] that all numbers considered in [9] were factored. We do not yet know methods that will factor all numbers listed in even the first edition of [7]. We don't know an algorithm that can complete the factorization of $F_{12}$, the smallest unfinished Fermat number (unless it has at most one large prime factor).

At this writing, all of the following most wanted numbers of the third edition of [7], published just a year ago, have been factored. The notation "$2,673-$ C151" means "the 151-digit composite divisor of $2^{673} - 1$."

Ten "Most Wanted" Factorizations of [7].

| | | | | | |
|---|---|---|---|---|---|
| 1. | $2,673-$ | C151 | 6. | $6,257-$ | C173 |
| 2. | $2,647+$ | C169 | 7. | $5,289+$ | C156 |
| 3. | $3,397-$ | C178 | 8. | $5,298+$ | C189 |
| 4. | $3,397+$ | C162 | 9. | $12,178+$ | C145 |
| 5. | $10,223-$ | C211 | 10. | $11,197+$ | C205 |

If Cunningham had made a similar list for [9], it would probably look like this:

Ten "Most Wanted" Factorizations of [9].

| | | | | | |
|---|---|---|---|---|---|
| 1. | $2,79-$ | C21 | 6. | $5,22+$ | C13 |
| 2. | $2,83-$ | C23 | 7. | $6,17+$ | C13 |
| 3. | $2,67+$ | C21 | 8. | $10,20+$ | C16 |
| 4. | $3,28+$ | C12 | 9. | $11,16+$ | C12 |
| 5. | $10,23-$ | C23 | 10. | $12,11+$ | C11 |

Since Cunningham had not actually tested the remaining cofactors for primality, the notation "C21" here means merely, "a 21-digit integer of questionable character." In fact the "C23" of $2,83-$, the "C23" of $10,23-$, the "C13" of $5,22+$ and the "C11" of $12,11+$ all turned out to be prime. The other six numbers really are composite.

The largest Fermat number known to be composite today is $F_{2145351}$, since John Cosgrove discovered the divisor $3 \cdot 2^{2145353} + 1$ on February 21, 2003. This factor is one of the largest known primes. The largest known prime today is the Mersenne prime $M_{13466917}$ discovered by the Great Internet Mersenne Prime Search, GIMPS, on November 14, 2001. Lew Baxter recently discovered that the repunit $(10^{86453}-1)/9$ is a probable prime. Earlier, Dubner found that $(10^{49081}-1)/9$ is also a probable prime. The largest repunit whose primality proof has been completed is $(10^{1031} - 1)/9$, proved by Williams and Dubner (see Section 12.4 of [46]).

## References


[1] L. M. Adleman, C. Pomerance, and R. S. Rumely. On distinguishing prime numbers from composite numbers. *Ann. of Math.*, 117:173–206, 1983.

[2] W. R. Alford and C. Pomerance. Implementing the self-initializing quadratic sieve on a distributed network. In A. van der Poorten, I. Shparlinski, and H. G. Zimmer, editors, *Number Theoretic and Algebraic Methods in Computer Science*, pages 163–174, Moscow, 1993.

[3] A. O. L. Atkin and F. Morain. Elliptic curves and primality proving. *Math. Comp.*, 61:29–68, 1993.

[4] R. Baillie and S. S. Wagstaff, Jr. Lucas pseudoprimes. *Math. Comp.*, 35:1391–1417, 1980.

[5] R. P. Brent, G. L. Cohen, and H. J. J. te Riele. Improved techniques for lower bounds for odd perfect numbers. *Math. Comp.*, 57:857–868, 1991.

[6] J. Brillhart, D. H. Lehmer, and J. L. Selfridge. New primality criteria and factorizations of $2^m \pm 1$. *Math. Comp.*, 29:620–647, 1975.

[7] 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, First edition, 1983, Second edition, 1988, Third edition, 2002. Electronic book available at `http://www.ams.org/online_bks/conm22`.

[8] H. Cohen and H. W. Lenstra, Jr. Primality testing and Jacobi sums. *Math. Comp.*, 42:297–330, 1984.

[9] 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.

[10] J. A. Davis and D. B. Holdridge. Factorization using the quadratic sieve algorithm. In D. Chaum, editor, *Advances in Cryptology—CRYPTO '83*, pages 103–113, Plenum Press, New York, 1984.

[11] H. Dubner and R. Dubner. The development of a powerful, low-cost computer for number theory applications. *J. Rec. Math.*, 18:81–86, 1986.

[12] C. F. Gauss. *Disquisitiones Arithmeticae*. Yale University Press, New Haven, English edition, 1966.

[13] J. L. Gerver. Factoring large numbers with a quadratic sieve. *Math. Comp.*, 41:287–294, 1983.

[14] S. Goldwasser and J. Kilian. Almost all primes can be quickly certified. In *Proc. Eighteenth Annual ACM Symp. on the Theory of Computing (STOC), Berkeley, May 28-30, 1986*, pages 316–329. ACM, 1986.

[15] S. W. Golomb. *Shift Register Sequences*. Holden-Day, San Francisco, California, 1967.

[16] M. Kraitchik. *Théorie des nombres, Tome II*. Gauthiers-Villars, Paris, France, 1926.

[17] A. M. Legendre. *Théorie des nombres, Tome I*. Gauthiers-Villars, Paris, France, 1830.

[18] D. H. Lehmer. Tests for primality by the converse of Fermat's theorem. *Bull. Amer. Math. Soc.*, 33:327–340, 1927.

[19] D. H. Lehmer. A photo-electric number sieve. *Amer. Math. Monthly*, 40:401–406, 1933.

[20] D. N. Lehmer. Review of [9]. *Bull. Amer. Math. Soc.*, 32:720, 1926.

[21] A. K. Lenstra and H. W. Lenstra, Jr. *The Development of the Number Field Sieve*. Springer-Verlag, New York, 1993.

[22] A. K. Lenstra and M. S. Manasse. Factoring with two large primes. *Math. Comp.*, 63:785–798, 1994.

[23] H. W. Lenstra, Jr. Primality testing algorithms (after Adleman, Rumley and Williams). In *Seminar Bourbaki 33 (1980/81), Lecture Notes in Mathematics*, volume 901, pages 243–258, Springer-Verlag, Berlin, 1981.

[24] H. W. Lenstra, Jr. Factoring integers with elliptic curves. *Ann. of Math.*, 126:649–673, 1987.

[25] W. Looff. Über die Periodicität der Decimalbrüche. *Archiv der mathematik und Physik.*, 16:54–57, 1851.
[26] E. Lucas. *Théorie des nombres, Tome I.* Librarie Blanchard, Paris, France, 1961.
[27] P. Mihăilescu. Cyclotomy primality proving—recent developments. In *Algorithmic Number Theory (Portland, OR, 1998), Lecture Notes in Computer Science*, volume 1423, pages 99–110, Springer-Verlag, Berlin, 1981.
[28] M. A. Morrison and J. Brillhart. A method of factoring and the factorization of $F_7$. *Math. Comp.*, 29:183–205, 1975.
[29] Michael A. Morrison. A note on primality testing using Lucas sequences. *Math. Comp.*, 29:181–182, 1975.
[30] U. S. Army Corps of Engineers. Engineers and Irrigation: Report of the Board of Commissioners on the Irrigation of the San Joaquin, Tulare, and the Sacramento Valleys of the State of California. Publication number EP 870-1-39, 1873. Also see the URL: `http://www.usace.army.mil/inet/usace-docs/eng-pamphlets/ep870-1-39` .
[31] P. Pepin. Sur la formule $2^{2^n} + 1$. *C. R. Acad. Sci. Paris*, 85:329–331, 1877.
[32] H. C. Pocklington. The determination of the prime or composite nature of large numbers. *Proc. Cambridge Philos. Soc.*, 18:29–30, 1914–16.
[33] J. M. Pollard. Theorems on factorization and primality testing. *Proc. Cambridge Philos. Soc.*, 76:521–528, 1974.
[34] J. M. Pollard. A Monte Carlo method for factorization. *Nordisk Tidskr. Informationsbehandling (BIT)*, 15:331–335, 1975.
[35] C. Pomerance. Analysis and comparison of some integer factoring algorithms. In H. W. Lenstra, Jr. and R. Tijdeman, editors, *Computational Methods in Number Theory, Part 1*, volume 154 of *Math. Centrum Tract*, pages 89–139, CWI, Amsterdam, 1982.
[36] C. Pomerance, J. L. Selfridge, and S. S. Wagstaff, Jr. The pseudoprimes to $25 \cdot 10^9$. *Math. Comp.*, 35:1003–1026, 1980.
[37] E. Proth. Théorèmes sur les nombres premiers. *C. R. Acad. Sci. Paris*, 87:926, 1878.
[38] K. G. Reuschle. *Mathematische Abhandlung, enthaltend: Neue zahlentheoretische Tabellen.* Königl. Gymnasium Stuttgart, 1856.
[39] R. L. Rivest, A. Shamir, and L. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Comm. A. C. M.*, 21(2):120–126, 1978.
[40] Raphael M. Robinson. Mersenne and Fermat numbers. *Proc. Amer. Math. Soc.*, 5:842–846, 1954.
[41] R. D. Silverman. The multiple polynomial quadratic sieve. *Math. Comp.*, 48:329–339, 1987.
[42] J. W. Smith and S. S. Wagstaff, Jr. An extended precision operand computer. In *Proc. of the Twenty-First Southeast Region ACM Conference*, pages 209–216, ACM, 1983.
[43] A. E. Western. Allan Joseph Cunningham. *J. London Math. Soc.*, 3:317–318, 1928.
[44] H. C. Williams. Primality testing on a computer. *Ars Combinatoria*, 32:127–185, 1978.
[45] H. C. Williams. A $p + 1$ method of factoring. *Math. Comp.*, 39:225–234, 1982.
[46] H. C. Williams. *Édouard Lucas and Primality Testing*, volume 22 of *Canadian Mathematics Society Series of Monographs and Advanced Texts*. John Wiley & Sons, New York, 1998.
[47] H. C. Williams and R. Holte. Some observations on primality testing. *Math. Comp.*, 32:905–917, 1978.
[48] H. C. Williams and J. S. Judd. Determination of the primality of $N$ using factors of $N^2 \pm 1$. *Math. Comp.*, 30:157–172, 1976.
[49] H. C. Williams and J. S. Judd. Some algorithms for primality testing using generalized Lehmer functions. *Math. Comp.*, 30:867–886, 1976.
[50] Samuel Yates. *Repunits and Repetends*. Samuel Yates, Delray Beach, Florida, 1982.