ACTA ARITHMETICA
XXXV (1979)

## Conspectus materiae tomi XXXV, fasciculi 3



La revue est consacrée à la Théorie des Nombres
The journal publishes papers on the Theory of Numbers
Die Zeitschrift veröffentlicht Arbeiten aus der Zahlentheorie
Журнал посвящен теории чисел

L'adresse de la Rédaction et de l'échange | Address of the Editorial Board and of the exchange | Die Adresse der Schriftleitung und des Austausches | Адрес редакции и книгообмена

ACTA ARITHMETICA
ul. Śniadeckich 8, 00-950 Warszawa

Les auteurs sont priés d'envoyer leurs manuscrits en deux exemplaires
The authors are requested to submit papers in two copies
Die Autoren sind gebeten um Zusendung von 2 Exemplaren jeder Arbeit
Рукописи статей редакция просит предлагать в двух экземплярах



ISBN 83-01-01226-9 ISSN 0065-1036

PRINTED IN POLAND

WROCŁAWSKA DRUKARNIA NAUKOWA

# Diophantine representation of Mersenne and Fermat primes

by

JAMES P. JONES* (Calgary)

**1. Introduction.** In 1970 it was shown that Hilbert's tenth problem was recursively unsolvable. Hilbert had asked in 1900 for an algorithm to decide the solubility of all Diophantine equations. Yu.V. Matijasevič [10], [11], using 1961 results of Martin Davis, Julia Robinson and Hilary Putnam [2], proved that every recursively enumerable set is Diophantine. That is to say, he proved that each recursively enumerable set $S$ may be represented in the form

$$x \in S \leftrightarrow \exists x_1, x_2, \ldots, x_k \,[P(x, x_1, \ldots, x_k) = 0] \tag{1.1}$$

where $P$ is a polynomial with integer coefficients and the quantified variables range over nonnegative integers. Since it was well known that there exist recursively enumerable but nonrecursive sets, the unsolvability of Hilbert's tenth problem follows immediately from Matijasevič's theorem.

One very surprising consequence of Matijasevič's Theorem is that every recursively enumerable set $S$ may be represented in the form

$$x \in S \leftrightarrow \exists x_1, x_2, \ldots, x_n \,[Q(x_1, x_2, \ldots, x_n) = x]. \tag{1.2}$$

This follows from a theorem of Hilary Putnam [15]. Putnam noticed that for $P$ as in (1.1), the positive values of the polynomial $Q = x(1-P^2)$ coincide exactly with the members of $S$. For if $0 < x(1-P^2)$, then $P = 0$. Notice that $n = k+1$ so that $Q$ has one more variable than $P$.

Thus polynomial formulae exist for virtually all the different sets commonly considered in the theory of numbers. Using methods developed during the course of research on Hilbert's tenth problem, such polynomials may actually be constructed and written down.

* This paper was written during the author's 1975–76 sabbatical leave at the University of California, Berkeley. The author wishes to express his gratitude to Professors Julia Robinson, Raphael M. Robinson and D. H. Lehmer for their generous advice and assistance.

A polynomial in 2 variables, representing the set of Fibonacci numbers, was constructed in [7]. A polynomial representing the set of all prime numbers is given in [6] and [12] and [25].

In this paper we construct three polynomials, representing respectively the Mersenne primes, the even perfect numbers, and the Fermat primes. The three polynomials are easily written down in completely explicit form. We will prove

THEOREM 1. *Each of the following three sets is represented by the given polynomial*:

(1) *The Mersenne primes*:

$$n\{1-[4b+3-n]^2-b([2+hn^2-a]^2+[n^3d^3(nd+2)(h+1)^2+1-m^2]^2+$$
$$+[db+d+chn^2+g(4a-5)-kn]^2+[(a^2-1)c^2+1-k^2n^2]^2+$$
$$+[4(a^2-1)i^2c^4+1-f^2]^2+$$
$$+[(kn+lf)^2-((a+f^2(f^2-a))^2-1)\cdot(b+1+2jc)^2-1]^2)\}.$$

(2) *The even perfect numbers*:

$$(2b+2)n\{1-[4b+3-n]^2-b([2+hn^2-a]^2+[n^3d^3(nd+2)\cdot(h+1)^2+$$
$$+1-m^2]^2+$$
$$+[db+d+chn^2+g(4a-5)-kn]^2+[(a^2-1)c^2+1-k^2n^2]^2+$$
$$+[4(a^2-1)i^2c^4+1-f^2]^2+$$
$$+[(kn+lf)^2-((a+f^2(f^2-a))^2-1)\cdot(b+1+2jc)^2-1]^2)\}.$$

(3) *The Fermat primes*:

$$(6g+5)\{1-[bh+(a-12)c+n(24a-145)-d]^2-[16b^3h^3(bh+1)\times$$
$$\times(a+1)^2+1-m^2]^2-$$
$$-[3g+2-b]^2-[2be+e-bh-1]^2-[k+b-c]^2-[(a^2-1)c^2+1-d^2]^2-$$
$$-[4(a^2-1)i^2c^4+1-f^2]^2-$$
$$-[(d+lf)^2-((a+f^2(f^2-a))^2-1)\cdot(b+2jc)^2-1]^2\}.$$

In each case the claim is that the given set of numbers is identical with the set of positive values of the associated polynomial, as the variables run thru the nonnegative integers. The polynomial (1) has 13 variables, $a, b, c, d, f, g, h, i, j, k, l, m, n$, and is of the 26th degree. Polynomial (2) contains the same 13 variables and has degree 27. The third polynomial (3) has one additional variable, $e$, and degree 25.

Of course these polynomials also assume certain negative values, about which nothing is claimed. This shortcoming cannot be avoided. It is impossible to represent Mersenne primes, even perfect numbers or Fermat primes, by polynomials taking no other values. We prove this.

THEOREM 2. *Let $S$ denote any one of the following three sets: Mersenne primes, perfect numbers, or Fermat primes. Let $P(x_1, x_2, \ldots, x_n)$ be any polynomial. If $P(x_1, x_2, \ldots, x_n) \in S$ for all nonnegative integers $x_1, x_2, \ldots, x_n$, then $P$ is a constant.*



PROOF. The proof depends only upon a simple divisibility property shared by these three sets. It will therefore apply equally well to any other set $S$ possessing this property. The property is

$$\text{(D)} \qquad a \in S \wedge \beta \in S \wedge a|\beta \to a = \beta.$$

Plainly, property (D) holds for any set of primes. (D) also holds if $S$ is a set of perfect numbers. To see this recall that $n$ is *perfect* if $\sigma(n) = 2n$ where $\sigma(n)$ denotes the sum of the divisors of $n$. Now for $1 < \gamma$, $\gamma\sigma(a) < \sigma(\gamma a)$. Taking $\beta = \gamma a$ yields the result.

Now suppose that a polynomial $P(x_1, x_2, \ldots, x_k)$ maps nonnegative integers into the set $S$. The coefficients of an integer valued polynomial must be rational numbers, by the Lagrange Interpolation Theorem. Let $l$ be any common multiple of the denominators of coefficients of $P(x_1, x_2, \ldots, x_k)$. Let $P(0, 0, \ldots, 0) = a$. We may suppose $a \neq 0$ because, if $0 \in S$, then $S = \{0\}$ by (D). Let $\beta = P(n_1 la, n_2 la, \ldots, n_k la)$. Then $\beta \equiv a \pmod a$ because $P(x_1, \ldots, x_k)$ is a polynomial. Hence $a|\beta$. Hence $a = \beta$, by (D). Thus $P(n_1 la, n_2 la, \ldots, n_k la)$ is constant in $n_1, n_2, \ldots, n_k$. Hence $P(x_1, \ldots, x_k)$ is a polynomial of degree zero. The theorem is proved.

A polynomial is a special case of an *algebraic function*. Theorem 2 generalizes to algebraic functions, because an integer valued algebraic function is necessarily a polynomial (cf. T. Kojima [26], Theorem 3, also Skolem [21], Satz 27, and [6], Theorem 4.2). Hence

COROLLARY. *Let $S$ denote any one of the following three sets: Mersenne primes, perfect numbers or Fermat primes. Let $f(z_1, z_2, \ldots, z_n)$ be any algebraic function. If $f(z_1, z_2, \ldots, z_n) \in S$ for all nonnegative integers $z_1, z_2, \ldots, z_n$, then $f$ is a constant.*

It is interesting to consider the question of the minimum number of variables necessary in the polynomials constructed here. Concerning this question, Yu.V. Matijasevič and Julia Robinson proved in [13] that the number of unknowns in any Diophantine equation may be reduced to 13. Recently this result has been improved by Matijasevič to 9 unknowns. From this it would follow that the three sets discussed here could be defined in 9 unknowns and hence that 10 variables are sufficient in the Putnam polynomials. We will prove here that these three sets are definable in 6 unknowns.

THEOREM 3. *Let $S$ denote any one of the following sets: Mersenne primes, even perfect numbers or Fermat primes. Then $S$ is the positive part of the range of a polynomial in 7 variables.*

This value, 6, is almost certainly not best possible, but the question of how far it can be reduced is a very difficult one, closely connected with the old problem of whether there are infinitely many Mersenne or

Fermat primes. A finite set of numbers can be represented by a polynomial in 1 variable. An infinite set of primes is easily seen to require at least 2 variables (cf. [6], Theorem 4.1).

At the present time only twenty five Mersenne primes are known. These are the numbers $2^n-1$ for the following values of $n$: 2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, 127, 521, 607, 1279, 2203, 2281, 3217, 4253, 4423, 9689, 9941, 11213, 19937, 21701.

The first twenty five even perfect numbers are therefore obtained by substituting these values of $n$ into Euclid's formula $2^{n-1}(2^n-1)$. The three giant Mersenne primes

$$2^{11213}-1, \quad 2^{19937}-1, \quad 2^{21701}-1,$$

are the largest known primes at the present time. They were discovered by D. Gillies [4], B. Tuckerman [23], and two students Laura Nickel and Curtis Noll, age 18. Sierpiński [20] gives an explanation of how such large numbers can be proved prime, using a theorem of E. Lucas and D. H. Lehmer [9]. We will use this same theorem to formulate our Diophantine definition of the Mersenne primes, in Section 3.

At the present time we are unable to prove that there exists a Mersenne prime greater than $M_{21701}$. And the situation with regard to the Fermat primes seems even less hopeful. Only five Fermat primes are known at the present time, $F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$ and $F_4 = 65537$. All larger Fermat numbers, $F_n = 2^{2^n}+1$ which have been investigated to date have turned out to be composite. In particular $F_n$ is known to be composite for $4 < n < 20$ and for many larger values of $n$. R. M. Robinson proved $F_{1945}$ composite [20].

On the other side, we are also unable to prove the existence of infinitely many composite Fermat numbers. And no one has succeeded in proving the existence of infinitely many composite Mersenne numbers with prime index. It is widely believed that there are infinitely many Mersenne primes and therefore infinitely many even perfect numbers. The fact that an odd perfect number has yet to be found makes it seem very likely that the polynomial (2) actually includes all perfect numbers.

**2. The Pell equation.** We shall require a number of lemmas concerning the solutions of the Pell equation $x^2-(a^2-1)y^2 = 1$. We shall use the notation of [13]. Proofs not given may be found in [1], [6], [13], [16], [17]. All variables denote nonnegative integers unless otherwise delimited.

The solutions of the special Pell equation $x^2-(a^2-1)y^2 = 1$ can be generated algebraically by the equation

$$\chi_a(n)+\psi_a(n)\sqrt{a^2-1} = (a+\sqrt{a^2-1})^n$$



or as Lucas sequences with the defining equations

$$\chi_a(0) = 1, \quad \chi_a(1) = a, \quad \chi_a(n+2) = 2a\chi_a(n+1)-\chi_a(n),$$
$$\psi_a(0) = 0, \quad \psi_a(1) = 1, \quad \psi_a(n+2) = 2a\psi_a(n+1)-\psi_a(n).$$

These sequences have the following properties:

LEMMA 2.1. $\chi_a(n) \equiv \chi_b(n) \pmod{a-b}$ *and* $\psi_a(n) \equiv \psi_b(n) \pmod{a-b}$.

LEMMA 2.2. $\chi_a(2n) = 2\chi_a(n)^2-1$ *and* $\psi_a(2n) = 2\chi_a(n)\psi_a(n)$.

LEMMA 2.3. $\chi_a(n) \equiv s^n+\psi_a(n)\cdot(a-s) \pmod{2as-s^2-1}$.

LEMMA 2.4. $(s^2-1)s^n\psi_a(n) \equiv s(s^{2n}-1) \pmod{2as-s^2-1}$.

Proof. Square both sides of (2.3). Use $\chi_a^2(n) = (a^2-1)\psi_a^2(n)+1$ and then multiply thru by $s$.

LEMMA 2.5. *If* $0 < s < a$, *then* $a \leqslant 2as-s^2-1$.

Proof. $a \leqslant as \leqslant as+s-1 = as+(1+s)s-s^2-1 \leqslant as+as-s^2-1$.

LEMMA 2.6. *For* $2 \leqslant X$, *the condition*

$$(*) \qquad X^3(X+2)\cdot(y+1)^2+1 = \square$$

*implies that* $X-1+X^{X-2} \leqslant y$. *Conversely, for any non-negative* $X$, $(*)$ *has arbitrarily large solutions* $y$.

Proof (cf. [6], Lemma 2.3 or the First Lemma of Exponential Size in [13]).

LEMMA 2.7. *Let* $0 < s < a$. *Suppose* $y^3 < a$ *and* $z^3 < a$. *Then for any number* $\psi$ *both* $(s^2-1)y\psi \equiv s(y^2-1) \pmod{2as-s^2-1}$ *and* $(s^2-1)z\psi \equiv s(z^2-1) \pmod{2as-s^2-1}$ *imply* $y = z$.

Proof. Multiplying the congruences by $z$ and $y$ respectively we obtain

$$(s^2-1)y\psi z \equiv sz(y^2-1) \quad \text{and} \quad (s^2-1)z\psi y \equiv sy(z^2-1) \pmod{2as-s^2-1}.$$

Hence $sz(y^2-1) \equiv sy(z^2-1)$ and therefore $s(y-z)\cdot(yz+1) \equiv 0 \pmod{2as-s^2-1}$. But $s \perp 2as-s^2-1$. So $(y-z)\cdot(yz+1) \equiv 0 \pmod{2as-s^2-1}$. Now

$$|y-z|\cdot|yz+1| \leqslant (a^{1/3}-1)\cdot(a^{2/3}+1) < a \leqslant 2as-s^2-1$$

by Lemma 2.5. Therefore $(y-z)\cdot(yz+1) = 0$. Since $yz \geqslant 0$, we have $y-z = 0$. ∎

The next lemma yields a new definition of exponentiation in 5 unknowns. This method of defining the exponential relation by means of the congruence of Lemma 2.4, was pointed out to us by Julia Robinson.

LEMMA 2.8. *Let* $0 < S$. *The exponential relation* $Y = S^B$ *holds if and*

*only if there exist integers $A$ and $C$ such that*

(i) $S < A$,

(ii) $S^{3B} < A$, $Y^3 < A$,

(iii) $(S^2-1)\,YC \equiv S(Y^2-1) \pmod{2AS-S^2-1}$,

(iv) $C = \psi_A(B)$.

Proof. By Lemmas 2.4, 2.5, and 2.7. Note that the conditions (i) and (ii) may be replaced by the condition of Lemma 2.6 with $X = 3B+Y+2$.

Julia Robinson and Yu.V. Matijasevič [13] have worked out a Diophantine definition of the relation $C = \psi_A(B)$ which uses only 3 unknowns. This is given in the next lemma. For a proof see [13].

LEMMA 2.9. *Let $1 < A$ and $0 < B$. The relation $C = \psi_A(B)$ holds if and only if there exist integers $D, E, F, G, H, I$ and nonnegative integers $i, j$ such that*

A1. $DFI = \square$, $F \mid H-C$, $B \leqslant C$,

A2. $D = (A^2-1)C^2+1$,

A3. $E = 2(i+1)D(e+1)C^2$,

A4. $F = (A^2-1)E^2+1$,

A5. $G = A+F(F-A)$,

A6. $H = B+2jC$,

A7. $I = (G^2-1)H^2+1$.

This definition has the convenient built-in feature that any other divisibility condition, for example (iii) above, may be combined with that in A1. For $F \perp e+1$ so that $F \mid H-C$ and $e+1 \mid P$ is equivalent to $F(e+1) \mid (H-C)\cdot(e+1)+FP$. Hence only 5 unknowns are needed to define the exponential relation by the method of Lemma 2.8. When $1 < B$, we may replace $j$ by $j+1$ in A6 so that $0 < H-C$ in A1. This is important for applications of Theorem 5.1:

The equations A1–A7 may be rewritten as follows:

LEMMA 2.10. *Let $1 < A$ and $0 < B$. The relation $C = \psi_A(B)$ holds, if and only if there exist integers $E, G, H, I$, and nonnegative integers $D, F, i, j$ such that*

P1. $D \leqslant I$, $F \mid I-D$, $B \leqslant C$,

P2. $D^2 = (A^2-1)C^2+1$,

P3. $E = 2ieC^2$,

P4. $F^2 = (A^2-1)E^2+1$,

P5. $G = A+F^2(F^2-A)$,

P6. $H = B+2jC$,

P7. $I^2 = (G^2-1)H^2+1$.



Proof. Lemma 2.10 may be proved exactly as Theorem 4 is proved in [13]. The only change required is to replace the second step down lemma for the $\psi$ sequence by the corresponding lemma for the $\chi$ sequence (Lemma 2.24 of Davis [1]), cf. also [6], Lemma 2.5.

Now if we take $e = 1$ and express the conditions $D \leqslant I$ and $F \mid I-D$ by $(\exists l)(I = D+lF)$, then the unknowns $E, G, H$ and $I$ eliminate by substitution and the system P1–P7 reduces to the following simple set (used in writing out (1), (2) and (3)).

Q1. $B \leqslant C$,

Q2. $D^2 = (A^2-1)C^2+1$,

Q3. $F^2 = 4(A^2-1)i^2C^4+1$,

Q4. $(D+lF)^2 = \left(\left[A+F^2(F^2-A)\right]^2-1\right)(B+2jC)^2+1$.

When these equations are used in the definition of exponentiation, then, if we wish, we may use the congruence of Lemma 2.3 rather than that of Lemma 2.4 because $\chi_A(n)$ is now available in the form of $D$.

**3. The Mersenne primes and even perfect numbers.** The basic connection between these two sets of numbers was discovered by Euclid and Euler who proved that an even number is perfect if and only if it is of the form $2^{n-1}(2^n-1)$ where $2^n-1$ is prime. To determine the primality of a Mersenne number $2^n-1$, we may use a test worked out by Lucas and Lehmer ([9], [20]). This test uses the sequence $s_n$ defined by $s_1 = 4$ and $s_{n+1} = s_n^2-2$.

LEMMA 3.1 (Lucas – Lehmer [9]). *Let $N = 2^n-1$, $n > 2$. $N$ is prime, if and only if $N \mid s_{n-1}$.*

Mersenne numbers are always odd and $s_n$ is always even, so the test may equally well be based on the sequence $t_n = s_n/2$. This sequence has the defining equations $t_1 = 2$ and $t_{n+1} = 2t_n^2-1$. Fortunately the sequence $t_n$ is closely related to the sequence of solutions of the Pell equation. The author and his student D. Wiens [24] discovered

LEMMA 3.2 $t_n = \chi_2(2^{n-1})$.

Proof. From Lemma 2.2 we see that the two sequences have the same defining equations. ∎

Now let $b = 2^{n-2}-1$ so that $N = 2^n-1 = 4b+3$. Then $N$ is a Mersenne prime if and only if $b = 0$, or $b+1$ pow 2 and $N \mid \chi_2(b+1)$. Let $S$ be any fixed positive power of 2, eg. 2 or 4. Then the condition $b+1$ pow 2 is equivalent to $b+1 \mid S^{b+1}$. Thus $N = 4b+3$ is a Mersenne prime if and only if $b = 0$ or there exist numbers $d, B, Y$ satisfying

(i) $B = b+1$, (ii) $Y = Bd$, (iii) $Y = S^B$, and (iv) $N \mid \chi_2(B)$.

The exponential relation (iii) may be defined by the equations of Lemmas 2.8 and 2.9. These equations define $\psi_A(B)$ rather than $\psi_2(B)$, which we need for (iv). Nevertheless, if we are careful to choose $A \equiv 2(\mathrm{mod}\, N)$, then the test condition (iv) may also be defined in terms $C = \psi_A(B)$. Using Lemma 2.1 one can show

if $A \equiv 2(\mathrm{mod}\, N)$, then $N|\chi_2(B) \leftrightarrow N^2|(A^2-1)C^2+1$,

if $A \equiv 2(\mathrm{mod}\, N^2)$, then $N|\chi_2(B) \leftrightarrow N^2|3C^2+1$.

It is interesting to note that the method here, working with the Pell equation modulo $N$, is very much analogous to the situation in actual computational practice where one works with the sequence $s_n$ modulo $N$.

Thus we obtain from Lemmas 2.6, 2.8, and 2.9, the following equations for the Mersenne primes:

LEMMA 3.3. *The number $4b+3$ is a Mersenne prime if and only if $b = 0$ or there exist integers $A, B, C, D, E, F, G, H, I, N, S, X, Y$ and non-negative integers $d, g, h, i, j$ such that*

(1) $S = 4$,

(2) $N = 4b+3$,

(3) $B = b+1$,

(4) $Y = Bd$,

(5) $A = 2+(h+1)N$,

(6) $X = Nd$,

(7) $X^2(X+2)(h+1)^2+1 = \square$,

(8) $(S^2-1)YC \equiv S(Y^2-1)(\mathrm{mod}\, 2AS-S^2-1)$,

(9) $DFI = \square$, $F|H-C$, $C = g+B$,

(10) $D = (A^2-1)C^2+1$,

(11) $E = 2(i+1)\times$ $\times D(e+1)C^2$,

(12) $F = (A^2-1)E^2+1$,

(13) $G = A+F(F-A)$,

(14) $H = B+2jC$,

(15) $I = (G^2-1)H^2+1$,

(16) $N^2|D$.

Proof. Suppose $b > 0$ and conditions (1)–(16) hold. Then $1 < A$ and $0 < B$ and by Lemma 2.9, (9)–(15) imply that $C = \psi_A(B)$. Conditions (1), (5) and (8) imply $Y \neq 0$. Hence $d \neq 0$ by (4). By (2), (3) $3B < N$ and hence $3Y < X$ by (4), (6). By (2) and (6) $7 \leqslant X$. Now (2) and (3) imply that $3B+1 \leqslant N \leqslant X$. By Lemma 2.6, $X^{X-2} \leqslant h < A$ so $Y^3 < A$. Also $N^{X-1} \leqslant NX^{X-2} \leqslant hN < A$ hence $S^{3B} < A$. By (8) and Lemma 2.8 we have $Y = S^B$. By (16), $N|\chi_A(B)$. By (5), $A \equiv 2(\mathrm{mod}\, N)$. Hence by Lemma 2.1, $N|\chi_2(B)$. Thus (i)–(iv) hold and $4b+3$ is a Mersenne prime.

Conversely, suppose $4b+3$ is a Mersenne prime and $b > 0$. Let $S = 4$ and put $N = 4b+3$. Choose $d, B$ and $Y$ satisfying (i)–(iv). Put $X = Nd$. By Lemma 2.6 we may choose $h$ satisfying (7). Put $A = 2+(h+1)N$. Put $C = \psi_A(B)$. Lemma 2.4 implies condition (8). By Lemma 2.9 we may choose non-negative integers $g, i, j$ and integers $D, E, F, G, H, I$ satisfying (9)–(15). Here $D = \chi_A^2(B)$. By (iv), $N|\chi_2(B)$. By (5), $A \equiv 2(\mathrm{mod}\, N)$. So by Lemma 2.1, $N|\chi_A(B)$. Hence (16) holds. Hence (1)–(16) all hold. ∎

From the equations and conditions of Lemma 3.3 it is easy to construct the polynomial formulas (1) and (2) representing Mersenne primes and even perfect numbers respectively. We proceed with this.

Proof of Theorem 1 (formulas (1) and (2)). We obtain shorter formulas if we first make a few modifications. Lemma 3.3 remains true if we replace (1) by $S = 2$, (5) by $A = 2+hN^2$, (8) by

$$D \equiv Y+C(A-2)(\mathrm{mod}\, 2AS-S^2-1),$$

(9)–(15) by Q2–Q3 and (16) by $N|D$. We need not include condition Q1 for we have $D^2 = (A^2-1)C^2+1 \equiv 3C^2+1(\mathrm{mod}\, N^2)$ by (5). Hence $N^2|3C^2+1$ by (16). So $3B^2+1 \leqslant N^2 \leqslant 3C^2+1$ and therefore $B \leqslant C$. Thus Q1 is implied by the other conditions. The proof that $Y \neq 0$ is a little different than before. We must use the fact that $C = \psi_A(B)$ so that $Y \equiv S^B(\mathrm{mod}\, 2AS-S^2-1)$ by (8) and Lemma 2.3. Then $S^B$ is a power of 2 whereas $2AS-S^2-1$ is an odd number. So $Y \neq 0$. The rest of the proof goes thru without change.

The polynomials (1) and (2) are constructed from these modified equations. First eliminate the variables $S, B, Y, X$ by substitution. Replace $A, C, F, N$ by lower case letters. Replace $\square$ by $m^2$ in (7) and $N|D$ by $D = kN$ in (16). Transpose all terms in the equations to one side, sum the squares of the equations and apply (essentially) the method of Putnam [15] explained in § 1. The construction of formula (2) proceeds similarly. It follows from Euclid's formula that $4b+3$ is a Mersenne prime if and only if $(2b+2)(4b+3)$ is an even perfect number. ∎

Proof of Theorem 3 for Mersenne primes and even perfect numbers. Here we show how to reduce the number of unknowns to 6. Consider again the conditions (1)–(16) of Lemma 3.3. The variables $S, N, B, Y, A, X, D, E, F, G, H, I$ may be eliminated by substitution. Then remain two square conditions, (7) and (9), and three divisibility conditions, (8), (9) and (16), involving the parameter $b$ and the unknowns $d, g, h, i, j$. By (1) and (5), $2AS-S^2-1 \equiv -1(\mathrm{mod}\, N)$. Hence $N \perp 2AS-S^2-1$. Therefore the two divisibility conditions (8) and (16) may be combined into one divisibility condition with divisor $N^2(2AS-S^2-1)$. (This is why we took $S = 4$ in (1).) If we now put $e+1 = N(2AS-S^2-1)$ in (11), then $F, N$ and $2AS-S^2-1$ will be relatively prime in pairs so that all three divisibility conditions may be combined into one with divisor $FN^2(2AS-S^2-1)$. Now $e+1$ will be positive if we replace $h$ by $h+1$ in (5). The divisor in condition (8) will then also be positive, but the dividend may well be negative. Hence both should be squared. If we also replace $j$ by $j+1$ in (14) then $H-C \geqslant 0$ and so the entire dividend will be nonnegative. The divisor, $FN^2(2AS-S^2-1)^2$ will also be positive

by the choice of $S$. Applying [13] the Relation Combining Theorem (see § 5) we obtain a polynomial $M_2(b, d, g, h, i, j, n)$ (in six unknowns) with the property that $4b+3$ is a Mersenne prime if and only if $\exists d, g, h, i, j, n$ such that $b=0$ or $M_2=0$. Hence the seven variable polynomial $(4b+3)\times$ $\times(1-bM_2^2)$ represents Mersenne primes. And the seven variable polynomial $(2b+2)(4b+3)(1-bM_2^2)$ represents the set of all even perfect numbers. ∎

OPEN PROBLEM. The Lucas – Lehmer primality test for Mersenne numbers, $N=2^n-1$ (Lemma 3.1) involves the condition $N|s_{n-1}$. Can we replace this condition by $N^2|s_{n+1}$? The latter condition is easily seen to be necessary. Is it sufficient?

**4. The Fermat primes.** Fermat's numbers are defined by $F_n=2^{2^n}+1$. Thus it might appear necessary to define a double exponential to define Fermat primes. Fortunately this is not so. We need only define primality for numbers of the form $2^m+1$, since any prime number of this form is necessarily a Fermat number.

The primality of a number of the form $2^m+1$ may be determined by a simple test due to T. Pepin [14]. This test also appears in R. M. Robinson [18] and Sierpiński [20]. The test is based on Euler's criterion which states that if $N$ is an odd prime and $N\nmid a$, then $a^{(N-1)/2}\equiv(a/N)(\mathrm{mod}\,N)$, where on the right side of the congruence we have a Legendre symbol.

LEMMA 4.1 (Pepin [14]). *Let $N=2^m+1$ and suppose that $N\nmid a$ and $(a/N)=-1$. Then $N$ is prime, if and only if $a^{(N-1)/2}\equiv-1(\mathrm{mod}\,N)$.*

Proof. If $N$ is prime then the congruence holds by Euler's criterion. For the converse, suppose that the congruence holds. Then $a^{2^{m-1}}\equiv-1(\mathrm{mod}\,N)$ but $a^{2^m}\equiv1(\mathrm{mod}\,N)$. So $2^m$ is the exact order of $a$ to the modulus $N$. The congruence also implies $a\perp N$ so that Euler's Theorem, $a^{\varphi(N)}\equiv1(\mathrm{mod}\,N)$ holds. Thus $2^m|\varphi(N)$. Hence $N-1=2^m\leqslant\varphi(N)$. If $N$ were composite, then we would have $\varphi(N)<N-1$. Hence $N$ is prime. ∎

There are several choices for $a$. For example $(3/N)=-1$ and $(6/N)=-1$ $(N>5)$. But we prefer $a=12$. It is not difficult to show, using quadratic reciprocity, that when $N=2^m+1$ is prime and $m>1$ then $(12/N)=-1$. This choice of $a$ will allow us to define both the Pepin test condition, and the condition $N-1$ pow 2, using only one exponential, a power of 12. For this purpose $a=6$ would also do but if $N=5$, then $(6/N)=+1$ and we have an exception. For this reason we take $a=12$.

LEMMA 4.2. *All the Fermat numbers $F_n$ $(n>0)$, have the form $6g+5$.*

Proof. For $n>0$, $2^{2^n}\equiv4(\mathrm{mod}\,6)$. Hence $F_n\equiv5(\mathrm{mod}\,6)$.

LEMMA 4.3. *$N=6g+5$ is a Fermat prime, if and only if there exists $Y$ such that*

(1) $Y=12^{3g+2}$, (2) $3g+2|Y$, (3) $Y\equiv-1(\mathrm{mod}\,N)$.



Proof. Since $N=6g+5$, we have $N-1\perp3$. Condition (2) asserts that $(N-1)/2$ divides a power of 12. Hence $N-1$ is a power of 2. Condition (3) is Pepin's congruence test for the primality of $N$.

Now from Lemmas 4.3, 2.8 and 2.9 we obtain the following equations for the Fermat primes. By Lemma 4.2, the definition will include all Fermat primes except $F_0=3$.

LEMMA 4.4. *For any nonnegative integer $g$, $6g+5$ is a Fermat prime, if and only if there exist integers $A, B, C, D, E, F, G, H, I, S, X, Y$ and nonnegative integers $h, i, j, k, y$ such that*

(1) $X=3B+Y+S+2$,

(2) $X^3(X+2)\cdot(y+1)^2+1=\square$,

(3) $(S^2-1)YC \equiv S(Y^2-1)(\mathrm{mod}\,2AS-S^2-1)$,

(4) $A=(y+1)\cdot(6g+5)+6$,

(5) $B=3g+2$,

(6) $S=12$,

(7) $Y=Bh$,

(8) $6g+5\,|\,Y+1$,

(9) $DFI=\square$, $F|H-C$, $C=k+B$,

(10) $D=(A^2-1)C^2+1$,

(11) $E=2(i+1)\times\times D(e+1)C^2$,

(12) $F=(A^2-1)E^2+1$,

(13) $G=A+F(F-A)$,

(14) $H=B+2(j+1)C$,

(15) $I=(G^2-1)H^2+1$.

Here we have taken $A=(y+1)\cdot(6g+5)+6$ (rather than $A=y$), so that $2AS-S^2-1>0$ and $6g+5\perp2AS-S^2-1$. Hence as before all 3 divisibility conditions (3), (8) and (9) may be combined into one divisibility condition by choosing $e+1=(6g+5)\cdot(2AS-S^2-1)$ so that the divisors are relatively prime in pairs.

After $A, B, \ldots, Y$ have been eliminated by substitution there remain only one divisibility condition and two square conditions involving the parameter $g$ and the unknowns $h, i, j, k, y$. As before these three conditions are definable in 1 additional unknown, $n$, by the Relation Combining Theorem of [13] (cf. § 5). The result is a polynomial $M_2(g, h, i, j, k, y, n)$ with the property that $6g+5$ is a Fermat prime, if and only if $\exists h, i, j, k, y, n$ $M_2=0$. Hence the Fermat primes $(>3)$ are representable by the 7 variable polynomial $(6g+5)\{1-M_2(g, h, i, j, y, n)^2\}$.

When writing out the polynomial (3), given in the introduction, we have omitted equation (4), taken $y=a$ in (2), used 2.3 instead of 2.4 in (3) and equations Q1–Q4 instead of A1–A7. Variables $S, X, Y$ were eliminated and $A, B, C, D, F$ retained and replaced by the lower case letters $a, b, c, d, f$.

**5. The degree.** What will be the degree of the 7 variable polynomials constructed here? The Relation Combining Theorem, as stated in [13], is somewhat uneconomical with respect to the degree. However, Yu.V.

Matijasevič has since worked out a more efficient version of the Relation Combining Theorem. We state this version here:

THEOREM 5.1. *For all integers* $A_1, \ldots, A_q, B, C, D, V_1, \ldots, V_q$ *with* $0 < B$, $0 \leqslant C$, $1 + |\sqrt{A_i}| \leqslant V_i$ $(i = 1, \ldots, q)$, *the conditions* $A_i = \square$ $(i = 1, \ldots, q)$, $B | C$ *and* $0 < D$ *all hold if and only if* $M_q(A_1, \ldots, A_q, B, C, D, n, V_1, \ldots, V_q) = 0$ *for some* $n$, *where* $M_q$ *is the following* $2^q$*-fold product over all combinations of signs*

$$M_q = \prod\prod [Bn + C - B(2D-1)\cdot(C + W_q \pm \sqrt{A_1} \pm \sqrt{A_2} W_1 \pm \sqrt{A_3} W_2 \pm \ldots \ldots \pm \sqrt{A_q} W_{q-1})],$$

*and* $W_i = V_1 V_2 \ldots V_i$.

A direct calculation, based on Theorem 5.1, gives the following values for the degree. The degree of $M_2$ is 456 for the Mersenne prime definition and 452 for the Fermat prime definition. Hence the 7 variable Mersenne prime representing polynomial of Theorem 3 has degree 914. The 7 variable even perfect number polynomial has degree 915 and that of the Fermat primes degree 905.

Of course the degree of all of these polynomials can be reduced to 5 by a well known method of substitution due to Skolem [22] (of. Davis [1], Theorem 7.5). But this method of reducing the degree increases the number of variables, from 7 to about 20 in our case.

## References


[1] Martin Davis, *Hilbert's tenth problem is unsolvable*, Amer. Math. Monthly 80 (1973), pp. 233–269.

[2] Martin Davis, Hilary Putnam and Julia Robinson, *The decision problem for exponential Diophantine equations*, Ann. of Math. 74 (1961), pp. 425–436. = Математика 8.5 (1964), pp. 69–79.

[3] Martin Davis, Yuri Matijasevič, and Julia Robinson, *Hilbert's tenth problem. Diophantine equations: Positive aspects of a negative solution*, Proceedings of the Symposium on Hilbert's problems, Amer. Math. Soc. 1976, pp. 323–378.

[4] Donald Gillies, *Three new Mersenne primes, and the statistical theory*, Mathematics of Computation 18 (1964), pp. 93–97.

[5] James P. Jones, *Three universal representations of recursively enumerable sets*, Journ. Symbolic Logic 43 (1978), pp. 335–351.

[6] James P. Jones, Daihachiro Sato, Hideo Wada, and Douglas Wiens, *Diophantine representation of the set of prime numbers*, Amer. Math. Monthly 83 (1976), pp. 449–464; MR 54, 2615.

[7] James P. Jones, *Diophantine representation of the Fibonacci numbers*, Fibonacci Quarterly 13 (1975), pp. 84–88. MR 52, 3035.

[8] — *Diophantine representation of the Lucas numbers*, ibid. 14 (1976), p. 134.

[9] D. H. Lehmer, *On Lucas's test for the primality of Mersenne's numbers*, Journ. London Math. Soc. 10 (1935), pp. 162–165.





[10] Юрий Матиясевич, *Диофантовость перечислимых множеств*, Докл. АН СССР 191 (1970), pp. 279–282. = *Enumerable sets are diophantine*, Soviet Math. Doklady 11 (1970), pp. 354–358.

[11] — *Диофантово представление перечислимых предикатов*, Изв. АН СССР, Сер. Матем. 35 (1971), pp. 3–30. = *Diophantine representation of enumerable predicates*, Mathematics of the USSR – Izvestija 5 (1971), pp. 1–28.

[12] — *Диофантово представление множества простых чисел*, Докл. АН СССР 196.4 (1971), pp. 770–773. = *Diophantine representation of the set of prime numbers*, Soviet Math. Doklady 12 (1971), pp. 249–259.

[13] Yuri Matijasevič and Julia Robinson, *Reduction of an arbitrary Diophantine equation to one in* 13 *unknowns*, Acta Arith. 27 (1975), pp. 521–553.

[14] T. Pepin, *Sur la formule* $2^{2^n} + 1$, C. R. Acad. Sci. Paris 85 (1877), pp. 329–331.

[15] Hilary Putnam, *An unsolvable problem in number theory*, Journal of Symbolic Logic 25 (1960), pp. 220–232. = Математика 8.5 (1964), pp. 55–67.

[16] Julia Robinson, *Diophantine decision problems*, M.A.A. Studies in Mathematics 6 (1969), [Studies in Number Theory, W. J. Leveque, editor], pp. 76–116.

[17] — *Existential definability in arithmetic*, Trans. Amer. Math. Soc. 72 (1952), pp. 437–449. = Математика 8.5 (1964), pp. 3–14. MR 14, 4.

[18] Raphael M. Robinson, *The converse of Fermat's theorem*, Amer. Math. Monthly 64 (1957), pp. 703–710.

[19] — *Mersenne and Fermat numbers*, Proc. Amer. Math. Soc. 5 (1954), pp. 842–846.

[20] Wacław Sierpiński, *Elementary Theory of Numbers*, P.W.N., Warsaw 1964, 480 pp.

[21] Thoralf Skolem, *Untersuchungen über die möglichen Verteilungen ganzzahliger Lösungen gewisser Gleichungen*, Skrifter utgit av Videnskapsselskapet i Kristiania, 1921, No 17, 57 pp.

[22] — *Diophantische Gleichungen*, Springer, Berlin 1938.

[23] Bryant Tuckerman, *The 24th Mersenne prime*, Proc. Nat. Acad. Sci. 68 (1971), pp. 2319–2320.

[24] Douglas Wiens, *Characterizations of the Perfect Numbers*, Master's Thesis. Department of Mathematics, University of Calgary, August 1974, v+78 pp.

[25] Ю. В. Матиясевич, *Простые числа перечисляются полиномом от* 10 *переменных*, Зап. Научн. Семинаров Ленингр. отд. Матем. ин-та им. В. А. Стеклова АН СССР 68 (1977), pp. 62–82.

[26] T. Kojima, *Note on number-theoretic properties of algebraic functions*, Tôhoku Math. J. 8, pp. 24–37.



DEPARTMENT OF MATHEMATICS
UNIVERSITY OF CALGARY
Calgary, Alberta, Canada



*Received on 11. 5. 1976*
*and in revised form on 27. 1. 1977* (849)