THE UNIVERSITY OF CALGARY

DIOPHANTINE CHARACTERIZATIONS

OF THE PERFECT NUMBERS

by

DOUGLAS P. WIENS

A THESIS

SUBMITTED TO THE FACULTY OF GRADUATE STUDIES

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE OF

MASTER OF SCIENCE

DEPARTMENT OF MATHEMATICS

STATISTICS AND COMPUTING SCIENCE

CALGARY, ALBERTA

August, 1974

ABSTRACT

In his 1900 address before the International Congress of Mathematicians [6], David Hilbert asked for an algorithm to decide of a polynomial equation, in several variables, with integer coefficients, whether or not the equation was solvable in integers. In 1970 it was shown that this, Hilbert's tenth problem, is recursively unsolvable. Yuri Matijasevič, by using results of Martin Davis, Julia Robinson and Hilary Putnam [3], gave the negative solution to the problem when he proved that *every recursively enumerable set is Diophantine* [9], [10].

DEFINITION: *A relation* $R(x_1,\ldots,x_k)$, *in non-negative integers, is Diophantine if there exists a polynomial* $P(x_1,\ldots,x_k,y_1,\ldots,y_n)$, *with integer coefficients, such that the relation* $R(x_1,\ldots,x_k)$ *holds just in case the equation* $P(x_1,\ldots,x_k,y_1,\ldots,y_n) = 0$ *is solvable in non-negative integers.*

Knowing, from Matijasevič's results, that there exist polynomials representing the Mersenne primes and the even perfect numbers, we here construct some which are simpler than would be given by following Matijasevič's constructions exactly. For example, we construct polynomials P and Q, with integer coefficiencts, satisfying

$$\alpha \text{ is a Mersenne prime} \Leftrightarrow (\exists x_1,x_2,\ldots,x_{11})_{\geq 0}\ P(\alpha,x_1,x_2,\ldots,x_{11}) = 0$$

$$\beta \text{ is an even perfect number} \Leftrightarrow (\exists y_1,y_2,\ldots,y_{12})_{\geq 0}\ Q(\beta,y_1,y_2,\ldots,y_{12}) = 0.$$

Applying the "method of Putnam" [13] we then have:

$$\alpha \text{ is a Mersenne prime} \Leftrightarrow [P = 0] \Leftrightarrow \alpha(1-P^2) = \alpha$$

$$\beta \text{ is an even perfect number} \Leftrightarrow [Q = 0] \Leftrightarrow \beta(1-Q^2) = \beta.$$

Thus, we are able to exhibit the Mersenne primes and the even perfect numbers as the positive parts of the ranges of polynomials with several variables and integer coefficients. (Note that if P and Q assume only non-negative values, as they will in our case, then they need not be squared.)

The question of the existence of odd perfect numbers remains open. We could still, however, construct a polynomial whose positive range is *all* perfect numbers, even or odd, by using the result of Matijasevič referred to above, since the function $\sigma(n)$ (the sum of the divisors of n) is recursive. The length of such a polynomial, though, would be prohibitive, as it would utilize a bounded universal quantifier. We refer the reader to [8] to see the problems involved in such a construction.

ACKNOWLEDGEMENTS

I would like to thank my supervisor, Dr. J.P. Jones, for the idea behind this thesis, as well as for his assistance and guidance throughout its preparation.

Financial support during the preparation of this work was provided by the Province of Alberta.

TABLE OF CONTENTS

CHAPTER I

PRELIMINARY NUMBER THEORY

1.0. DEFINITIONS, THE ARITHMETICAL FUNCTION σ.

For any positive integer n, define $\sigma(n)$ to be the sum of the divisors of n, including n itself.

We say n is *perfect* if $\sigma(n) = 2n$.

A number of the form $N = 2^n - 1$, n a positive integer, is called a *Mersenne number*; if N is prime, we say N is a *Mersenne prime*.

Note that if N is prime, then so is n; for if $n=kl$ $(k,l>1)$, then $2^k-1 \mid 2^n-1$.

If $n = p_1^{a_1} p_2^{a_2} \ldots p_l^{a_l}$, with p_i prime $(1 \le i \le l)$, then the divisors of n are the numbers $p_1^{b_1} p_2^{b_2} \ldots p_l^{b_l}$ where $0 \le b_i \le a_i$; $i = 1,2,\ldots,l$. Hence

$$\sigma(n) = \sum_{b_1=0}^{a_1} \sum_{b_2=0}^{a_2} \cdots \sum_{b_l=0}^{a_l} p_1^{b_1} p_2^{b_2} \cdots p_l^{b_l}$$

$$= \prod_{i=1}^{l} (1 + p_i + p_i^2 + \ldots + p_i^{a_i})$$

$$= \prod_{i=1}^{l} \left(\frac{p_i^{a_i+1} - 1}{p_i - 1} \right) . \qquad (1)$$

An arithmetical function f is called multiplicative if $(m,m') = 1 \Rightarrow f(mm') = f(m)f(m')$. It is clear from (1) that σ is multiplicative.

LEMMA 1.1. (Euclid). *If* $2^{n+1} - 1$ *is prime, then* $2^n(2^{n+1} - 1)$ *is perfect.*

Proof. Write $2^{n+1} - 1 = p$, $N = 2^n p$.

$$\begin{aligned} \text{Then } \sigma(N) &= \sigma(2^n)\sigma(p) \\ &= (1 + 2 + 2^2 + \ldots + 2^n)(p + 1) \\ &= (2^{n+1} - 1)(2^{n+1}) \\ &= 2N. \end{aligned}$$

LEMMA 1.2. (Euler). *Any even perfect number is of the form* $2^n(2^{n+1} - 1)$, *where* $2^{n+1} - 1$ *is prime.*

Proof. We can write any even number in the form $N = 2^n b$, where $n > 0$ and b is odd. Then

$$\sigma(N) = \sigma(2^n)\sigma(b) = (2^{n+1}-1)\sigma(b) .$$

Since N is perfect,

$$\sigma(N) = 2N = 2^{n+1}b,$$

and so

$$\frac{b}{\sigma(b)} = \frac{2^{n+1}-1}{2^{n+1}} ,$$

a fraction in its lowest terms. Thus

$$b = (2^{n+1}-1)c, \quad \sigma(b) = 2^{n+1}c ,$$

where c is an integer.

If $c > 1$, then b has at least the divisors b, c, 1, so that

$$\sigma(b) \geq b+c+1 = 2^{n+1}c+1 > 2^{n+1}c = \sigma(b) \quad ,$$

a contradiction.

Hence $c = 1$, $N = 2^n(2^{n+1}-1)$, and $\sigma(2^{n+1}-1) = 2^{n+1}$. But, if $2^{n+1}-1$ is not prime, it has divisors other than itself and 1, and $\sigma(2^{n+1}-1) > 2^{n+1}$. Hence $2^{n+1}-1$ is prime, and the lemma is proved.

From Lemmas 1.1 and 1.2, we see that β is an even perfect number if and only if it is of the form $\alpha(\alpha+1)/2$, where α is a Mersenne prime.

In order to prove the major theorem of this section (Theorem 1.26) we must develop some facts concerning congruences and residues. The proofs are those given in [5].

We denote by $\phi(m)$ (Euler's ϕ) the number of positive integers not greater than and prime to m. If a is prime to m, then so is any number x congruent to $a \pmod{m}$. There are $\phi(m)$ classes of residues prime to m, and any set of $\phi(m)$ residues, one from each class, is called a *complete set of residues prime to m*. One such complete set is the set of $\phi(m)$ numbers less than and prime to m.

LEMMA 1.3. *If* $a_1, a_2, \ldots, a_{\phi(m)}$ *is a complete set of residues prime to m, and* $(k,m) = 1$, *then*

$$ka_1, ka_2, \ldots, ka_{\phi(m)}$$

is also such a set.

Proof. The numbers of the second set are plainly all prime to m, and no two of them are congruent, for $ka_i \equiv ka_j \pmod{m}$ implies $a_i \equiv a_j \pmod{m}$.

LEMMA 1.4. (The Fermat-Euler Theorem). *If* $(a,m) = 1$, *then* $a^{\phi(m)} \equiv 1 \pmod{m}$.

Proof. If x runs through a complete system of residues prime to m, then, by Lemma 1.3, ax also runs through such a system. Hence, taking the product of each set, we have

$$\Pi(ax) \equiv \Pi x \pmod{m}$$

or

$$a^{\phi(m)}\Pi x \equiv \Pi x \pmod{m} .$$

Since every number x is prime to m, their product is prime to m; and hence

$$a^{\phi(m)} \equiv 1 \pmod{m} .$$

LEMMA 1.5. (Fermat's Theorem). *If* p *is prime, and* $p \dagger a$, *then*

$$a^{p-1} \equiv 1 \pmod{p} .$$

Proof. Put $m = p$ in Lemma 1.4.

Now, let us suppose that p is an odd prime, that $p \dagger a$, and that x is one of the numbers

$$1,2,3,\ldots,p-1.$$

Then, by Lemma 1.3, just one of the numbers

$$1\cdot x, 2\cdot x, \ldots, (p-1)x$$

is congruent to $a \pmod{p}$. There is therefore a unique x' such that

$$xx' \equiv a(\text{mod } p), \quad 0 < x' < p \ .$$

We call x' the associate of x. There are then two possibilities: either there is at least one x associated with itself, so that $x' = x$, or there is no such x.

(i) Suppose that the first alternative is the true one and that x_1 is associated with itself. In this case the congruence

$$x^2 \equiv a(\text{mod } p)$$

has the solution $x = x_1$; and we say that a is a *quadratic residue* of p, or (when there is no danger of a misunderstanding) simply a *residue* of p. Plainly

$$x = p-x_1 \equiv -x_1(\text{mod } p)$$

is another solution of the congruence. Also, if $x' = x$ for any other value x_1 of x, we have

$$x_1^2 \equiv a, \quad x_2^2 \equiv a, \quad (x_1-x_2)(x_1+x_2) = x_1^2-x_2^2 \equiv 0(\text{mod } p) \ .$$

Hence either $x_2 \equiv x_1$ or

$$x_2 \equiv -x_1 \equiv p-x_1;$$

and there are just two solutions of the congruence, namely x_1 and $p-x_1$.

In this case the numbers

$$1,2,\ldots,p-1$$

may be grouped as x_1, $p-x_1$, and $\frac{1}{2}(p-3)$ pairs of unequal associated numbers.

Now

$$x_1(p-x_1) \equiv -x_1^2 \equiv -a(\text{mod } p) ,$$

while $$xx' \equiv a(\text{mod } p)$$

for any associated pair x, x'. Hence

$$(p-1)! = \Pi x \equiv -a\cdot a^{\frac{1}{2}(p-3)} \equiv -a^{\frac{1}{2}(p-1)}(\text{mod } p) .$$

(ii) If the second alternative is true and no x is associated with itself, we say a is a *quadratic non-residue* of p, or simply a *non-residue* of p. In this case the congruence

$$x^2 \equiv a(\text{mod } p)$$

has no solution, and the numbers

$$1,2,\ldots,p-1$$

may be arranged in $\frac{1}{2}(p-1)$ associated pairs. Hence

$$(p-1)! = \Pi x \equiv a^{\frac{1}{2}(p-1)}(\text{mod } p) .$$

We define 'Legendre's symbol' $\left(\frac{a}{p}\right)$, where p is an odd prime and a is any number not divisible by p, by

$$\left(\frac{a}{p}\right) = +1, \text{ if } a \text{ is a residue of } p,$$

$$\left(\frac{a}{p}\right) = -1, \text{ if } a \text{ is a non-residue of } p.$$

It is plain that $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$ if $a \equiv b(\text{mod } p)$. We have thus proved

LEMMA 1.6. *If p is an odd prime and a is not a multiple of p, then*

$$(p-1)! \equiv -\left(\frac{a}{p}\right) a^{\frac{1}{2}(p-1)} \pmod{p} .$$

LEMMA 1.7. (Wilson's Theorem). $(p-1)! \equiv -1 \pmod{p}$.

Proof. The congruence

$$x^2 \equiv 1 \pmod{p}$$

has the solutions $x = \pm 1$, hence

$$\left(\frac{1}{p}\right) = 1 .$$

Put $a = 1$ in Lemma 1.6.

LEMMA 1.8. $\left(\frac{a}{p}\right) \equiv a^{\frac{1}{2}(p-1)} \pmod{p}$.

Proof. From Lemmas 1.6 and 1.7,

$$-1 \equiv -\left(\frac{a}{p}\right) a^{\frac{1}{2}(p-1)} \pmod{p} .$$

Multiplying by $-a^{\frac{1}{2}(p-1)}$ gives

$$a^{\frac{1}{2}(p-1)} \equiv \left(\frac{a}{p}\right) a^{p-1} \pmod{p} ,$$

and the result follows by Lemma 1.5.

LEMMA 1.9. (Gauss's Lemma). $\left(\frac{m}{p}\right) = (-1)^{\mu}$, *where μ is the number of members of the set*

$$m, 2m, 3m, \ldots, \tfrac{1}{2}(p-1)m,$$

whose least positive residues (mod p) *are greater than* $\frac{1}{2}p$.

Proof. Note that 'residue' here has its usual meaning and is not an abbreviation for 'quadratic residue'. If p is an odd prime, there is just one residue of $n(\bmod p)$ between $-\frac{1}{2}p$ and $\frac{1}{2}p$. We call this residue the *minimal* residue of $n(\bmod p)$; it is positive or negative according as the least non-negative residue of n lies between 0 and $\frac{1}{2}p$ or between $\frac{1}{2}p$ and p.

We now suppose that m is an integer, positive or negative, not divisible by p, and consider the minimal residues of the $\frac{1}{2}(p-1)$ numbers

$$m, 2m, 3m, \ldots, \tfrac{1}{2}(p-1)m \ . \qquad (2)$$

We can write these residues in the form

$$r_1, r_2, \ldots, r_\lambda, -r'_1, -r'_2, \ldots, -r'_\mu,$$

where $\lambda + \mu = \frac{1}{2}(p-1)$, $0 < r_i < \frac{1}{2}p$, $0 < r'_i < \frac{1}{2}p$.

Since the numbers (2) are incongruent, no two r can be equal, and no two r'. If an r and an r' are equal, say $r_i = r'_j$, let am, bm be the two of the numbers (2) such that

$$am \equiv r_i \, , \ bm \equiv -r'_j \pmod p \ .$$

Then
$$am + bm \equiv 0 (\bmod p) \ ,$$

and so
$$a + b \equiv 0 (\bmod p) \ ,$$

which is impossible because $0 < a < \frac{1}{2}p$, $0 < b < \frac{1}{2}p$.

It follows that the numbers r_i, r'_j are a rearrangement of the numbers

$$1,2,\ldots,\tfrac{1}{2}(p-1)\ ,$$

and therefore that

$$m\cdot 2m\cdot\ldots\cdot\tfrac{1}{2}(p-1)m \equiv (-1)^{\mu}1\cdot 2\cdot\ldots\cdot\tfrac{1}{2}(p-1)\,(\mathrm{mod}\ p)$$

and so $$m^{\frac{1}{2}(p-1)} \equiv (-1)^{\mu}(\mathrm{mod}\ p)\ .$$

But $\left(\frac{m}{p}\right) \equiv m^{\frac{1}{2}(p-1)}(\mathrm{mod}\ p)$ by Lemma 1.8.

LEMMA 1.10. *2 is a quadratic residue of primes of the form $8n \pm 1$ and a quadratic non-residue of primes of the form $8n \pm 3$.*

Proof. Take $m = 2$ in Lemma 1.9. Then the numbers (2) are

$$2,4,\ldots,p-1\ .$$

In this case λ is the number of positive even integers less than $\tfrac{1}{2}p$.

We write $[x]$ for the largest integer which does not exceed x. With this notation,

$$\lambda = [\tfrac{1}{4}p]\ .$$

But $\lambda + \mu = \tfrac{1}{2}(p-1)$,

and so $$\mu = \tfrac{1}{2}(p-1) - [\tfrac{1}{4}p]\ .$$

If $p \equiv 1(\mathrm{mod}\ 4)$, then

$$\mu = \tfrac{1}{2}(p-1) - \tfrac{1}{4}(p-1) = \tfrac{1}{4}(p-1) = [\tfrac{1}{4}(p+1)]\ ,$$

and if $p \equiv 3 \pmod 4$, then

$$\mu = \tfrac{1}{2}(p-1) - \tfrac{1}{4}(p-3) = \tfrac{1}{4}(p+1) = [\tfrac{1}{4}(p+1)] .$$

Hence
$$\left(\frac{2}{p}\right) \equiv (-1)^{[\frac{1}{4}(p+1)]} \pmod p ,$$

that is to say
$$\left(\frac{2}{p}\right) = 1, \quad \text{if } p = 8n \pm 1,$$

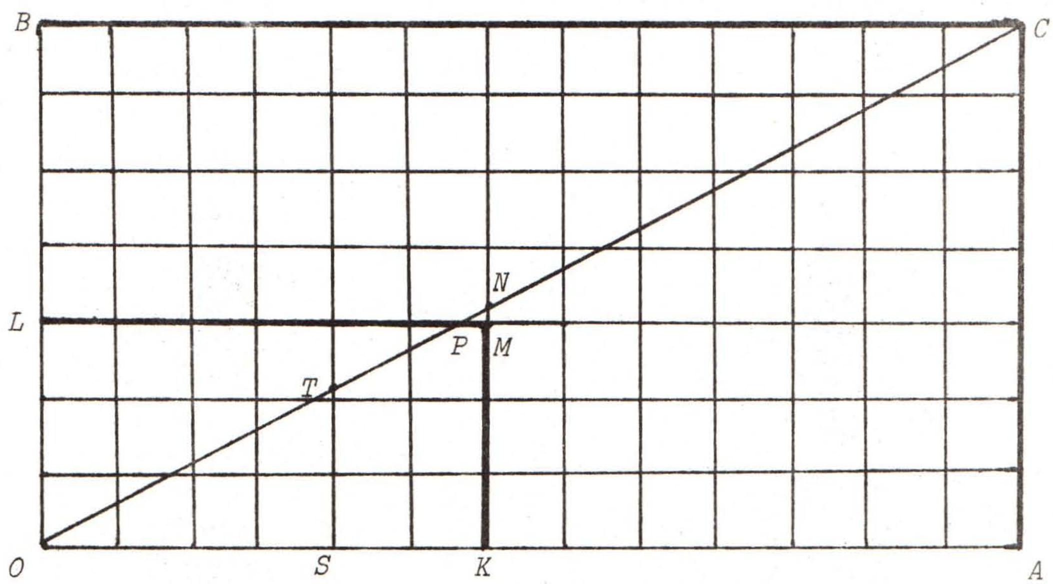
$$\left(\frac{2}{p}\right) = -1, \quad \text{if } p = 8n \pm 3.$$

LEMMA 1.11. *If p and q are distinct odd primes, if $p' = \frac{1}{2}(p-1)$, $q' = \frac{1}{2}(q-1)$, and if*

$$S(q,p) = \sum_{s=1}^{p'} \left[\frac{sq}{p}\right] ,$$

then $S(q,p) + S(p,q) = p'q'$.

Proof.



The proof may be stated in a geometrical form. In the figure, AC and BC are $x = p$, $y = q$, and KM and LM are $x = p'$, $y = q'$. If (as in the figure) $p > q$, then $q'/p' < q/p$, and M falls below the diagonal OC.

Since
$$q' < \frac{qp'}{p} < q'+1 ,$$
there is no integer between $KM = q'$ and $KN = qp'/p$.

We count up, in two different ways, the number of lattice points in the rectangle $OKML$, counting the points on KM and LM but not those on the axes. In the first place, this number is plainly $p'q'$. But there are no lattice points on OC (since p and q are prime), and none in the triangle PMN except perhaps on PM. Hence the number of lattice points in $OKML$ is the sum of those in the triangles OKN and OLP (counting those on KN and LP but not those on the axes).

The number on ST, the line $x = s$, is $[sq/p]$, since sq/p is the ordinate of T. Hence the number in OKN is
$$\sum_{s=1}^{p'} \left[\frac{sq}{p}\right] = S(q,p) .$$

Similarly, the number in OLP is $S(p,q)$, and the conclusion follows.

LEMMA 1.12. (Gauss's Law of Reciprocity). *If* p *and* q *are distinct odd primes, then*
$$\left(\frac{p}{q}\right) \left(\frac{q}{p}\right) = \left(-1\right)^{p'q'} .$$

Proof. We can write

$$kq = p\left[\frac{kq}{p}\right] + U_k\,, \tag{3}$$

where $$1 \le k \le p',\quad 1 \le U_k \le p-1.$$

Here U_k is the least positive residue of $kq \pmod p$. If $U_k = V_k \le p'$, then U_k is one of the minimal residues r_i of Lemma 1.9, while if $U_k = W_k > p'$, then U_k-p is one of the minimal residues $-r'_j$. Thus

$$r_i = V_k,\quad r'_j = p-W_k$$

for every i, j, and some k.

The r_i and r'_j are, as we saw in Lemma 1.9, the numbers $1,2,\ldots,p'$ in some order. Hence, if

$$R = \sum r_i = \sum V_k,\quad R' = \sum r'_j = \sum(p-W_k) = \mu p - \sum W_k$$

(where μ is, as in Lemma 1.9, the number of the r'_j), we have

$$R + R' = \sum_{\nu=1}^{p'} \nu = \frac{1}{2}\,\frac{p-1}{2}\,\frac{p+1}{2} = \frac{p^2-1}{8}\,,$$

and so

$$\mu p + \sum V_k - \sum W_k = \tfrac{1}{8}(p^2-1)\,. \tag{4}$$

On the other hand, summing (3) from $k = 1$ to $k = p'$, we have

$$\tfrac{1}{8}q(p^2-1) = pS(q,p) + \sum U_k = pS(q,p) + \sum V_k + \sum W_k\,. \tag{5}$$

From (4) and (5) we deduce

$$\tfrac{1}{8}(p^2-1)(q-1) = pS(q,p) + 2\sum W_k - \mu p \,. \tag{6}$$

Now $q-1$ is even, and $p^2-1 \equiv 0 \pmod 8$ (If $p = 2n+1$ then $p^2-1 = 4n(n+1) \equiv 0 \pmod 8$), so that the left hand side of (6) is even, and also the second term on the right. Hence (since p is odd)

$$S(q,p) \equiv \mu \pmod 2 \,,$$

and therefore, by Lemma 1.9,

$$\left(\frac{q}{p}\right) = (-1)^{\mu} = (-1)^{S(q,p)} \,.$$

Finally,
$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{S(q,p)+S(p,q)} = (-1)^{p'q'} \,,$$

by Lemma 1.11.

LEMMA 1.13. *If p and q are odd primes, then*

$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)$$

unless both p and q are of the form $4n + 3$, in which case

$$\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right) \,.$$

Proof. Immediate from Lemma 1.12.

The proof of Theorem 1.26 will utilize some basic properties of two sequences of integers, which we now develop.

1.14. DEFINITIONS.

Let

$$a = 1 + \sqrt{3}, \qquad b = 1 - \sqrt{3}$$

so that

$$a + b = 2, \qquad ab = -2, \qquad a - b = 2\sqrt{3}.$$

We define two sequences of integers U_r and V_r by

$$U_r = (a^r - b^r)/a-b$$

$$V_r = a^r + b^r$$

LEMMA 1.15. (i) $U_1=1,\ U_2=2,\ U_{r+2}=2U_{r+1}+2U_r \quad (r \geq 0)$.

(ii) $V_1=2,\ V_2=8,\ V_{r+2}=2V_{r+1}+2V_r \quad (r \geq 0)$.

Proof. (i) The first two equalities are easily verified, and for $r \geq 0$,

$$U_{r+2} = \frac{a^{r+2}-b^{r+2}}{a-b}$$

$$= \frac{a^r(4+2\sqrt{3})-b^r(4-2\sqrt{3})}{a-b}$$

$$= \frac{2\ (a^r-b^r)}{a-b} + \frac{2(1+\sqrt{3})a^r-2(1-\sqrt{3})b^r}{a-b}$$

$$= 2U_r + 2U_{r+1} .$$

(ii) is similar.

LEMMA 1.16. $2U_{r+s} = U_rV_s + V_rU_s$.

Proof.

$$U_rV_s + V_rU_s = \frac{(a^r-b^r)(a^s+b^s)}{a-b} + \frac{(a^r+b^r)(a^s-b^s)}{a-b}$$

$$= \frac{2\ (a^{r+s}-b^{r+s})}{a-b}$$

$$= 2U_{r+s}\ .$$

LEMMA 1.17. $(-2)^{s+1}U_{r-s} = U_sV_r - U_rV_s\ . \qquad (r > s)$

Proof.

$$U_sV_r - U_rV_s = \frac{(a^s-b^s)(a^r+b^r)}{a-b} - \frac{(a^r-b^r)(a^s+b^s)}{a-b}$$

$$= \frac{-2\ (a^rb^s-a^sb^r)}{a-b}$$

$$= \frac{-2a^sb^s\ (a^{r-s}-b^{r-s})}{a-b}$$

$$= (-2)^{s+1}U_{r-s}\ .$$

LEMMA 1.18. $2V_{r+s} = V_rV_s + 12U_rU_s\ .$

Proof.

$$V_rV_s + 12U_rU_s = (a^r+b^r)(a^s+b^s) + \frac{12(a^r-b^r)(a^s-b^s)}{(a-b)^2}$$

$$= 2(a^{r+s}+b^{r+s})$$

$$= 2V_{r+s}\ .$$

LEMMA 1.19. $U_{2r} = U_r V_r$.

Proof.

$$U_r V_r = \frac{(a^r-b^r)(a^r+b^r)}{a-b}$$

$$= \frac{a^{2r}-b^{2r}}{a-b}$$

$$= U_{2r} \ .$$

LEMMA 1.20. $V_{2r} = V_r^2 + (-2)^{r+1}$.

Proof.

$$V_{2r} - V_r^2 = (a^{2r}+b^{2r}) - (a^r+b^r)^2$$

$$= -2(ab)^r$$

$$= (-2)^{r+1} \ .$$

LEMMA 1.21. $V_r^2 - 12U_r^2 = (-2)^{r+2}$.

Proof.

$$V_r^2 - 12U_r^2 = (a^r+b^r)^2 - \frac{12(a^r-b^r)^2}{(a-b)^2}$$

$$= 4(ab)^r$$

$$= (-2)^{r+2} \ .$$

1.22. DEFINITION. The rank of apparition of the odd prime p is the least positive subscript ω (if it exists) for which U_ω is divisible by p.

LEMMA 1.23. *If ω is the rank of apparition of p, then for any r, p divides*

U_r *if and only if* ω *divides* r.

Proof. Let S be the set of all subscripts r for which p divides U_r. From Lemmas 1.16 and 1.17 it follows that if r and s are members of S, so also are $r \pm s$. Hence S coincides with the set of all integer multiples of its least positive member ω.

LEMMA 1.24. (i) $U_p \equiv \left(\frac{3}{p}\right) (\text{mod } p)$. $(p > 3)$

(ii) $V_p \equiv 2 (\text{mod } p)$.

Proof. To prove (i) we expand U_p as follows:

$$U_p = \frac{1}{2\sqrt{3}}\{(1+\sqrt{3})^p - (1-\sqrt{3})^p\} = \sum_{k=0}^{\frac{1}{2}(p-1)} \binom{p}{2k+1} 3^k.$$

All the binomial coefficients are divisible by p, except the last which is equal to unity. Hence

$$U_p \equiv 3^{\frac{1}{2}(p-1)} \equiv \left(\frac{3}{p}\right) (\text{mod } p)$$

by Lemma 1.8.

To prove (ii) we expand V_p in like manner, thus

$$V_p = (1+\sqrt{3})^p + (1-\sqrt{3})^p = 2\sum_{k=0}^{\frac{1}{2}(p-1)} \binom{p}{2k} 3^k.$$

In this case all the binomial coefficients except the first are divisible by p. Hence (ii) follows at once.

LEMMA 1.25. *For any odd prime p, the rank of apparition of p exists and* *is* $\leq p+1$.

Proof. For $p = 3$ the result holds, since $3 | U_3$. Thus assume $p > 3$.

It is obviously sufficient to prove that p divides $U_{p+1}U_{p-1}$. From Lemmas 1.15, 1.16 and 1.17 we have

$$2U_{p+1} = 2U_p+V_p,$$

$$-4U_{p-1} = 2U_p-V_p.$$

Using Lemma 1.24, we have

$$\begin{aligned} -8U_{p+1}U_{p-1} &= 4U_p^2 - V_p^2 \\ &\equiv 4(\pm 1)^2 - 4 \\ &\equiv 0 \pmod{p}. \end{aligned}$$

THEOREM 1.26. (D.H. Lehmer, [9]). *The number* $N = 2^n-1$, *where* $n > 2$, *is a prime if, and only if,* N *divides the* $(n-1)$*-st term of the sequence*

$$S_1=4,\ S_2=14,\ S_3=194,\ \ldots,\ S_k,\ \ldots,$$

where $S_k = S_{k-1}^2-2$.

Proof. Let $N = 2^n-1$ be prime, $n > 2$. Then n is an odd prime. We have to show that S_{n-1} is divisible by N. Instead of the series S_k we may consider the series

$$8,\ 56, 3104, \ldots, \sigma_k, \ldots,$$

in which $\sigma_k = 2^{2^{k-1}} S_k$. Then it is sufficient to show that σ_{n-1} is divisible by N. Since

$$S_{k+1} = S_k^2 - 2 ,$$

we have $\sigma_{k+1} = \sigma_k^2 - 2^{2^k+1}$. By Lemma 1.20, with $r = 2^k$, we see that

$$V_{2^{k+1}} = V_{2^k}^2 - 2^{2^k+1} .$$

Moreover $V_2 = 8 = \sigma_1$. Hence, in general,

$$\sigma_k = V_{2^k}.$$

We have to show then that $V_{2^{n-1}} = V_{\frac{1}{2}(N+1)}$ is divisible by N. But from Lemma 1.20, with $r = \frac{1}{2}(N+1)$, we have

$$V_{N+1} = V_{\frac{1}{2}(N+1)}^2 - 4 \cdot 2^{\frac{1}{2}(N-1)} .$$

Therefore,

$$\begin{aligned} V_{\frac{1}{2}(N+1)}^2 &= V_{N+1} + 4 \cdot 2^{\frac{1}{2}(N-1)} \\ &\equiv V_{N+1} + 4\left(\frac{2}{N}\right) \pmod N \text{ by Lemma 1.8.} \\ &\equiv V_{N+1} + 4 \pmod N \text{ by Lemma 1.10.} \end{aligned}$$

Hence it is sufficient to show that

$$V_{N+1} \equiv -4 \pmod N . \qquad (7)$$

But (7) follows from Lemmas 1.24 and 1.18. In fact

$$2V_{N+1} = 2V_N + 12U_N .$$

To apply Lemma 1.24 with $p = N$, we note that $N \equiv 1 \pmod 3$ since n is odd,

and that
$$\left(\frac{3}{N}\right) = -\left(\frac{N}{3}\right) \text{ by Lemma 1.13}$$
$$= -\left(\frac{1}{3}\right)$$
$$= -1 \text{ by Lemma 1.8.}$$

Hence we have
$$V_{N+1} = V_N + 6U_N \equiv 2 - 6 \equiv -4 (\text{mod } N).$$

Hence (7) is established, and $N | S_{n-1}$.

Conversely, let S_{n-1} be divisible by $N = 2^n - 1$. Then N divides $\sigma_{n-1} = 2^{2n-2} S_{n-1} = V_{2^{n-1}}$. Now let p be any prime factor of N and let ω be the rank of apparition of p. Then p divides U_{2^n} since N divides $U_{2^{n-1}} V_{2^{n-1}}$, which is U_{2^n} by Lemma 1.19. By Lemma 1.23, ω divides 2^n. On the other hand, ω does not divide 2^{n-1}, for otherwise, by Lemma 1.23, p would divide $U_{2^{n-1}}$ as well as $V_{2^{n-1}}$. This is impossible by Lemma 1.21 since p is odd. Hence $\omega = 2^n$. By Lemma 1.25,
$$p \geq \omega - 1 = 2^n - 1 = N .$$

Hence $p = N$, so that N is prime.

The following theorem will be needed in Chapter II:

THEOREM 1.27. *If $N > 0$ and is not a perfect square, then the Pell equation*
$$x^2 - Ny^2 = 1$$
has infinitely many solutions in integers x, y.

Before proving Theorem 1.27, we develop some facts about continued fractions, using proofs given in [1] and [5]. We shall describe the function

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cdots + \cfrac{1}{a_N}}} \qquad (8)$$

of the $N+1$ variables

$$a_0,\ a_1,\ \ldots,\ a_n,\ \ldots,\ a_N$$

as a *finite continued fraction*, or, when there is no risk of ambiguity, simply as a *continued fraction*. Rather than use the notation (8), we shall usually write the continued fraction in one of the two forms

$$a_0 + \frac{1}{a_1+}\ \frac{1}{a_2+}\ \cdots\ \frac{1}{a_N}\ ,$$

or

$$[a_0, a_1, \ldots, a_N]\ .$$

We call $a_0, a_1, \ldots, a_N$ the *partial quotients*, or simply the *quotients*, of the continued fraction.

We find by calculation that

$$[a_0] = \frac{a_0}{1},\ [a_0, a_1] = \frac{a_1 a_0 + 1}{a_1}$$

and it is plain that

$$[a_0, a_1, \ldots, a_n] = [a_0, a_1, \ldots, a_{n-2}, a_{n-1} + \frac{1}{a_n}] \qquad (9)$$

and that

$$[a_0,a_1,\ldots,a_n] = [a_0,a_1,\ldots,a_{m-1},[a_m,a_{m+1},\ldots,a_n]] \tag{10}$$

for $1 \le m < n \le N$. We call

$$[a_0,a_1,\ldots,a_n] \quad (0 \le n \le N)$$

the n^{th} *convergent* to $[a_0,a_1,\ldots,a_N]$.

LEMMA 1.28. *If* p_n *and* q_n *are defined by*

$$p_0=a_0,\ p_1=a_1a_0+1,\ p_n=a_np_{n-1}+p_{n-2} \quad (2 \le n \le N) \tag{11}$$

$$q_0=1,\ \ q_1=a_1, \qquad q_n=a_nq_{n-1}+q_{n-2} \quad (2 \le n \le N) \tag{12}$$

then

$$[a_0,a_1,\ldots,a_n] = \frac{p_n}{q_n}.$$

Proof. We have already verified the lemma for $n = 0$ and $n = 1$. Let us suppose it to be true for $n \le m$, where $m < N$. Then

$$[a_0,a_1,\ldots,a_{m-1},a_m] = \frac{p_m}{q_m} = \frac{a_mp_{m-1} + p_{m-2}}{a_mq_{m-1} + q_{m-2}},$$

and p_{m-1}, p_{m-2}, q_{m-1}, q_{m-2} depend only on

$$a_0,\ a_1,\ldots,a_{m-1}.$$

Hence, using (9), we obtain

$$[a_0,a_1,\ldots,a_{m-1},a_m,a_{m+1}] = \left[a_0,a_1,\ldots,a_{m-1},a_m+\frac{1}{a_{m+1}}\right]$$

$$= \frac{\left(a_m+\frac{1}{a_{m+1}}\right)p_{m-1}+p_{m-2}}{\left(a_m+\frac{1}{a_{m+1}}\right)q_{m-1}+q_{m-2}}$$

$$= \frac{a_{m+1}(a_m p_{m-1}+p_{m-2})+p_{m-1}}{a_{m+1}(a_m q_{m-1}+q_{m-2})+q_{m-1}}$$

$$= \frac{a_{m+1}p_m+p_{m-1}}{a_{m+1}q_m+q_{m-1}}$$

$$= \frac{p_{m+1}}{q_{m+1}}$$

and the lemma is proved by induction.

It follows from (11) and (12) that

$$p_n q_{n-1} - p_{n-1}q_n = (a_n p_{n-1} + p_{n-2})q_{n-1} - p_{n-1}(a_n q_{n-1} + q_{n-2})$$

$$= -(p_{n-1}q_{n-2} - p_{n-2}q_{n-1}) .$$

Repeating the argument with $n-1, n-2, \ldots, 2$ in place of n, we obtain

$$p_n q_{n-1} - p_{n-1}q_n = (-1)^{n-1}(p_1 q_0 - p_0 q_1) = (-1)^{n-1} . \tag{13}$$

Now, let α be any irrational number. Let a_0 be the integral part of α. Then

$$\alpha = a_0 + \alpha' ,$$

where $0 < \alpha' < 1$. Put

$$\alpha' = \frac{1}{\alpha_1},$$

then
$$\alpha = a_0 + \frac{1}{\alpha_1}$$

where $\alpha_1 > 1$ and is irrational. Now repeat the operation on α_1, expressing it as

$$\alpha_1 = a_1 + \frac{1}{\alpha_2},$$

where $\alpha_2 > 1$. We can continue this process indefinitely. Having reached α_n, itself an irrational number greater than 1, we can express it as

$$\alpha_n = a_n + \frac{1}{\alpha_{n+1}},$$

where $\alpha_{n+1} > 1$, and a_n is a natural number. If we combine all the equations up to this one, we obtain for α the expression

$$\alpha = a_0 + \frac{1}{a_1 +}\;\frac{1}{a_2 +}\;\cdots\;\frac{1}{a_n +}\;\frac{1}{\alpha_{n+1}}.$$

The numbers a_0, a_1, ... are called, as before, the partial quotients of the continued fraction, and the *complete* quotient corresponding to a_n is α_n, or, what is the same thing, $a_n + \frac{1}{\alpha_{n+1}}$. The process can never come to an end, because each complete quotient is an irrational number.

Then by Lemma 1.29,

$$\alpha = \frac{\alpha_{n+1}p_n + p_{n-1}}{\alpha_{n+1}q_n + q_{n-1}}. \tag{14}$$

LEMMA 1.29. *With the above notation,*

$$\frac{p_n}{q_n} \to \alpha \text{ as } n \to \infty.$$

Proof. Equation (14) gives

$$\alpha - \frac{p_n}{q_n} = \frac{\alpha_{n+1}p_n+p_{n-1}}{\alpha_{n+1}q_n+q_{n-1}} - \frac{p_n}{q_n} = \frac{p_{n-1}q_n - q_{n-1}p_n}{q_n(\alpha_{n+1}q_n+q_{n-1})}$$

$$= \frac{\pm 1}{q_n(\alpha_{n+1}q_n+q_{n-1})}$$

using (13). Since $\alpha_{n+1} > a_{n+1}$, we have

$$\left|\alpha - \frac{p_n}{q_n}\right| < \frac{1}{q_n q_{n+1}} \to 0 \text{ as } n \to \infty . \quad (\text{since } q_n \geq n)$$

By a *quadratic irrational* we shall mean an (irrational) number which arises as a solution of a quadratic equation with integral coefficients. In particular, the square root of any natural number N, not a perfect square, is a quadratic irrational. If α is a quadratic irrational, then we denote by α' the second root of the quadratic equation satisfied by α, and call α' the *algebraic conjugate* of α, or simply the *conjugate* of α. If $\alpha > 1$ and $-1 < \alpha' < 0$, then we say that α is *reduced.*

An infinite continued fraction of the form

$$a_0 + \frac{1}{a_1+}\,\frac{1}{a_2+}\,\cdots\,\frac{1}{a_n+}\,\frac{1}{a_0+}\,\frac{1}{a_1+}\,\cdots ,$$

which is periodic from the beginning, is called *purely periodic.*

LEMMA 1.30. *If α is a reduced quadratic irrational, then the continued fraction for α is purely periodic.*

Proof. We know that α satisfies some quadratic equation

$$A\alpha^2 + B\alpha + C = 0 ,$$

where A, B, C are integers. Solving this equation, we can express α in the form

$$\alpha = \frac{-B \pm \sqrt{B^2-4AC}}{2A} = \frac{P \pm \sqrt{D}}{Q} ,$$

where P and Q are integers, and D is a positive integer which is not a perfect square. We can suppose that the + sign is attached to $\sqrt{D}$, for if it were the - sign, we could change it to the + sign by changing the signs of both the numbers P and Q. So

$$\alpha = \frac{P+\sqrt{D}}{Q}, \qquad \alpha' = \frac{P-\sqrt{D}}{Q} .$$

We note that

$$\frac{P^2-D}{Q} = \frac{B^2-(B^2-4AC)}{2A} = 2C,$$

so that P^2-D is a multiple of Q.

Since α is reduced, we have $\alpha > 1$ and $-1 < \alpha' < 0$. This means that

(i) $\alpha - \alpha' > 0$, that is $\frac{\sqrt{D}}{Q} > 0$, whence $Q > 0$;

(ii) $\alpha + \alpha' > 0$, that is $\frac{P}{Q} > 0$, whence $P > 0$;

(iii) $\alpha' < 0$, that is $P < \sqrt{D}$;

(iv) $\alpha > 1$, that is $Q < P+\sqrt{D} < 2\sqrt{D}$.

Thus a reduced quadratic irrational number α is of the form

$$\frac{P + \sqrt{D}}{Q} ,$$

where

$$P < \sqrt{D} \text{ and } Q < 2\sqrt{D} \ , \tag{15}$$

and also satisfies the condition that P^2-D is a multiple of Q.

Now let α be developed into a continued fraction. The first step in the process of development is to express α in the form

$$\alpha = a_0 + \frac{1}{\alpha_1} \ , \tag{16}$$

where a_0 is the integral part of α_1 and $\alpha_1 > 1$. It is easy to see that α_1 is again a reduced quadratic irrational, for the equation (16) implies that the conjugates of α and α_1 are connected by the similar relation

$$\alpha' = a_0 + \frac{1}{\alpha'_1} \ .$$

So

$$\alpha'_1 = -\frac{1}{a_0-\alpha'} \ ,$$

and since α' is negative, and a_0 is a natural number, we have $a_0 - \alpha' > 1$, and therefore α'_1 lies between -1 and 0. Similarly, all the subsequent complete quotients α_2, α_3, ... in the development are reduced quadratic irrationals.

As regards the form of α_1 we have

$$\frac{1}{\alpha_1} = \alpha - a_0 = \frac{P+\sqrt{D}}{Q} - a_0 = \frac{P-Qa_0+\sqrt{D}}{Q} \ .$$

Let $P_1 = -P+Qa_0$. Then

$$\alpha_1 = \frac{Q}{-P_1+\sqrt{D}} = \frac{P_1+\sqrt{D}}{Q_1},$$

where Q_1 is defined by

$$D - P_1^2 = QQ_1 . \tag{17}$$

Note that Q_1 is an integer, since $P^2 - D$ is a multiple of Q and $P_1 \equiv -P(\text{mod } Q)$. We have

$$\alpha_1 = \frac{P_1+\sqrt{D}}{Q_1},$$

and since α_1 is reduced, the integers P_1 and Q_1 are positive, and satisfy the conditions (15). Moreover $P_1^2 - D$ is a multiple of Q_1, by (17).

We are now in a position to see how the continued fraction process goes on. At the next step we start from α_1 instead of from α, but the process is just the same. Generally, each complete quotient has the form

$$\alpha_n = \frac{P_n+\sqrt{D}}{Q_n},$$

where P_n and Q_n are natural numbers which satisfy (15), and have the property that $P_n^2 - D$ is a multiple of Q_n. There are only finitely many possibilities for P_n and Q_n by (15), and eventually we must come to some pair of values which has occurred before. That is, we must come to some complete quotient which is the same as some earlier one, and from this point onwards the continued fraction is periodic.

We have still to prove that the continued fraction is *purely* periodic, that is, periodic from the beginning. To prove this, we shall show that if $\alpha_n = \alpha_m$, then $\alpha_{n-1} = \alpha_{m-1}$, and in this way we shall be able to work backwards to the beginning of the continued fraction. The proof depends on the fact that it is possible to relate the partial quotients a_n not only to the complete quotients α_n but also, in a somewhat similar way, to their conjugates. The relation between any complete quotient and the next is

$$\alpha_n = a_n + \frac{1}{\alpha_{n+1}} .$$

The same relation must connect their conjugates, so that

$$\alpha_n' = a_n + \frac{1}{\alpha_{n+1}'} .$$

Since each conjugate lies between -1 and 0, let us introduce the symbol β_n for $\frac{-1}{\alpha_n'}$. Then each of the numbers β_n is greater than 1. The last relation takes the form

$$-\frac{1}{\beta_n} = a_n - \beta_{n+1}, \text{ or } \beta_{n+1} = a_n + \frac{1}{\beta_n} .$$

It now follows from the last relation that a_n, in addition to being the integral part of α_n, can also be interpreted as being the integral part of β_{n+1}.

Now suppose that α_n and α_m are two equal complete quotients, where $m < n$. Then their conjugates α_n' and α_m' are also equal, and therefore $\beta_n = \beta_m$. By the result just proved, a_{n-1} is the integral part of β_n, and a_{m-1} is the integral part of β_m. Hence $a_{n-1} = a_{m-1}$. But

$$\alpha_{n-1} = a_{n-1} + \frac{1}{\alpha_n}, \quad \alpha_{m-1} = a_{m-1} + \frac{1}{\alpha_m} .$$

Hence $\alpha_{n-1} = \alpha_{m-1}$. Repeating the argument, we obtain $\alpha_{n-2} = \alpha_{m-2}$, and so on until we reach the fact that α_{n-m} is the same as α itself. Putting $n-m = r$, we have

$$\alpha = a_0 + \frac{1}{a_1+} \cdots \frac{1}{a_{r-1}+} \frac{1}{\alpha} ,$$

and this shows that the continued fraction for α is purely periodic.

Now let N be a natural number which is not a square, and consider $\sqrt{N} + a_0$, where a_0 is the integral part of $\sqrt{N}$. The conjugate of this number is $-\sqrt{N} + a_0$, which lies between -1 and 0. Hence the continued fraction for $\sqrt{N} + a_0$ is purely periodic, and since it obviously begins with $2a_0$, it is of the form

$$\sqrt{N} + a_0 = 2a_0 + \frac{1}{a_1+} \frac{1}{a_2+} \cdots \frac{1}{a_n+} \frac{1}{2a_0+} \cdots$$

LEMMA 1.31. *The Pell equation*

$$x^2 - Ny^2 = 1 ,$$

where $N > 0$ and is not a square, has a solution in integers x, y with $y \neq 0$.

Proof. As above,

$$\sqrt{N} = a_0 + \frac{1}{a_1+} \frac{1}{a_2+} \cdots \frac{1}{a_n+} \frac{1}{2a_0+} \frac{1}{a_1+} \cdots .$$

Now let $\frac{p_{n-1}}{q_{n-1}}$ and $\frac{p_n}{q_n}$ be the two convergents coming immediately before the term $2a_0$, that is

$$\frac{p_{n-1}}{q_{n-1}} = a_0 + \frac{1}{a_1+} \quad \cdots \quad \frac{1}{a_{n-1}}, \quad \frac{p_n}{q_n} = a_0 + \frac{1}{a_1+} \quad \cdots \quad \frac{1}{a_n} .$$

By the formula (14), we have

$$\sqrt{N} = \frac{\alpha_{n+1}p_n+p_{n-1}}{\alpha_{n+1}q_n+q_{n-1}} , \tag{18}$$

where α_{n+1} is the complete quotient after a_n, that is

$$\alpha_{n+1} = 2a_0 + \frac{1}{a_1+} \quad \cdots = \sqrt{N} + a_0 .$$

Substituting this value for α_{n+1} in (18), we obtain

$$\sqrt{N}(\sqrt{N}+a_0)q_n + \sqrt{N}q_{n-1} = (\sqrt{N}+a_0)p_n+p_{n-1} .$$

Since $\sqrt{N}$ is irrational, and all the other numbers are integers, this equation implies the two equations

$$Nq_n = a_0p_n+p_{n-1} ,$$

$$a_0q_n + q_{n-1} = p_n .$$

These may be regarded as expressing p_{n-1} and q_{n-1} in terms of p_n and q_n:

$$p_{n-1} = Nq_n - a_0p_n, \quad q_{n-1} = p_n - a_0q_n .$$

Now substitute in (13). We obtain

$$p_n(p_n-a_0q_n) - q_n(Nq_n-a_0p_n) = (-1)^{n-1} ,$$

or $$p_n^2 - Nq_n{}^2 = (-1)^{n-1} . \tag{19}$$

Hence $x = p_n$ and $y = q_n$ provides a solution of the equation

$$x^2 - Ny^2 = (-1)^{n-1} .$$

If n is odd, we have a solution of Pell's equation. If not, we observe that the same argument would apply to the two convergents at the end of the next period. Since the term a_n, where it occurs for the second time, would be a_{2n+1} if the terms were numbered consecutively, we have to change n in (19) to $2n+1$, giving

$$p_{2n+1}^{\ 2} - Nq_{2n+1}^{\ 2} = (-1)^{2n} = 1 .$$

This completes the proof of Lemma 1.31.

Proof of Theorem 1.27. Let x_1, y_1 and x_2, y_2 be integers which satisfy

$$x^2 - Ny^2 = 1.$$

Let $x' + y'\sqrt{N} = (x_1+y_1\sqrt{N})(x_2+y_2\sqrt{N})$.

Then $x' - y'\sqrt{N} = (x_1-y_1\sqrt{N})(x_2-y_2\sqrt{N})$.

Multiplying gives $$x'^2 - Ny'^2 = (x_1^2-Ny_1^2)(x_2^2-Ny_2^2) = 1,$$

and the result follows by Lemma 1.31.

CHAPTER II

PELL'S EQUATION AND THE EXPONENTIAL RELATION

In this chapter, we develop some basic facts about a special type of Pell equation, and use them to give a Diophantine definition of the exponential relation $q = p^k$. Unless otherwise mentioned, all numbers are *non-negative* integers. The proofs of 2.1 - 2.24, 2.26, and 2.27 are essentially those in [3] and [12]. Theorem 2.25 is a generalization of a result due to J. Robinson and Y. Matijasevič, [12]. 2.28 - 2.30 are due to J. Jones, [8].

We consider the Pell equation:

$$\left.\begin{array}{l} \qquad\qquad x^2 - dy^2 = 1, \qquad x,y \geq 0 \\ \text{where } d = a^2 - 1, \qquad a > 1. \end{array}\right\} \qquad (*)$$

Note the obvious solutions to (*):

$$x = 1 \qquad y = 0$$

$$x = a \qquad y = 1.$$

LEMMA 2.0. *For any positive integer t, there is a non-zero solution to* (*) *in which $t|y$.*

Proof. We desire a solution to the equation

$$x^2 - d(zt)^2 = 1.$$

Put $N = dt^2$. Then $N > 0$ and is not a square, so the result follows immediately from Theorem 1.27.

LEMMA 2.1. *There are no integers x, y, positive, negative or zero, which satisfy* (*) *for which* $1 < x+y\sqrt{d} < a+\sqrt{d}$.

Proof. Let x,y satisfy (*). Since

$$1 = (a+\sqrt{d})(a-\sqrt{d}) = (x+y\sqrt{d})(x-y\sqrt{d}) \quad ,$$

the inequality implies (taking negative reciprocals),

$$-1 < -x+y\sqrt{d} < -a+\sqrt{d}.$$

Adding the inequalities:

$$0 < 2y\sqrt{d} < 2\sqrt{d} \quad ,$$

i.e. $0 < y < 1$, a contradiction.

LEMMA 2.2. *Let x, y and x', y' be integers, positive, negative, or zero which satisfy* (*). *Let*

$$x'' + y''\sqrt{d} = (x+y\sqrt{d})(x'+y'\sqrt{d}) \quad .$$

Then x'', y'' satisfy (*).

Proof. As in Theorem 1.27.

DEFINITION. $\chi_a(n)$, $\psi_a(n)$ are defined for $n \geq 0$, $a > 1$, by setting $\chi_a(n) + \psi_a(n)\sqrt{d} = (a+\sqrt{d})^n$.

When it is unnecessary to mention explicitly the dependence on a, we write simply $\chi(n)$, $\psi(n)$.

LEMMA 2.3 *$\chi(n)$, $\psi(n)$ satisfy* (*).

Proof. Immediate by induction using Lemma 2.2.

LEMMA 2.4. *Let x, y be a non-negative solution of* (*). *Then for some n, $x = \chi(n)$, $y = \psi(n)$.*

Proof. To begin with $x+y\sqrt{d} \geq 1$. On the other hand the sequence $(a+\sqrt{d})^n$ increases to infinity. Hence for some $n \geq 0$,

$$(a+\sqrt{d})^n \leq x+y\sqrt{d} < (a+\sqrt{d})^{n+1} .$$

If there is equality, the result is proved; so suppose otherwise:

$$\chi(n) + \psi(n)\sqrt{d} < x + y\sqrt{d} < (\chi(n)+\psi(n)\sqrt{d})(a+\sqrt{d}) .$$

Since $(\chi(n)+\psi(n)\sqrt{d})(\chi(n)-\psi(n)\sqrt{d}) = 1$, the number $\chi(n) - \psi(n)\sqrt{d}$ is positive. Hence, $1 < (x+y\sqrt{d})(\chi(n)-\psi(n)\sqrt{d}) < a+\sqrt{d}.$ But this contradicts Lemmas 2.1 and 2.2.

LEMMA 2.5. $\chi(m\pm n) = \chi(m)\chi(n) \pm d\psi(n)\psi(m)$, *and*

$$\psi(m\pm n) = \chi(n)\psi(m) \pm \chi(m)\psi(n) .$$

Proof.

$$\begin{aligned}\chi(m+n) + \psi(m+n)\sqrt{d} &= (a+\sqrt{d})^{m+n} \\ &= (\chi(m)+\psi(m)\sqrt{d})(\chi(n)+\psi(n)\sqrt{d}) \\ &= \big(\chi(m)\chi(n)+d\psi(n)\psi(m)\big) + \big(\chi(n)\psi(m)+\chi(m)\psi(n)\big)\sqrt{d} .\end{aligned}$$

Hence,

$$\chi(m+n) = \chi(m)\chi(n) + d\psi(n)\psi(m)$$

$$\psi(m+n) = \chi(n)\psi(m) + \chi(m)\psi(n) .$$

Similarly, $(\chi(m-n)+\psi(m-n)\sqrt{d})(\chi(n)+\psi(n)\sqrt{d}) = \chi(m) + \psi(m)\sqrt{d}.$ So

$$\chi(m-n) + \psi(m-n)\sqrt{d} = (\chi(m)+\psi(m)\sqrt{d})(\chi(n)-\psi(n)\sqrt{d}) ,$$

and one proceeds as above.

LEMMA 2.6. $\chi(2n) = 2\chi^2(n) - 1$, $\psi(2n) = 2\chi(n)\psi(n)$.

Proof. Immediate from Lemma 2.5 and the defining condition $d\psi^2(n) = \chi^2(n)-1$.

LEMMA 2.7. $\psi(m\pm 1) = a\psi(m) \pm \chi(m)$, *and* $\chi(m\pm 1) = a\chi(m) \pm d\psi(m)$.

Proof. Take $n = 1$ in Lemma 2.5.

LEMMA 2.8. $\bigl(\chi(n),\psi(n)\bigr) = 1.$

Proof. If $t\,|\,\chi(n)$ and $t\,|\,\psi(n)$, then $t\,|\,\chi^2(n) + d\psi^2(n)$, i.e., $t\,|\,1$.

LEMMA 2.9. $\psi(n)\,|\,\psi(nk) \qquad (n,k > 0).$

Proof. Obvious when $k=1$. Proceeding by induction, using the addition formula (Lemma 2.5),

$$\psi\bigl(n(m+1)\bigr) = \chi(n)\psi(nm) + \chi(nm)\psi(n) .$$

By the induction hypothesis, $\psi(n)\,|\,\psi(nm)$.

Hence, $\psi(n)\,|\,\psi\bigl(n(m+1)\bigr)$.

LEMMA 2.10. $\psi(n)\,|\,\psi(t)$ *if and only if* $n\,|\,t \qquad (n > 0)$.

Proof. Lemma 2.9 gives the implication in one direction. For the converse suppose $\psi(n)\,|\,\psi(t)$ but $n \nmid t$. So one can write $t = nq+r$, $0 < r < n$. Then,

$$\psi(t) = \chi(r)\psi(nq) + \chi(nq)\psi(r) .$$

Since $\psi(n)\,|\,\psi(nq)$, it follows that $\psi(n)\,|\,\chi(nq)\psi(r)$. But $\bigl(\psi(n),\chi(nq)\bigr) = 1$. (If $d\,|\,\psi(n), d\,|\,\chi(nq)$, then by Lemma 2.9 $d\,|\,\psi(nq)$, which by Lemma 2.8 implies $d = 1$.) Hence $\psi(n)\,|\,\psi(r)$. But, since $r < n$, we have $\psi(r) < \psi(n)$ (e.g., by Lemma 2.7). This is a contradiction.

LEMMA 2.11. $\psi(nk) \equiv k\chi^{k-1}(n)\psi(n) \bmod \psi^3(n) \qquad (n > 0)$.

Proof. $\chi(nk) + \psi(nk)\sqrt{d} = (a+\sqrt{d})^{nk}$

$$= (\chi(n)+\psi(n)\sqrt{d})^k$$

$$= \sum_{j=0}^{k} \binom{k}{j} \chi^{k-j}(n)\psi^j(n)d^{j/2}$$

So,

$$\psi(nk) = \sum_{\substack{j=1 \\ j \text{ odd}}}^{k} \binom{k}{j} \chi^{k-j}(n)\psi^j(n)d^{(j-1)/2}$$

But all terms of this expansion for which $j > 1$ are $\equiv 0 \bmod \psi^3(n)$.

LEMMA 2.12. $\psi^2(n) \mid \psi(n\psi(n))$. $(n > 0)$.

Proof. Set $k=\psi(n)$ in Lemma 2.11.

LEMMA 2.13. (First step down lemma) *If* $\psi^2(n) \mid \psi(t)$, *then* $\psi(n) \mid t$. $(n > 0)$.

Proof. By Lemma 2.10, $n \mid t$. Set $t = nk$. Using Lemma 2.11, $\psi(n)^2 \mid k\chi^{k-1}(n)\psi(n)$, i.e. $\psi(n) \mid k\chi^{k-1}(n)$. But by Lemma 2.8, $(\psi(n), \chi(n)) = 1$. So, $\psi(n) \mid k$ and hence $\psi(n) \mid t$.

LEMMA 2.14. $\chi(n+1) = 2a\chi(n) - \chi(n-1)$ *and* $\psi(n+1) = 2a\psi(n) - \psi(n-1)$.

Proof. By Lemma 2.7,

$$\chi(n+1) = a\chi(n) + d\psi(n), \qquad \psi(n+1) = a\psi(n) + \chi(n),$$

$$\chi(n-1) = a\chi(n) - d\psi(n), \qquad \psi(n-1) = a\psi(n) - \chi(n).$$

So, $\chi(n+1) + \chi(n-1) = 2a\chi(n)$, $\quad \psi(n+1) + \psi(n-1) = 2a\psi(n)$.

LEMMA 2.15. $\psi(n) \equiv n \bmod a\text{-}1$.

Proof. For $n = 0,1$ equality holds. Proceeding inductively using $a \equiv 1 \bmod a\text{-}1$:

$$\psi(n+1) = 2a\psi(n) - \psi(n-1)$$

$$\equiv 2n - (n-1) \bmod a\text{-}1.$$

LEMMA 2.16. *If $a \equiv b \bmod c$, then for all n,*

$$\chi_a(n) \equiv \chi_b(n), \qquad \psi_a(n) \equiv \psi_b(n) \bmod c.$$

Proof. For $n = 0,1$ the congruence is an equality, or is equivalent to the assumed congruence. Proceeding by induction:

$$\psi_a(n+1) = 2a\psi_a(n) - \psi_a(n-1)$$

$$\equiv 2b\psi_b(n) - \psi_b(n-1) \bmod c$$

$$= \psi_b(n+1)$$

and similarly for $\chi(n)$.

LEMMA 2.17. $\chi_a(n) - \psi_a(n)(a-y) \equiv y^n \bmod 2ay - y^2 - 1$.

Proof. $\chi(0) - \psi(0)(a-y) = 1$ and $\chi(1) - \psi(1)(a-y) = y$, so the result holds for $n=0$ and $n=1$. Using Lemma 2.14 and proceeding by induction:

$$\chi(n+1) - \psi(n+1)(a-y) = 2a[\chi(n)-\psi(n)(a-y)] - [\chi(n-1)-\psi(n-1)(a-y)]$$

$$\equiv 2ay^n - y^{n-1}$$

$$= y^{n-1}(2ay - 1)$$

$$\equiv y^{n-1}y^2$$

$$= y^{n+1} \bmod 2ay - y^2 - 1.$$

LEMMA 2.18. *For all n, $\psi(n+1) > \psi(n) \geq n$; $(2a-1)^n \leq \psi_a(n+1) \leq (2a)^n$.*

Proof. By Lemma 2.7, $\psi(n+1) > \psi(n)$. Since $\psi(0) = 0 \geq 0$, it follows by induction that $\psi(n) \geq n$ for all n.

For the second part, $\psi_a(1) = 1$ and $\psi_a(2) = 2a$. By Lemma 2.14, $(2a-1)\psi(n) \leq 2a\psi(n) - \psi(n-1) = \psi(n+1) \leq 2a\psi(n)$ and the result follows by induction.

LEMMA 2.19. *For all n, $\chi_a(n+1) > \chi_a(n) \geq a^n$; $\chi_a(n) \leq (2a)^n$.*

Proof. By Lemmas 2.7 and 2.14 $a\chi_a(n) \leq \chi_a(n+1) \leq 2a\chi_a(n)$. The result follows by induction.

LEMMA 2.20. $\psi(2n\pm m) \equiv \mp\psi(m) \bmod \chi(n)$.

Proof. By Lemmas 2.5 and 2.6,

$$\psi(2n\pm m) = \chi(m)\psi(2n) \pm \chi(2n)\psi(m)$$

$$\equiv \mp\psi(m) \bmod \chi(n).$$

LEMMA 2.21. $\psi(4n \pm m) \equiv \pm\, \psi(m) \bmod \chi(n)$.

Proof. By Lemma 2.20

$$\begin{aligned}\psi(4n \pm m) &\equiv -\psi(2n \pm m) \\ &\equiv \pm\, \psi(m) \bmod \chi(n).\end{aligned}$$

LEMMA 2.22. (i) $\psi_a(n) < \frac{1}{2}\chi_a(n)$ *for* $a > 2$; (ii) $\psi_2(n-1) < \frac{1}{2}\chi_2(n)$.

Proof. (i) If $a > 2$, then $4\psi_a^2(n) < (a^2-1)\psi_a^2(n)+1 = \chi_a^2(n)$.

(ii) By Lemma 2.7,

$$0 \le \psi_2(n-1) = 2\psi_2(n)-\chi_2(n), \text{ i.e. } \psi_2(n) \ge \tfrac{1}{2}\chi_2(n).$$

Thus $\frac{1}{2}\chi_2(n) \ge \chi_2(n) - \psi_2(n)$.

By Lemma 2.7 again,

$$\psi_2(n-1) < \chi_2(n-1) + \psi_2(n-1) = \chi_2(n) - \psi_2(n).$$

Thus $\frac{1}{2}\chi_2(n) > \psi_2(n-1)$.

LEMMA 2.23. *Let* $\psi(j) \equiv \pm\psi(i) \bmod \chi(n)$, $n > 0$, $0 \le i \le j \le n$. *Then* $i = j$.

Proof. If $a > 2$, then Lemma 2.22 together with the inequalities $0 = \psi(0) < \psi(1) < \ldots < \psi(n)$ imply $j = i$.

Suppose $a = 2$, but $i \neq j$. Then Lemma 2.22 implies $j = n$, and Lemma 2.8 implies $i > 0$. Then $n > 1$. Since

$$0 < \psi_2(n)-\psi_2(i) < \psi_2(n) < \chi_2(n),$$

we cannot have $\psi_2(j) \equiv \psi_2(i)$. So $\psi_2(j) \equiv -\psi_2(i)$.

Put $i = n-k$. Then $0 < k < n$. By Lemma 2.5, $\psi_2(i) \equiv \chi_2(k)\psi_2(n) \bmod \chi_2(n)$. Hence $\psi_2(j) = \psi_2(n) \equiv -\chi_2(k)\psi_2(n) \bmod \chi_2(n)$, i.e. $1 + \chi_2(k) \equiv 0 \bmod \chi_2(n)$, since $(\chi_2(n),\psi_2(n)) = 1$. But since $n > 1$ we have, by Lemma 2.7, $0 < 1+\chi_2(k) < d\psi_2(n-1)+a\chi_2(n-1) = \chi_2(n)$. This is a contradiction. Thus, $i = j$.

LEMMA 2.24. (Second step down lemma) *If* $\psi(j) \equiv \psi(i) \bmod \chi(n)$ *then* $j \equiv \pm i \bmod 2n$ $(n > 0)$.

Proof. First, assume $i \leq n$, $j \leq 4n$. If $j \leq n$ then by Lemma 2.23, $i = j$. If $n < j \leq 2n$, then set $\overline{j} = 2n-j$ so $0 \leq \overline{j} < n$. By Lemma 2.20, $\psi(\overline{j}) \equiv \psi(j) \equiv \psi(i) \bmod \chi(n)$, so by Lemma 2.23, $i = \overline{j} \equiv -j \bmod 2n$. If $2n < j \leq 4n$, set $\overline{j} = 4n-j$ so $0 \leq \overline{j} < 2n$. By Lemma 2.21 $\psi(\overline{j}) \equiv -\psi(j) \equiv -\psi(i) \bmod \chi(n)$, and a repetition of the above method shows that $j \equiv -i \bmod 2n$ if $\overline{j} < n$, and $j \equiv i \bmod 2n$ if $n \leq \overline{j} < 2n$.

Next, if $i \leq n$, $j > 4n$, write $j = 4nq+\overline{j}$, $0 < \overline{j} < 4n$. By Lemma 2.21, $\psi(j) \equiv \psi(\overline{j}) \bmod \chi(n)$ and the result follows as above.

Thus the result holds for $0 \leq i \leq n$ and all j. Repeating the procedure shows that it also holds for all i.

THEOREM 2.25. *Suppose* $a > 1$, $b_k > 0$, $k = 1,2,\ldots,m$. *Then*

$$x_k = \chi_a(b_k) \text{ and } y_k = \psi_a(b_k)$$

if and only if the following system of equations has a solution in *non-negative integers:*

I_k. $$x_k^2 = (a^2-1)y_k^2+1.$$

II. $$u^2 = (a^2-1)v^2+1.$$

III_k. $$s_k^2 = (e^2-1)t_k^2+1.$$

IV. $$v = 2(w+1)y_1^2 y_2^2 \dots y_m^2.$$

V. $$e = (a-1)(u^2-1)^2+1.$$

VI_k. $$t_k = y_k+f_k u.$$

VII_k. $$t_k = b_k+2g_k y_k.$$

$VIII_k$. $$b_k \le y_k. \qquad \text{(i.e. } b_k+c_k = y_k)$$

Proof. Let there be given a solution to I_k - $VIII_k$. By $VIII_k$, VII_k and IV,

$$y_k > 0, \quad t_k > 0, \quad v > 0.$$

Then by I_k, II, and III_k, there are positive integers i_k, j_k, n such that

$$x_k = \chi_a(i_k), \qquad y_k = \psi_a(i_k)$$

$$u = \chi_a(n), \qquad v = \psi_a(n)$$

$$s_k = \chi_e(j_k), \qquad t_k = \psi_e(j_k).$$

By IV, II, and V,

$$e \equiv 1 \bmod 2y_k$$

so that

$$t_k = \psi_e(j_k) \equiv \psi_1(j_k) = j_k \bmod 2y_k \tag{1}$$

by Lemma 2.16. By VII_k,

$$t_k \equiv b_k \bmod 2y_k. \tag{2}$$

By (1) and (2),

$$b_k \equiv j_k \bmod 2y_k. \tag{3}$$

On the other hand,

$$e \equiv a \bmod u$$

by V so that

$$t_k = \psi_e(j_k) \equiv \psi_a(j_k) \bmod u$$

by Lemma 2.16. Also

$$t_k \equiv y_k \bmod u$$

by VI_k. Hence

$$\psi_a(i_k) \equiv \psi_a(j_k) \bmod \chi_a(n), \tag{4}$$

since $y_k = \psi_a(i_k)$ and $u = \chi_a(n)$. Now

$$y_k^2 | \psi_a(n)$$

by IV so by Lemma 2.13,

$$y_k | n.$$

Hency by (4) and Lemma 2.24,

$$j_k \equiv \pm i_k \bmod 2y_k. \tag{5}$$

By (3) and (5) we have

$$b_k \equiv \pm i_k \bmod 2y_k.$$

Also

$$b_k \leq y_k$$

by $VIII_k$, and

$$i_k \leq \psi_a(i_k) = y_k$$

by Lemma 2.18. Thus $b_k = i_k$ and

$$x_k = \chi_a(b_k), \quad y_k = \psi_a(b_k) \quad (k=1,2,\ldots,m),$$

as required.

Conversely, set $x_k = \chi_a(b_k)$, $y_k = \psi_a(b_k)$ $(k=1,2,\ldots,m)$. Then I_k and $VIII_k$ hold. By Lemma 2.0, choose $h > 0$ such that

$$2y_1^2y_2^2 \ldots y_m^2 | \psi_a(h),$$

and set

$$u = \chi_a(h), \quad v = \psi_a(h).$$

Then II and IV hold. Let e be given by V. Set

$$s_k = \chi_e(b_k), \quad t_k = \psi_e(b_k),$$

satisfying III_k. Then

$$t_k \equiv b_k \bmod 2y_k$$

by Lemma 2.15, V, II and IV. Also

$$t_k \geq b_k$$

by Lemma 2.18, so g_k can be chosen satisfying VII_k.

By our choice of e,

$$e \equiv a \bmod u$$

so that by Lemma 2.16,

$$t_k \equiv y_k \bmod u. \tag{6}$$

Now $e \geq a$ since $u > 1$, so that

$$t_k \geq y_k.$$

This, together with (6), shows that VI_k can be satisfied.

This completes the proof of Theorem 2.25.

LEMMA 2.26. *If x and y are non-negative integers, and if*

$$\left((x+3)^2-1\right)(x+2)^2(y+1)^2 + 1 = z^2$$

for some integer z, then $y > x^x$.

Proof. Put $x+3 = d$. Then $d > 2$ and by Theorem 1.27 there are infinitely many solutions of

$$(d^2-1)(d-1)^2(y+1)^2 + 1 = z^2.$$

Also, $(d-1)(y+1) = \psi_d(w)$ for some w, and

$$w \equiv (d-1)(y+1) \bmod d-1,$$

by Lemma 2.15. Since $(d-1)(y+1) \neq 0$, w is a positive multiple of $d-1$, and

$$\psi_d(w) \geq \psi_d(d-1).$$

Hence

$$(d-1)(y+1) \geq (2d-1)^{d-2}$$

by Lemma 2.18, i.e.

$$(x+2)(y+1) \geq (2x+5)^{x+1}$$

so

$$y > x^x.$$

LEMMA 2.27. *If* $p, k > 0$ *and* $u > p^k$, *then* $2up - p^2 - 1 > p^k$.

Proof. Set $g(p) = 2up-p^2-1$. Then (since $u \geq 2$) $g(1) = 2u-2 \geq u$. For $1 \leq p < u$, $g'(p) = 2u-2p > 0$. So $g(p) \geq u$ for $1 \leq p < u$. Then for $u > p^k \geq p$, $2up-p^2-1 \geq u > p^k$.

LEMMA 2.28. *If* $k \geq 2$, $u \geq 2$, $d = u^2-1$ *then*

$$u + \frac{u}{(u+1)^{k-1}} \leq \sqrt{d} + 1.$$

Proof.

$$u + \frac{u}{(u+1)^{k-1}} \leq u + \frac{u}{u+1} = \frac{u^2+2u}{u+1} \leq \sqrt{u^2-1} + 1,$$

provided

$$u^2+u-1 \leq (u+1)\sqrt{u^2-1}\ ,$$

which holds for $u \geq \sqrt{2}$.

LEMMA 2.29. *If $u > p^k > 0$, then*

$$\psi_u(k)(u-p) + p^k \leq \chi_u(k).$$

Proof. For $k=0$ or $k=1$, equality holds.

For $k \geq 2$, we have (since $p > 0$ and $u \geq 2$)

$$u-p + \frac{p^k}{\psi_u(k)} \leq u-1 + \frac{p^k}{(2u-1)^{k-1}} \quad \text{by Lemma 2.18}$$

$$< u-1 + \frac{u}{(u+1)^{k-1}}$$

$$\leq \sqrt{d} \quad \text{by Lemma 2.28.}$$

Hence

$$\psi_u(k)(u-p) + p^k \leq \sqrt{d}\psi_u(k) < \chi_u(k).$$

THEOREM 2.30. *Suppose $p > 0$, $k > 0$. Then $q = p^k$ if and only if the following system of equations has a solution in non-negative integers:*

I. $$a = p+q+k+3.$$

II. $$(a+2)a^3(u+1)^2+1 = z^2.$$

III. $$c \leq \psi_2(u).$$

IV. $$s \leq c.$$

V. $$t^2=(u^2-1)s^2+1$$

VI. $\quad u-1 \mid s-k \quad$ (*and $s-k$ may be assumed non-negative*).

VII. $\quad t = q+s(u-p) + r(2up-p^2-1).$

Proof. Let there by given a solution to *I* - *VII*. By *II*, Lemma 2.26, and *I*,

$$u > (a-2)^{(a-2)} > 4. \tag{7}$$

Then

$$q = a-p-k-3 \leq a-5 < (a-2)^{(a-2)}-1 < u-1 \leq 2up-p^2-1,$$

provided

$$u(2p-1) \geq p^2.$$

But by (7) and *I*,

$$u(2p-1) > (a-2)^{(a-2)}(2p-1) > p^k(2p-1) \geq p^2,$$

so $q < 2up-p^2-1$. (8)

By *V*, there is an n such that

$$s = \psi_u(n), \quad t = \chi_u(n).$$

By Lemma 2.15,

$$s \equiv n \bmod u-1,$$

and by *VI*,

$$s \equiv k \bmod u-1,$$

so

$$n \equiv k \bmod u-1. \tag{9}$$

Now, $n < u-1$, for if $n \le 2$, then $n < 3 < u-1$ by (7); and if $n > 2$, then

$$4^{n} < 9^{n-1} \le (2u-1)^{n-1} \le \psi_u(n) = s \le c \le \psi_2(u) \le 4^{u-1}$$

by Lemma 2.18, *IV*, and *III*. Also,

$$k < a-2 < (a-2)^{(a-2)} \le u-1$$

by *I* and (7). Thus

$$n = k$$

by (9). By *VII*,

$$\chi_u(k) - \psi_u(k)(u-p) \equiv q \bmod 2up-p^2-1,$$

and by Lemma 2.17,

$$\chi_u(k) - \psi_u(k)\ (u-p) \equiv p^k \bmod 2up-p^2-1.$$

Thus

$$q \equiv p^k \bmod 2up-p^2-1. \tag{10}$$

By *I*,

$$p^k < (a-2)^{(a-2)} < u,$$

so by Lemma 2.27,

$$p^k < 2up-p^2-1. \tag{11}$$

By (8), (10) and (11),

$$q = p^k.$$

Conversely, set $q = p^k$ and let a be given by *I*. Choose u and z satisfying *II*, with u large enough so that

$$(2u)^{k-1} \leq 3^{u-1}.$$

Set

$$s = \psi_u(k), \quad t = \chi_u(k), \quad c = \psi_2(u),$$

satisfying *III* and *V*. Then $s \geq k$ by Lemma 2.18, and $s \equiv k \bmod u-1$ by Lemma 2.15, so *VI* is satisfied. Also,

$$s = \psi_u(k) \leq (2u)^{k-1} \leq 3^{u-1} \leq \psi_2(u) = c$$

by Lemma 2.18 and our choice of u. Thus *IV* is satisfied. By Lemma 2.17,

$$t \equiv q + s(u-p) \bmod 2up-p^2-1.$$

Since *I* - *VI* have already been satisfied,

$u > p^k > 0$, so by Lemma 2.29,

$$t \geq q + s(u-p).$$

Thus r may be chosen to satisfy *VII*.

CHAPTER III

CONSTRUCTION OF THE POLYNOMIALS

In this chapter, we construct two explicit polynomials, of degree 23, with 21 and 22 variables, whose positive ranges coincide with the set of Mersenne primes and the set of even perfect numbers respectively.

The diophantine definitions of the relations $x = \chi_a(k)$ and $y = \psi_a(k)$ can be used not only in defining the exponential relation, as in Theorem 2.30, but also in characterizing the sequence S_n, used for testing the primality of Mersenne numbers.

THEOREM 3.1. $S_n = 2\chi_2(2^{n-1})$.

Proof. We use induction on n.

$$S_1 = 4 = 2\chi_2(1),$$

and

$$\begin{aligned} S_{n+1} &= S_n^2 - 2 \\ &= 2(2\chi_2^2(2^{n-1}) - 1) \quad \text{by the induction hypothesis} \\ &= 2\chi_2(2^n) \quad \text{by Lemma 2.6.} \end{aligned}$$

DEFINITION 3.2. $\overline{MP}(\alpha) \equiv$ "α is a Mersenne prime other than 3."

In what follows, all quantifiers range over the non-negative integers.

LEMMA 3.3. $\overline{MP}(\alpha) \Leftrightarrow \exists n\left(\alpha = 2^{n+3}-1 \wedge \alpha \mid \chi_2(2^{n+1})\right)$.

Proof. $\overline{MP}(\alpha) \Leftrightarrow \exists n(\alpha = 2^{n+3}-1 \wedge \alpha \mid S_{n+2})$ by Theorem 1.26

$\Leftrightarrow \exists n\left(\alpha = 2^{n+3}-1 \wedge \alpha \mid 2\chi_2(2^{n+1})\right)$ by Theorem 3.1

$\Leftrightarrow \exists n\left(\alpha = 2^{n+3}-1 \wedge \alpha \mid \chi_2(2^{n+1})\right)$ since $(\alpha,2) = 1$.

We then have

$$\overline{MP}(\alpha) \Leftrightarrow \exists n,b',x'(\alpha+1 = 2^{n+3} \wedge 4b' = \alpha+1 \wedge x' = \chi_2(b') \wedge \alpha \mid x') \quad (1).$$

LEMMA 3.4. $\overline{MP}(\alpha)$ *if and only if the following system of equations has a solution in non-negative integers:*

A. $$a = 2 + (\alpha+1) + (n+3) + 3$$

B. $$(a+2)a^3(b+1)^2 + 1 = z^2$$

C. $$x^2 = 3p^2 + 1$$

D. $$u^2 = 3v^2 + 1$$

E. $$k^2 = (e^2-1)t_1^2 + 1$$

F. $$v = 2(w+1)p^2f^2$$

G. $$e = (u^2-1)^2 + 1$$

H. $$t_1 = p + gu$$

I. $$t_1 = b + 2hp$$

J. $$p = s+l$$

K. $$t^2 = (b^2-1)s^2 + 1$$

L. $$s = n+3+m(b-1)$$

M. $$t = \alpha+1+s(b-2)+r(4b-5)$$

N. $$x'^2 = 3f^2 + 1$$

O. $$q^2 = (e^2-1)t_2^2 + 1$$

P. $$t_2 = f + iu$$

Q. $$t_2 = b' + 2jf$$

R. $$b' \le f$$

S. $$4b' = \alpha + 1$$

T. $$x' = c\alpha$$

Proof. Let there by given a solution to *A*–*T*. By *B*, Lemma 2.26 and *A*,

$$b > (a-2)^{a-2} > 0. \tag{2}$$

Then *C*–*I* imply that

$$p \le \psi_2(b) \tag{3}$$

for if $b \le p$, then (2) and Theorem 2.25 show that

$$p = \psi_2(b),$$

and if $p < b$, then by Lemma 2.18

$$p < b \leq \psi_2(b).$$

Then A, B, J, K, L, M, and (3) imply, by Theorem 2.30, that

$$\alpha + 1 = 2^{n+3}. \tag{4}$$

By S, $b' > 0$, so Theorem 2.25 applies and by D, F, G, N–R,

$$x' = \chi_2(b'). \tag{5}$$

By (4), (5), S, T, and (1),

$$\overline{MP}(\alpha).$$

Conversely, if $\overline{MP}(\alpha)$, i.e. if the conditions of (1) are satisfied, then let a be given by A, and choose b and z satisfying B. Put

$$p = \psi_2(b).$$

Then by Theorem 2.25 we see that C–I can be satisfied, and by Theorem 2.30, J–M can be satisfied. Let b' be given by S. Then $b' > 0$ so by Theorem 2.25, N–R can be satisfied. Finally, T can be satisfied by (1).

The conditions of Lemma 3.4 may be expressed more economically.

LEMMA 3.5. $\overline{MP}(\alpha)$ *if and only if the following system of equations has a solution in non-negative integers:*

I. $$(\alpha+n+11)(\alpha+n+9)^3(b+1)^2 + 1 = z^2$$

II. $$x^2 = 3p^2 + 1$$

III. $$p = s + l$$

IV. $$u^2 = 12(w+1)^2p^4f^4$$

V. $$e = u^4 - 2u^2 + 2$$

VI. $$k^2 = (e^2-1)(p+gu)^2 + 1$$

VII. $$p + gu = b + 2hp$$

VIII. $$\left(\alpha+1+s(b-2) + r(4b-5)\right)^2 = (b^2-1)s^2 + 1$$

IX. $$s = n+3+m(b-1)$$

X. $$(c\alpha)^2 = 3f^2 + 1$$

XI. $$q^2 = (e^2-1)(f+iu)^2 + 1$$

XII. $$4(f+iu) = \alpha+1+8jf$$

Proof. First note that condition R of Lemma 3.4 may be omitted entirely, since if $b' > f$, then by N and S

$$x'^2 = 3f^2+1 \leq 3(b'-1)^2+1 < (4b'-1)^2 = \alpha^2,$$

so

$$0 < x' < \alpha,$$

contradicting T.

We then have

$$A,B \Leftrightarrow I; \quad C \Leftrightarrow II; \quad J \Leftrightarrow III; \quad D,F \Leftrightarrow IV; \quad G \Leftrightarrow V;$$

$$E,H \Leftrightarrow VI; \quad H,I \Leftrightarrow VII; \quad K,M \Leftrightarrow VIII; \quad L \Leftrightarrow IX; \quad N,T \Leftrightarrow X; \quad O,P \Leftrightarrow XI.$$

Also,

$$P,Q \Leftrightarrow f+iu = b'+2jf \Leftrightarrow XI,$$

using S and the fact that by I-IX,

$$\alpha+1 = 2^{n+3}$$

so there is an integer b' such that

$$4b' = \alpha+1.$$

By transposing the terms in each equation to one side and summing their squares, we get a non-negative polynomial P satisfying

$$\overline{MP}(\alpha) \Leftrightarrow P = 0.$$

Thus, α is a Mersenne prime (including 3) if and only if

$$(\alpha-3)^2P = 0. \tag{6}$$

The method of Putnam then gives

THEOREM 3.6. *The set of Mersenne primes is identical with the set of positive values of*

$$\alpha\left(1-(\alpha-3)^2([(\alpha+n+11)(\alpha+n+9)^3(b+1)^2+1-z^2]^2+[x^2-3p^2-1]^2+[p-s-l]^2+\right.$$
$$[u^2-12(w+1)^2p^4f^4]^2+[e-u^4+2u^2-2]^2+[k^2-(e^2-1)(p+gu)^2-1]^2+[p+gu-b-2hp]^2+$$
$$[(\alpha+1+bs-2s+4br-5r)^2-b^2s^2+s^2-1]^2+[s-n-3-mb+m]^2+[c^2\alpha^2-3f^2-1]^2+$$
$$\left.[q^2-(e^2-1)(f+iu)^2-1]^2+[4f+4iu-\alpha-1-8jf]^2)\right) ,$$

for non-negative integer values of the variables.

We saw in Chapter I that β is an even perfect number if and only if $2\beta = \alpha(\alpha+1)$, where α is a Mersenne prime. This gives

THEOREM 3.7. *The set of even perfect numbers is identical with the set of positive values of*

$$\beta\left(1-(\beta-6)^2([2\beta-\alpha^2-\alpha]^2+[(\alpha+n+11)(\alpha+n+9)^3(b+1)^2+1-z^2]^2+[x^2-3p^2-1]^2+\right.$$
$$[p-s-l]^2+[u^2-12(w+1)^2p^4f^4]^2+[e-u^4+2u^2-2]^2+[k^2-(e^2-1)(p+gu)^2-1]^2+$$
$$[p+gu-b-2hp]^2+[(\alpha+1+bs-2s+4br-5r)^2-b^2s^2+s^2-1]^2+[s-n-3-mb+m]^2+$$
$$\left.[c^2\alpha^2-3f^2-1]^2+[q^2-(e^2-1)(f+iu)^2-1]^2+[4f+4iu-\alpha-1-8jf]^2)\right) ,$$

for non-negative integer values of the variables.

Both of these polynomials assume certain negative values as well. This is unavoidable, as we shall now show.

THEOREM 3.8. [5][7]. *A polynomial $P(x_1,x_2,\ldots,x_n)$, with integer coefficients, which assumes only prime values must be constant.*

Proof. Let $P(x_1,x_2,\ldots,x_n)$ be a polynomial which assumes only prime values. Then $P(1,1,\ldots,1) = p$ is a prime. For any integers m_1, m_2, ... m_n, we have $P(1+m_1p,1+m_2p,\ldots,1+m_np) \equiv p \bmod p$.

But $P(1+m_1p,1+m_2p,\ldots,1+m_np)$ is prime. Hence for all integers $m_1,m_2,\ldots,m_n$,

$$P(1+m_1p,1+m_2p,\ldots,1+m_np) = p.$$

This implies that $P(x_1,x_2,\ldots,x_n)$ has degree zero.

COROLLARY 3.9. *A polynomial $P(x_1,x_2,\ldots,x_n)$, with integer coefficients, which assumes only Mersenne primes as values, must be constant.*

Proof. Immediate from Theorem 3.8.

THEOREM 3.10. *The set of all perfect numbers (even or odd) is not the exact range of a polynomial in several variables with integer coefficients.*

Proof. Let $P(x_1,x_2,\ldots,x_n)$ be such a polynomial. Then there exist numbers $a_1,a_2,\ldots,a_n$ such that

$$P(a_1,a_2,\ldots,a_n) = 6.$$

Let $m_1,m_2,\ldots,m_n$ be integers. Then

$$P(a_1+6m_1,a_2+6m_2\cdot,,,\cdot a_n+6m_n) \equiv 6 \bmod 6$$

$$\equiv 0 \bmod 2,$$

so $P(a_1+6m_1,a_2+6m_2,\ldots,a_n+6m_n)$ is an even perfect number, say

$$P(a_1+6m_1, a_2+6m_2, \dots, a_n+6m_n) = 2^{k-1}(2^k-1)$$

for some k (depending on $m_1, m_2, \dots, m_n$), where 2^k-1 is prime.

Then

$$6 | 2^{k-1}(2^k-1) \Rightarrow 3 | 2^k-1$$

$$\Rightarrow 2^k-1 = 3, \text{ since } 2^k-1 \text{ is prime.}$$

i.e.,

$$P(a_1+6m_1, a_2+6m_2, \dots, a_n+6m_n) = 6 \text{ for all integers } m_1, m_2, \dots, m_n.$$

Thus $P(x_1, x_2, \dots, x_n)$ has degree zero.

In the same way, we can prove

THEOREM 3.11. *A polynomial $P(x_1, x_2, \dots. x_n)$, with integer coefficients, which assumes only even perfect values must be constant.*

Thoralf Skolem [14] showed that every diophantine equation is equivalent to an equation of total degree 4. All that is necessary is to break up large products by introducing new unknowns and new equations of the form $z = xy$ and $z = x+y$. A system of equations $A_i = B_i$, of degree 2, is equivalent to an equation $\sum_i (A_i - B_i)^2 = 0$, of degree 4.

Skolem's method, when applied to equations *I-XII* of Lemma 3.5, yields an equivalent system of equations, of degree 2 and with 56 unknowns. Summing their squares and using the method of Putnam then gives a polynomial of degree 5, in 57 variables, whose positive range is the Mersenne primes. Similarly, the even perfect numbers may be exhibited as the positive range of a polynomial of degree 5, in 59 variables.

CHAPTER IV

REDUCTION OF THE NUMBER OF VARIABLES

We now give alternate definitions of the relations $C = \psi_A(B)$ and $y = x^n$, which are more economical, with respect to the number of unknowns, than those given previously. These, together with two "Relation-Combining Theorems", (Theorems 4.1 and 4.2) will allow us to construct a polynomial of 12 variables and degree 495, whose positive range is the Mersenne primes. As in Chapter III, this then gives a polynomial of 13 variables, and the same degree, whose positive range is the even perfect numbers.

Theorems 4.1 and 4.2 are adaptations of a more general theorem, due to Y. Matijasevič and J. Robinson in [12]. Theorems 4.3 and 4.4 are also from [12].

THEOREM 4.1. *Let R, S, T, U be integers (positive, negative or zero) where $R > 1$, $S \neq 0$. Then $Sq(R)$ ("R is a square") and $S|T$ and $U > 0$ if and only if*

$$F(R,S,T,U,x) = \left(S^2x+T^2-S^2(2U-1)(R+T^2)\right)^2-RS^4(2U-1)^2 = 0$$

for some non-negative integer x.

Proof. Let x be a non-negative root of F.

Then

$$S^2 | S^2x+T^2-S^2(2U-1)(R+T^2)$$

so

$$S | T.$$

Since R satisfies an equation of the form

$$y^2 - Rz^2 = 0,$$

where y and z are integers, R is a square. Also

$$x = \frac{-T^2+S^2(2U-1)(R+T^2)\pm\sqrt{R}S^2(2U-1)}{S^2} \qquad (1)$$

If $U \leq 0$, then since $2U-1 < 0$ and $0 < R+T^2 \pm\sqrt{R}$

$$x = \frac{-T^2+S^2[2U-1][R+T^2\pm\sqrt{R}]}{S^2} < 0 ,$$

a contradiction. So $0 < U$.

Conversely, if $Sq(R)$ and $S|T$ and $U > 0$, then put

$$x = \frac{-T^2+S^2(2U-1)(R+T^2)+\sqrt{R}S^2(2U-1)}{S^2} ,$$

as in (1). Then $F(R,S,T,U,x) = 0$.

In the same way, we can prove

THEOREM 4.2. *Let R, S, T, U be integers, $S > 0$, $T > 0$. Then $Sq(R)$ and $S|T$ and $U > 0$ if and only if*

$$G(R,S,T,U,x) = \left(Sx+T-S(2U-1)(R+T)\right)^2 - RS^2(2U-1)^2 = 0$$

for some non-negative integer x.

THEOREM 4.3. (Robinson-Matijasevič). *Consider the following system of equations:*

I. $\quad Sq(DFI),\ F \mid H-C,\ B \le C.$

II. $\quad D = (A^2-1)C^2 + 1.$

III. $\quad E = 2(i+1)DC^2.$

IV. $\quad F = (A^2-1)E^2 + 1.$

V. $\quad G = A + F(F-A).$

VI. $\quad H = B + 2jC.$

VII. $\quad I = (G^2-1)H^2 + 1.$

Suppose $A > 1$, $B > 0$, $C > 0$. Then $\psi_A(B) = C$ if and only if I-VII can be satisfied by non-negative integers i and j and integers D, E, F, G, H, I.

Proof. (Robinson-Matijasevic [12]). Suppose $A > 1$, $B > 0$, $C > 0$ and *I-VII* are satisfied. Then $D,\ldots I$ are all positive ($F > A$ since $F = (A+1)(A-1)E^2 + 1$ and $A > 1$). We will first show that D, F and I are co-prime and hence each is a square by *I*. We obtain in turn

$$E \equiv 0,\quad F \equiv 1,\quad G \equiv 1,\quad I \equiv 1 \pmod D \qquad 1)$$

by III, IV, V, VII respectively. Next

$$G \equiv A, \quad H \equiv C, \quad I \equiv D \pmod{F}, \qquad 2)$$

the first two congurences by V and I respectively, and then using them, together with II, to obtain the third.

Then,

$$(F,D) = (I,D) = 1$$

by 1), and

$$(I,F) = 1$$

since $I \equiv D(\text{mod } F)$ and $(I,D) = 1$. Hence D, F and I are all squares, so there are positive integers p,q,r such that

$$C = \psi_A(p), \quad D = \chi_A^2(p),$$

$$E = \psi_A(q), \quad F = \chi_A^2(q),$$

$$H = \psi_G(r), \quad I = \chi_G^2(r).$$

Now,

$$G \equiv 1 \pmod{2C}$$

by III, IV and V, so that

$$\begin{aligned} H = \psi_G(r) &\equiv \psi_1(r) \pmod{2C} \quad \text{(by Lemma 2.16)} \\ &\equiv r \pmod{2C}. \end{aligned}$$

Also,

$$H \equiv B(\text{mod } 2C)$$

by VI, so that

$$r \equiv B \pmod{2C}. \qquad 3)$$

On the other hand,

$$G \equiv A \pmod{F}$$

by V, so that

$$H = \psi_G(r) \equiv \psi_A(r) \pmod{F}$$

by Lemma 2.16, and

$$H \equiv C \pmod{F}$$

by I. Hence

$$\psi_A(r) \equiv \psi_A(p) \ \left(\mathrm{mod}\ \chi_A(q)\right) \qquad 4)$$

since $C = \psi_A(p)$ and $F = \chi_A^2(q)$.

Now

$$C^2 \mid \psi_A(q)$$

by III, so by Lemma 2.13,

$$C \mid q.$$

Hence by 4) and Lemma 2.24,

$$r \equiv \pm p \pmod{2C}. \qquad 5)$$

By 3) and 5),

$$B \equiv \pm p \pmod{2C}.$$

By I,

$$B \leq C$$

and by Lemma 2.19,

$$p \leq \psi_A(p) = C,$$

so $B = p$ and

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

Conversely, suppose $A > 1$, $B > 0$, $C > 0$ and $\psi_A(B) = C$. Put

$$D = \chi_A^2(B),$$

satisfying *II*. Choose $q > 0$ so that

$$2DC^2 \mid \psi_A(q).$$

For this, q may be any multiple of $2B\psi_A(2B)$, since

$$4DC^2 = \left(2\chi_A(B)\psi_A(B)\right)^2 = \psi_A^2(2B)$$

by Lemma 2.6, and

$$\psi_A^2(2B) \mid \psi_A\left(2B\psi_A(2B)\right)$$

by Lemma 2.12. Put

$$E = \psi_A(q)$$

and choose i satisfying *III*. Let F and G be given by *IV* and *V*. Put

$$H = \psi_G(B).$$

Since *II*-*V* have already been satisfied,

$$G \equiv 1 \pmod{2C}.$$

Hence

$$\psi_G(B) \equiv B \pmod{2C},$$

and $\psi_G(B) \geq B$, so we can choose j satisfying *VI*. Let I be given by *VII*. Finally, D, F and I are all squares by the hypothesis and the choice of E and H; $G \equiv A \pmod{F}$ so

$$H = \psi_G(B) \equiv \psi_A(B) = C \pmod{F},$$

and

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

Hence I is satisfied and the theorem is proved.

Note that we can eliminate D, E, F, G, H, I by means of *II-VII*, leaving only the two unknowns i and j and parameters A, B and C.

We now consider the exponential relation $y = x^n$. Here we shall again follow the treatment given in [12]. Suppose $x > 0$ and $n > 0$. From Lemma 2.18,

$$\psi_A(B) \sim (2A)^{B-1} \text{ as } A \to \infty.$$

Hence

$$\frac{\psi_{Mx}(n+1)}{\psi_M(n+1)} \to x^n \text{ as } M \to \infty.$$

Let

$$p = \frac{\psi_{Mx}(n+1)}{\psi_M(n+1)},$$

and define by $\langle p \rangle$ the nearest integer to p. ($\langle p \rangle$ is undefined if p is an integer plus a half.) We wish to find a lower bound M_0 such that for $M > M_0$,

$$\langle p \rangle = x^n .$$

To make the necessary estimates, we will use the inequalities

(i) $$(1-\alpha)^q \geq 1-q\alpha > 0 \qquad \text{for } 0 \leq \alpha < \frac{1}{q}$$

(ii) $$(1-\alpha)^{-1} \leq 1+2\alpha \qquad \text{for } 0 \leq \alpha \leq \frac{1}{2} .$$

Then for $M \geq n$,

$$\begin{aligned} p &\leq \frac{(2Mx)^n}{(2M-1)^n} \quad \text{by Lemma 2.18} \\ &= x^n\left(1 - \frac{1}{2M}\right)^{-n} \\ &\leq x^n\left(1 - \frac{n}{2M}\right)^{-1} \\ &\leq x^n\left(1 + \frac{n}{M}\right) , \end{aligned}$$

and

$$\begin{aligned} p &\geq \frac{(2Mx-1)^n}{(2M)^n} \\ &= x^n\left(1 - \frac{1}{2Mx}\right)^n \\ &\geq x^n\left(1 - \frac{n}{2Mx}\right) . \end{aligned} \qquad 6)$$

Hence if M is so large that

$$\frac{nx^n}{M} < \frac{1}{2} , \qquad 7)$$

then $|x^n - p| < \frac{1}{2}$ and $\langle p \rangle = x^n$. Also if $M > n$, then

$$p > \tfrac{1}{2}x^n$$

by 6). If $y = \langle p \rangle$, that is

$$(p-y)^2 < \tfrac{1}{4},$$

and if

$$M > 4n(y+1)$$

then

$$y+1 > p > \tfrac{1}{2}x^n,$$

so

$$M > 2nx^n,$$

satisfying 7), and

$$y = \langle p \rangle = x^n.$$

THEOREM 4.4. (Robinson-Matijasevič). *Consider the following system of equations:*

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

II. $$Sq\left((M^2-1)L^2 + 1\right)$$

III. $$\left(\frac{C}{L} - y\right)^2 < \tfrac{1}{4}\,,\ xyn > 0$$
$$(\text{or } (L^2-4(C-Ly)^2)xyn > 0)$$

IV. $$M = 4n(y+1) + x + 2$$

V. $$L = n + 1 + l(M-1)$$

VI. $$A = Mx$$

VII. $$B = n + 1.$$

Then $x > 0$, $n > 0$ and $y = x^n$ if and only if I-VII can be satisfied by non-negative integers x, y, n, l and integers M, L, A, B, C.

Proof. Suppose *I-VII* hold. *III* implies $x > 0$, $y > 0$, $n > 0$. $L > 0$ by *IV* and *V* so there is an integer L' such that

$$L = \psi_M\bigl(n+1+L'(M-1)\bigr)$$

by *II*, *V* and Lemma 2.15. Also $L' \geq 0$ since $M-1 > n+1$ by *IV*. We will first show that $L' = 0$ by contradiction. For $L' > 0$,

$$\frac{\psi_{Mx}(n+1)}{\psi_M\bigl(n+1+L'(M-1)\bigr)} \leq \frac{\psi_{Mx}(n+1)}{\psi_M(n+1+M-1)}$$

$$\leq \frac{(2Mx)^n}{(2M-1)^{M+n-1}}$$

$$= \frac{(2M)^n}{(2M-1)^{2n}} \cdot \frac{x^n}{(2M-1)^{M-n-1}}$$

$$< \frac{1}{2} ,$$

provided $2M-1 > x$ and $M > 2n+1$. Both of these conditions on M follow from *IV*. Here we used the fact that $n > 0$ so $(2M-1)^{2n} > 2\cdot(2M)^n$.

Thus if $L' > 0$ then

$$y = \left\langle \frac{C}{L} \right\rangle = 0$$

by the first part of *III*, contradicting the second part.

Hence $L' = 0$ and

$$L = \psi_M(n+1).$$

Then by *III*, *IV* and the argument preceding Theorem 4.4,

$$y = \langle p\rangle = x^n.$$

On the other hand, suppose $y = x^n$, $x > 0$, $n > 0$. Let M, A, B, C be given by *IV*, *VI*, *VII*, *I*. Let

$$L = \psi_M(n+1),$$

then *II* holds and

$$L \equiv n+1 \pmod{M-1}$$

by Lemma 2.15. Also $n+1 < M-1$ by our choice of M, so we can choose l satisfying *V*. Finally, *III* holds since $y = x^n = \langle p\rangle$ by the argument above.

LEMMA 4.5. $\overline{MP}(\alpha) \Leftrightarrow \exists B_1, n, h(\alpha+1 = 2^{n+3} \wedge 4B_1 = \alpha+1 \wedge h = \psi_2(B_1) \wedge \alpha^2 | 3h^2+1)$.

Proof. By Lemma 3.3,

$$\overline{MP}(\alpha) \Leftrightarrow \exists n, B_1, D_1(\alpha+1 = 2^{n+3} \wedge 4B_1 = \alpha+1 \wedge D_1 = \chi_2(B_1) \wedge \alpha | D_1).$$

Put

$$h = \psi_2(B_1),$$

then

$$D_1^2 = 3h^2 + 1$$

so $\alpha | D_1$ implies

$$\alpha^2 | 3h^2 + 1.$$

Conversely, if $h = \psi_2(B_1)$ and $\alpha^2 | 3h^2 + 1$, then put

$$D_1 = \chi_2(B_1),$$

then $\alpha^2 | D_1^2$ so

$$\alpha \,|D_1.$$

LEMMA 4.6. *$\overline{MP}(\alpha)$ if and only if the following system of equations can be satisfied by non-negative integers α, i, j, k, l, m, n and integers A, B, g, D, E, F, G, H, I, L, M, B_1, h, D_1, E_1, F_1, G_1, H_1, I_1:*

i) $$Sq(DFI),\quad F|H-g,\quad B \le g$$

ii) $$D = (A^2-1)g^2 + 1$$

iii) $$E = 2(i+1)Dg^2$$

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

v) $$G = A + F(F-A)$$

vi) $$H = B + 2jg$$

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

viii) $$Sq\big((M^2-1)L^2 + 1\big)$$

ix) $$L^2 - 4\big(g-L\ (\alpha+1)\big)^2 > 0$$

x) $$M = 4\big((n+3)(\alpha+2) + 1\big)$$

xi) $$L = n + 4 + l(M-1)$$

xii) $$A = 2M$$

xiii) $$B = n + 4$$

xiv) $$Sq(16D_1F_1I_1), \quad 4F_1 \mid 4H_1 - 4h, \quad \alpha+1 \le 4h$$

xv) $$D_1 = 3h^2 + 1$$

xvi) $$E_1 = 2(k+1)D_1h^2$$

xvii) $$F_1 = 3E_1^2 + 1$$

xviii) $$G_1 = 2 + F_1(F_1-2)$$

xix) $$4H_1 = \alpha+1+8mh$$

xx) $$16I_1 = (G_1^2-1)(4H_1)^2 + 16$$

xxi) $$\alpha^2 \mid 3h^2 + 1.$$

Proof. Suppose *i)*-*xxi)* are satisfied. By *xii)*, *xiii)*, and *i)*, $A > 1$, $B > 0$, $g > 0$, so Theorem 4.3 applies, and *i)*-*vii)* imply

$$g = \psi_A(B).$$

This, together wit *viii)*-*xiii)*, implies

$$\alpha+1 = 2^{n+3}, \tag{8}$$

by Theorem 4.4. Then there is an integer B_1 satisfying

$$0 < 4B_1 = \alpha+1. \tag{9}$$

9) and *xiv)*-*xx)* imply

$$h = \psi_2(B_1). \tag{10}$$

By 8), 9), 10), *xxi)* and Lemma 4.5,

$\overline{MP}(\alpha)$.

Conversely, if α is a Mersenne prime other than 3, i.e. if the conditions of Lemma 4.5 hold, then substituting the appropriate terms into the conditions of Theorems 4.3 and 4.4 gives *i*)-*xxi*).

We can eliminate from *i*)-*xxi*) all but the non-negative integers α, g, h, i, j, k, l, m, n. ($g,h > 0$ by *i*) and *xiv*).) After doing this, we have

$$\overline{MP}(\alpha) \Leftrightarrow \exists ghijklmn \left(Sq(R_i) \wedge S_i | T_i \wedge U_i > 0 \ (i = 1,2,3) \right) ,$$

where

$$R_1 = DFI \text{ is of degree } 120$$

$$R_2 = (M^2-1)L^2 + 1 \text{ is of degree } 9$$

$$R_3 = 16\ D_1F_1I_1 \text{ is of degree } 56$$

$$S_1 = F \text{ is of degree } 22$$

$$T_1 = H-g \text{ is of degree } 2$$

$$S_2 = 4F_1 \text{ is of degree } 10$$

$$T_2 = 4H_1-4h \text{ is of degree } 2$$

$$S_3 = \alpha^2$$

$$T_3 = 3h^2 + 1$$

$$U_1 = g-B+1 = g-n-3$$

$$U_2 = L^2 - 4\big(g-L(\alpha+1)\big)^2 \text{ is of degree } 8$$

$$U_3 = 4h - \alpha.$$

We can now apply Theorems 4.1 and 4.2, to get $\overline{MP}(\alpha) \Leftrightarrow \exists defghijklmn$ $(G^2(R_1,S_3,T_3,U_3,d) + F^2(R_2,S_2,T_2,U_2,e) + F^2(R_3,S_1,T_1,U_1,f) = 0)$. Here, $G(R_1,S_3,T_3,U_3,d)$ has the highest degree - 246. The method of Putnam then gives

THEOREM 4.7. *The set of Mersenne primes is identical with the positive range of*

$$\alpha\big(1-(\alpha-3)^2(G^2(R_1,S_3,T_3,U_3,d) + F^2(R_2,S_2,T_2,U_2,e) + F^2(R_3,S_1,T_1,U_1,f))\big) ,$$

a polynomial of degree 495, *for non-negative integer values of its* 12 *variables* α, d, e, f, g, h, i, j, k, l, m, n.

THEOREM 4.8. *The set of even perfect numbers is identical with the positive range of*

$$\beta\big(1-(\beta-6)^2\big((2\beta-\alpha(\alpha+1))^2+G^2(R_1,S_3,T_3,d_3,d)+F^2(R_2,S_2,T_2,U_2,e)+F^2(R_3,S_1,T_1,U_1,f)\big)\big) ,$$

a polynomial of degree 495, *for non-negative integer values of its* 13 *variables* α, β, d, e, f, g, h, i, j, k, l, m, n.

We can also develop these polynomials by using the definition of the exponential relation given in Theorem 2.30, along with a generalization of Theorem 4.3 to the case $\psi_A(B_1) = C_1$, $\psi_A(B_2) = C_2$, for $A = 2$. This results in a polynomial with 13 variables, of degree 255, whose positive range is the Mersenne primes.

BIBLIOGRAPHY

1. H. Davenport, *The Higher Arithmetic*, Hutchinson's University Library, 1952, *viii* + 172 pp.

2. Martin Davis, *Computability and Unsolvability*, McGraw-Hill, 1958, *xxv* + 210 pp.

3. Martin Davis, *Hilbert's Tenth Problem is Unsolvable*, Amer. Math. Monthly 80 (1973), 233-269.

4. Martin Davis, Hilary Putnam and Julia Robinson, *The Decision Problem For Exponential Diophantine Equations*, Ann. of Math. 74 (1961), 425-436.

5. G.H. Hardy and E.M. Wright, *An Introduction to the Theory of Numbers*, Fourth Edition, Oxford University Press, 1960, *xvi* + 421 pp.

6. David Hilbert, *Mathematische Probleme*, Vortrag, gehalten auf dem internationalen Mathematiker-Kongress zu Paris 1900, Nachrichten Akad. Wiss. Gottingen, Math.-Phys. KL. (1900), 253-297. English translation: Bull. Amer. Math. Soc., 8 (1901-1902), 437-479.

7. J.P. Jones, *Polynomial Formula for the Prime Numbers*, preprint.

8. J.P. Jones, *Universal Diophantine Equation*, preprint.

9. D.H. Lehmer, *On Lucas's Test for the Primality of Mersenne's numbers*, Journal London Math. Soc. (1935), 162-165.

10. Yuri Matijasevič, *Enumerable sets are Diophantine*, Doklady Akademii Nauk SSSR, 191 (1970), 279-282. English translation: Soviet Math, Doklady, 11 (1970), 354-358.

11. Yuri Matijasevič, *Diophantine Representation of Enumerable Predicates*, Izvestija Akademii Nauk SSSR. Serija Matematičeskaja, 35 (1971), 3-30. English translation: Mathematics of the USSR - Izuestija 5 (1971), 1-28.

12. Yuri Matijasevič and Julia Robinson, *Reduction of an arbitrary Diophantine Equation to One in 13 Unknowns*, Acta Arithmetica (forthcoming).

13. Hilary Putnam, *An Unsolvable Problem in Number Theory*, Journal of Symbolic Logic 25 (1960), 220-232.

14. Thoralf Skolem, *Diophantische Gleichungen*, Springer, Berlin, 1938.

APPENDIX

THEOREM 1. *Suppose* $n_k > 0$, $a > 1$, $k = 1,2,\ldots,m$. *Then*

$$x_k = \chi_a(n_k) \text{ and } y_k = \psi_a(n_k) \qquad (k=1,2,\ldots,m)$$

if and only if the following system of equations can be satisfied by non-negative integers:

$$I_k.\quad x_k^2 = (a^2-1)y_k^2 + 1$$

$$II.\quad u^2 = (a^2-1)v^2 + 1$$

$$III_k.\quad s_k^2 = (b^2-1)t_k^2 + 1$$

$$IV.\quad v = 4ry_1^2y_2^2\ldots y_m^2$$

$$V.\quad b = a + u^2(u^2-a)$$

$$VI_k.\quad s_k = x_k + c_k u$$

$$VII_k.\quad t_k = n_k + 4d_k y_k$$

$$VIII_k.\quad n_k \le y_k.$$

Proof. As in [3]. There, two equations ($b = 1+4py = a+qu$) are used to express the conditions $b \equiv 1 \bmod 4y$ and $b \equiv a \bmod u$. Here, Equation V, together with IV and II, accomplishes the same thing.

THEOREM 2. *The set of Mersenne primes is identical with the set of positive values of*

$$\alpha\{1-(\alpha-3)^2([(\alpha+n+11)(\alpha+n+9)^2(b+1)^2+1-z^2]^2+[(s+l)^2-3p^2-1]^2+[u^2-48k^2p^4f^4-1]^2+$$
$$[(s+l+gu)^2-(e^2-1)(b+4hp)^2-1]^2+[e-u^4+2u^2-2]^2+[(\alpha+1+bs-2s+4br-5r)^2-b^2s^2+s^2-1]^2+$$
$$[s-n-3-mb+m]^2+[c^2\alpha^2-3f^2-1]^2+[16(c\alpha+iu)^2-(e^2-1)(\alpha+1+16jf)^2-16]^2)\},$$

a polynomial of degree 23, *for non-negative integer values of its* 18 *variables.*

THEOREM 3. *The set of even perfect numbers is identical with the set of positive values of*

$$\beta\big(1-(\beta-6)^2([2\beta-\alpha^2-\alpha]^2+[(\alpha+n+11)(\alpha+n+9)^2(b+1)^2+1-z^2]^2+[(s+l)^2-3p^2-1]^2+[u^2-48k^2p^4f^4-1]^2$$
$$+[(s+l+gu)^2-(e^2-1)(b+4hp)^2-1]^2+[e-u^4+2u^2-2]^2+[(\alpha+1+bs-2s+4br-5r)^2-b^2s^2+s^2-1]^2+$$
$$[s-n-3-mb+m]^2+[c^2\alpha^2-3f^2-1]^2+[16(c\alpha+iu)^2-(e^2-1)(\alpha+1+16jf)^2-16]^2)\big),$$

a polynomial of degree 23, *for non-negative integer values of its* 19 *variables.*