MATHEMATICS OF COMPUTATION
VOLUME 64, NUMBER 210
APRIL 1995, PAGES 863–868

THE TWENTY-SECOND FERMAT NUMBER IS COMPOSITE

R. CRANDALL, J. DOENIAS, C. NORRIE, AND J. YOUNG

ABSTRACT. We have shown by machine proof that $F_{22} = 2^{2^{22}} + 1$ is composite. In addition, we reenacted Young and Buell's 1988 resolution of F_{20} as composite, finding agreement with their final Selfridge-Hurwitz residues. We also resolved the character of all extant cofactors of F_n, $n \leq 22$, finding no new primes, and ruling out prime powers.

1. METHOD OF PROOF

The character of $F_n = 2^{2^n} + 1$ for $n \geq 1$ may be resolved by way of the Pepin test. One form of this test states that for $m \geq 2$, if $p = 2^m + 1$ is a quadratic nonresidue modulo an odd prime q, then p is prime if and only if

$$q^{(p-1)/2} \equiv -1 \pmod{p}.$$

We may compute and report, then, the residue R_n defined as a least nonnegative value,

$$R_n = 3^{(F_n-1)/2} \pmod{F_n},$$

to declare F_n prime or composite as R_n is or is not $(F_n - 1) \pmod{F_n}$, respectively. The procedure of evaluating R_n has been used in previous years to prove various F_n composite. In fact, F_7, F_8, F_{10}, F_{13}, F_{14}, and F_{20} have been shown composite in this way [6, 8]. Note that many F_n can be shown composite with relative ease, by the simple expedient of exhibiting a small, explicit factor. Selfridge and Hurwitz [6] started a practice of reporting, in their case for F_7, F_8, F_{13}, and F_{14}, the three numbers

$$R_n \; (\mathrm{mod}\; 2^{35} - 1,\, 2^{36},\, 2^{36} - 1).$$

This three-modulus report is akin to a "parity check" or checksum, in that two independent random large integers have a probability of about $2^{-(35+36+36)}$ of simultaneous agreement in all three moduli. The reporting of the three moduli is not, of course, a complete record of the Pepin residue; but such a report is convenient for two reasons. First, the three moduli are small and easy to shuttle between testing sites. Second, for $n > 5$, the simple fact of a nonvanishing second Selfridge-Hurwitz residue indicates that F_n is composite.

2. LARGE-INTEGER ARITHMETIC

The primary run for F_{22} was carried out on an Amdahl 5995M model 4550 mainframe, with squaring (the central operation in the Pepin test) performed

Received by the editor November 23, 1993 and, in revised form, February 15, 1994.
1991 *Mathematics Subject Classification*. Primary 11Y11, 11A51.

via the discrete weighted transform (DWT) algorithm [2]. The DWT is essentially an FFT, but with signal elements weighted on foreknowledge that reduction modulo F_n will be performed. We chose a digit size $W = 2^{16}$, so that $F_{22} = W^{2^{18}} + 1$. In this representation a typical residue has $256K$ digits. Whereas the traditional "zero-padding" for (acyclic) FFT multiplication would involve a run length of $N = 2^{19}$, the DWT approach requires only run length $N/4$ to perform the necessary negacyclic convolution, i.e., to obtain a square (mod F_{22}). A (cyclic convolution) version of the DWT, appropriate in cases where reduction modulo $2^q - 1$ is to be performed after squaring, has also been used in recent Lucas-Lehmer verifications of new Mersenne primes, notably $2^{756839} - 1$ and $2^{859433} - 1$, those test cases having been communicated to us by D. Slowinski [7]. To convey an idea of scale for the Fermat numbers in question, we observe that even the cofactor of F_{21} is larger than the square of the latter, largest known Mersenne prime. It is perhaps also of interest that DWT methods were used for the elliptic-curve arithmetic that uncovered (via elliptic-curve (ECM) factorization) the two newest factors of F_{13} shown in Table 2 [1, 2]. Many machines perform the FFT or DWT fastest when floating-point arithmetic is used. In order to control floating-point transform errors, we invoked a balanced-digit representation. Instead of digits conventionally in $[0, W-1]$, we adopted digits in $[-W/2, W/2-1]$. It is known empirically that such balanced representations reduce DWT convolution errors considerably [2].

3. Main result

There is always the question: How do we know our Pepin squares are correct? One of the authors [CN] performed a novel, parallel determinism-checking task. In this scheme, the mainframe (thought of as a "wavefront") performed Pepin squares, depositing residues for, say, the ath square and the bth square. These square "endpoints" were stored for various pairs (a, b) and the difference $b - a$ relatively small, say, $b - a \sim 1000$. Then many workstations, even given a unique ath square, would perform $b - a$ squarings, expecting to find the mainframe's reported bth square. The workstations used software programs different from the mainframe program. In addition, various deterministic points were checked by another author [JY] on Cray machinery. In the Cray runs, the hardware was obviously different, but the software was likewise different and so amounted to a third distinct implementation.

The result is that R_{22} is not $(F_{22}-1) \pmod{F_{22}}$, so F_{22} is indeed composite. Our Selfridge-Hurwitz moduli are reported below for reference by future investigators. The "wavefront" run took more than seven months, with the parallel determinism check always running close behind. We estimate the total number of arithmetic operations (on machine words) be in excess of 10^{16}. At various times during the long F_{22} run, we worked (with separate machinery) on other F_n in order to complete some heretofore missing entries in existing tables. We hereby report, as Table 1, all of the Selfridge-Hurwitz residues, in decimal, for $5 \le n \le 22$. A glance at R_{22} indicates that F_{22} is indeed composite; in fact the table amounts to a report that all F_n in the stated range are composite. The entries for R_{20} are in complete agreement with the report of [8] (although note that their three moduli were displayed in *octal* representation).

TABLE 1. Selfridge-Hurwitz residues (in decimal) for composite numbers F_5 through F_{22}. R_n is the Pepin residue $3^{(F_n-1)/2}$ (mod F_n). For $n > 5$, primality of F_n would necessitate the value zero in the (mod 2^{36}) column

n	R_n (mod $2^{35}-1$)	R_n (mod 2^{36})	R_n (mod $2^{36}-1$)
5	10324303	10324303	10324303
6	9190530327	8845352501	9017941414
7	5799525263	3909272836	44591026080
8	30627284506	46310188723	35403253324
9	28173182079	19661770102	54966870189
10	28022031617	36399120536	54182679152
11	3934743084	66666487080	44928212591
12	300454051	64546579219	3387502849
13	3434508623	52529728350	52864871946
14	15173315214	54038984522	1986493987
15	14110954287	7124011679	42435904961
16	173595305	24695037109	65390296136
17	14982977589	14726733277	2770550506
18	10874364700	46106404592	14070013587
19	6407009455	22254317980	58676148574
20	15265819636	16865158641	35626292569
21	30981963597	22442941248	300257643
22	12323430823	973723434	8733349067

4. Primality tests for the cofactors

A convenient primality test for Fermat cofactors is due to Suyama [3]. Let

$$F_n = fG,$$

where f is, say, a known small factor (not necessarily prime) and the character of G is in question. If G is prime, then it must happen that $3^G = 3 \pmod G$. This in turn can be cast as

$$R_n^2 \equiv 3^{f-1} \pmod G.$$

The beauty of the Suyama test is that it can be run on the R_n that has already been computed as the final Pepin residue. If this last congruence fails, G is composite. Note also that the power $f-1$ tends to be relatively small, so just a handful of squarings and multiplications are required to resolve currently extant cofactors (once R_n is in hand). Incidentally, for the larger Fermat numbers in our stated range, it is more efficient to compute first R_n^2 and 3^{f-1} (mod F_n), then to effect a final reduction modulo G_n. The reason is that arithmetic modulo a Fermat number can be carried out with shifts and adds/subtracts alone. For $n \leq 22$, we resolved the two open cases; namely:

$$F_{19} = f_{19} * G_{19} = 4561072932012449292289 * G_{19}$$
$$F_{21} = f_{21} * G_{21} = 4485296422913 * G_{21}$$

finding both G cofactors composite. For possible use by future investigators, we report the Suyama residues:

$$(R_{19}^2 \ (\text{mod} G_{19}))\ (\text{mod } 2^{16}) = 51945,$$
$$(3^{f_{19}-1}\ (\text{mod } G_{19}))\ (\text{mod } 2^{16}) = 14357,$$
$$(R_{21}^2 \ (\text{mod} G_{21}))\ (\text{mod } 2^{16}) = 41530,$$
$$(3^{f_{21}-1}\ (\text{mod } G_{21}))\ (\text{mod } 2^{16}) = 40393,$$

where every modulus is given its least nonnegative value.

5. Prime powers

It was recommended to us by H. W. Lenstra Jr. that, for the convenience of future investigators, we also verify (the practical expectation) that none of the proven composites is a prime power. First, we know F_n cannot itself be a prime power p^k, $k > 1$, because the Diophantine equation $p^k - 4^m = 1$ for $k > 1$ has no solutions. This is easy to see: If a solution exists and k is even, we have two positive squares that differ by 1, so k must be odd. But then $p^k - 1$ has the odd algebraic factor $1 + p + \cdots + p^{k-1}$, which cannot divide 4^m. This takes care of F_{22}, which therefore is neither p nor p^k. As for the cofactors G_{19}, G_{21}, there are at least two equivalent ways to show neither can be a prime power. One is to adopt the test used by the factorers of F_9 [4], which is to test

$$GCD(a^G - a, G)$$

for an a such that G does not divide $a^G - a$. If this $GCD = 1$, G cannot be a prime power. Luckily, we already had all the basic terms in hand for this test. In fact, the GCD can be turned immediately into

$$GCD((3^f)^G - 3^f, G) = GCD(3R^2 - 3^f, G) = GCD(R^2 - 3^{f-1}, G),$$

so that the Suyama compositeness test for G can be modified slightly to rule out *both* primality and prime-power structure: take the GCD of the difference of the two Suyama residues with G. If this $GCD = 1$, then G is neither a prime p nor p^k.

Taking a GCD of two numbers both in the million-bit region is problematic (we used a fast, recursive GCD implementation due to J. P. Buhler, because the classical Euclid algorithm is quite lethargic for numbers in this region). To avoid GCD altogether, a second approach is to assume that a sieving limit on G_n is known, say G_n is divisible only by primes $> P_n$. Then for all $k < \log G_n / \log P_n$, show that G_n cannot be a kth power by comparing, for small primes q, $G_n \pmod q$ and possible kth powers $\pmod q$ until an impossibility $\pmod q$ results for any q. As a practical matter, this test is competitive with the previous GCD test for $n > 16$. Though sieve results are required to limit the search on k, the GCD test required a Pepin residue or equivalent base a to have been calculated. So both methods require some preparation.

6. Status of Fermat numbers, $n \le 22$

Table 2 shows the current status, to the authors' knowledge, of F_n, $n \le 22$. Some salient observations are as follows. F_9 is a triumph of the Number Field Sieve [NFS] method [4]. However, NFS so far appears difficult to implement effectively for any larger F_n. F_{10} is the smallest Fermat number not completely

TABLE 2. Status table for Fermat numbers F_n; $0 \leq n \leq 22$. References for the factors are [1, 3, 4, 5]. The notation means: P = proven prime, C = proven composite. Boldface $\boldsymbol{C}$ indicates a result of the present report. None of the C, $\boldsymbol{C}$ cofactors is a prime power

n	F_n
0, 1, 2, 3, 4	P
5	641 * 6700417
6	274177 * 67280421310721
7	59649589127497217 * 5704689200685129054721
8	1238926361552897 * P
9	2424833* 7455602825647884208337395736200454918783366342657 * P
10	45592577 * 6487031809 * C
11	319489 * 974849* 167988556341760475137 * 3560841906445833920513 * P
12	114689 * 26017793 * 63766529 * 190274191361 * 1256132134125569 * C
13	2710954639361 * 2663848877152141313 * 3603109844542291969 * C
14	C
15	1214251009 * 2327042503868417 * C
16	825753601 * C
17	31065037602817 * C
18	13631489 * C
19	70525124609 * 646730219521 * $\boldsymbol{C}$
20	C
21	4485296422913 * $\boldsymbol{C}$
22	$\boldsymbol{C}$

factored (though F_{11} is completed). F_{14} is the smallest "genuine composite" amongst the Fermat numbers; i.e., compositeness is proved but no factor is yet known. Aspiring factorers should know that factors for the midrange, say, F_{10} through F_{14}, have been fairly well weeded out by applications of ECM, in the sense that there are probably no more hidden factors in this range possessed of less than thirty digits (but one cannot be completely sure yet—the observation is merely statistically motivated). A factorer should also note the sieving limits, as reported in [3], indicating that, in the higher range $n = 18 - 22$, hidden factors $(k2^{n+2} + 1)$ have been ruled out for $k < 2^{36}$. One might therefore summarize the current factoring status as follows: Direct sieving is a nearly exhausted option, the ECM may have just a little potential left (e.g., for the upper regions of Table 2), while the NFS seems hard to apply at any higher levels $n > 9$. Then there is the problem of the character of F_{24}, which character, on the basis of Pepin test complexity, would require (at the computation rate we have enjoyed) about ten years to resolve. Thus, as has always been the case with the Fermat numbers, many great challenges abound.

Note added in proof. The authors were notified by V. Trevisan and J. Carvalho, of Supercomputing Center (CESUP) of Universidade Federal do Rio Grande do Sul, Brazil, of a second calculation. They too find F_{22} composite. Their computation finished nine months after ours, but was performed entirely independently. In fact they were not aware of our result until they had finished. Furthermore, they reported to us exactly the same set of three Selfridge-Hurwitz residues as listed in our Table 1.

ACKNOWLEDGMENTS

We are grateful to J. P. Buhler and H. W. Lenstra Jr. for proofs, algorithms and advice they gave us during this project. For hospitality and resources we wish to thank NeXT, Inc.; Amdahl Corporation; Cray Research, Inc.; and Reed College.

BIBLIOGRAPHY

1. R. Crandall, *Projects in scientific computation*, Springer-Verlag, Santa Clara, CA, 1994, pp. 145–148.
2. R. Crandall and B. Fagin, *Discrete weighted transforms and large-integer arithmetic*, Math. Comp. **62** (1994), 305–324.
3. Wilfrid Keller, *Factors of Fermat numbers and large primes of the form* $k2^n+1$, manuscript.
4. A. K. Lenstra, H. W. Lenstra, Jr., M. S. Manasse, and J. M. Pollard, *The factorization of the ninth Fermat number*, Math. Comp. **61** (1993), 319–349.
5. H. Riesel, *Prime numbers and computer methods for factorization*, Birkhäuser, Boston, 1985, p. 377.
6. J. L. Selfridge and Alexander Hurwitz, *Fermat numbers and Mersenne numbers*, Math. Comp. **18** (1964), 146–148.
7. D. Slowinski, private communication.
8. J. Young and D. Buell, *The twentieth Fermat number is composite*, Math. Comp. **50** (1988), 261–263.

NeXT COMPUTER INCORPORATED, 900 CHESAPEAKE DRIVE, REDWOOD CITY, CALIFORNIA 94063

NeXT COMPUTER INCORPORATED, 900 CHESAPEAKE DRIVE, REDWOOD CITY, CALIFORNIA 94063

2358 WARFIELD WAY, APARTMENT C, SAN JOSE, CALIFORNIA 95122

655-F LONE OAK DRIVE, EAGAN, MINNESOTA 55105