THE EQUATION $1^p + 2^p + 3^p + \cdots + n^p = m^q$

BY

JUAN J. SCHÄFFER
in Montevideo

1. Introduction

E. Lucas [22] has proved that the diophantine equation

$$1^2 + 2^2 + \cdots + n^2 = m^2$$

has only the two solutions $n = m = 1$; $n = 24$, $m = 70$ (cf. [19]). In this paper we consider the more general equation

$$S_p(n) = 1^p + 2^p + \cdots + n^p = m^q \tag{1.1}$$

where p and q are given positive integers, and positive integral solutions are required. Some cases of this equation have been discussed before (see [7], Ch. 1, 23) and a very few simple ones solved, but no general solution has, to our knowledge, been attempted.

A few algebraic properties of $S_p(n)$, some of them new, are reviewed in Section 2. Section 3 deals with certain numerical properties of $S_p(n)$ required subsequently.

The study of equation (1.1) is divided into two parts. In Section 4 it is considered from a general point of view, and it is proved that, for any given choice of p, q, the number of solutions is finite, unless one of the following is the case: $q = 1$; $p = 3$, $q = 2$ (trivial cases); $p = 1$, $q = 2$; $p = 3$, $q = 4$; $p = 5$, $q = 2$ (Theorem 1). Also a result concerning the number of solutions is obtained.

In Sections 5 (cases with q odd) and 6 (q even), the complete determination of the solutions is obtained in several cases by means of theorems concerning algebraic diophantine equations of several kinds. The cases in which the number of solutions is infinite reduce to "Pellian" equations and can be solved completely. For the rest,

11 – 563801. *Acta mathematica*. 95. Imprimé le 2 mai 1956.

cases were considered with p ranging from 1 through 11, and with q in several classes of numbers. The bulk of the proofs in these sections consists of numerical computations, which are only briefly sketched. The results of these sections are collected in Section 7 (Theorem 2), and give weight to the conjecture that the case $p=q=2$, mentioned at the beginning of this introduction, is the only case with a finite number of solutions that has a solution other than the trivial $n=m=1$.

Most of the research was carried out at the Instituto de Matemática y Estadística, Universidad de la República, Montevideo, Uruguay. Some of the results were obtained in the course of a seminar at that University (1951). The author is indebted to J. F. Forteza, who originally suggested this topic, and to Prof. R. Laguardia for his guidance and numerous helpful suggestions; he also wishes to thank Profs. Th. Skolem and E. Selmer for the suggestions which have led to the final form of this paper.

2. Algebraic properties of $S_p(n)$

$S_p(n)$ may be expressed in terms of Bernoulli polynomials as

$$S_p(n)=\frac{1}{p+1}(B_{p+1}(n+1)-B_{p+1}(0)). \tag{2.1}$$

(Our notation for Bernoulli polynomials will be that of Nörlund's paper [25] throughout.)

We now apply some well-known facts concerning Bernoulli polynomials, ([25], pp. 127–130), and obtain the following results:

LEMMA 1. $S_1(n)=n(n+1)/2$; *for* $p\neq 1$ *we have:*

$$\begin{aligned} &\text{(i)} \quad S_p(n)=\frac{1}{k(p)}\cdot n(n+1)(2n+1)\cdot P_p(n) \\ &\text{(ii)} \quad S_p(n)=\frac{1}{k(p)}\cdot n^2(n+1)^2\cdot P_p(n) \end{aligned} \tag{2.2}$$

according as p *is* (i) *even, or* (ii) *odd;* $k(p)$ *is an integer selected in such a way that* $P_p(x)$ *be a polynomial with integral coefficients having no common factor. This polynomial satisfies the following conditions:*

a) $0,\ -1/2,\ -1$ *are not roots of* $P_p(x)$ *for any* p.

b) $P_p(x)\equiv P_p(-1-x)$.

c) $P_p(x)\equiv Q_p(x(x+1))$ *where* $Q_p(y)$ *is a polynomial with integral coefficients, which have no common factor.*

PROOF: A trivial consequence of the properties of Bernoulli polynomials. We merely point out that $Q_p(y)$ has integral coefficients since the leading coefficient of $x(x+1)$ is 1.

We are not concerned with the particular algebraic form of $P_p(x)$, except in two cases which we shall presently consider (Lemmas 2 and 5).

LEMMA 2. *For odd $p>1$, we cannot have $Q_p(y)\equiv(T(y))^2$ ($T(y)$ a polynomial) unless $p=3$ ($Q_3(y)\equiv 1$).*

PROOF: By Gauss's Theorem, we may always assume that $T(y)$ has integral coefficients. From (2.2) (ii) we should then have

$$S_p(n)=\frac{1}{k(p)}\cdot[n(n+1)\cdot T(n)]^2. \tag{2.3}$$

Since $S_p(1)=1$ it follows that $k(p)=(2\cdot T(1))^2$. Substituting this value in (2.3) and setting $n=2$, we obtain

$$S_p(2)=1+2^p=(3\cdot T(2)/T(1))^2=x^2$$

where x obviously must be an integer. However, the equation $1+2^p=x^2$ has obviously the unique solution $p=3$, since it implies $2^r-2^s=2$, $r+s=p$.

LEMMA 3. *Let P be a prime, n an arbitrary positive integer, and set $n=\sum_0^t n_i P^i$, where $0\le n_i\le P-1$. (The n_i are the digits of n written to the base P, and are therefore uniquely determined.) Then $\binom{n}{m(P-1)}\equiv 0 \pmod{P}$ for all integers m such that $0<m(P-1)<n$ if and only if $\sum_0^t n_i\le P-1$.*

LEMMA 4. *Let n be a positive integer such that $n\equiv 2 \pmod 4$. If P is any odd prime, set $n=\sum_0^{t(P)} n_{iP}P^i$, where $0\le n_{iP}\le P-1$. If both the following conditions are satisfied*

a) *Either $n\equiv 2 \pmod 3$ or $\sum_0^{t(3)} n_{i3}\le 2$*

b) *For all odd primes $P>3$, $\sum_0^{t(P)} n_{iP}\le P-1$,*

then n must be one of the numbers 2, 6, 10, 30.

Since the proofs of these lemmas would seriously interrupt our main line of reasoning, they are omitted here and given in full in Appendix I.

LEMMA 5. *For odd $p>1$, we cannot have $Q_p(y)\equiv(Ay+B)(T(y))^2$ ($A\neq 0$, $T(y)$ a polynomial) unless $p=5$. ($Q_5(y)\equiv 2y-1$).*

PROOF: By (2.1) and Lemma 1, c), the degree of $Q_p(y)$ is $(p-3)/2$. The degree of $T(y)$ would therefore be $(p-5)/4$. Since this must be an integer, we have $p\equiv 1 \pmod 4$. Setting $2r=p+1$ we have

$$2r\equiv 2 \pmod 4. \tag{2.4}$$

The assumption, together with (2.1), (2.2) (ii) and condition c) of Lemma 1 now imply

$$B_{2r}(x)-B_{2r}\equiv x^2(x-1)^2(ax^2-ax+b)(c_0x^{r-3}+\cdots+c_{r-3})^2 \tag{2.5}$$

where a, b, c_i $(i=0, 1, \ldots, r-3)$ are rational numbers.

On the other hand we have from [25], p. 123: $B_{2r}(x)\equiv \sum_0^{2r}\binom{2r}{j}\cdot B_j\cdot x^{2r-j}$. Since by assumption $p>1$, we have $B_{2r-1}=B_p=0$, and hence

$$B_{2r}(x)-B_{2r}\equiv \sum_0^{2r-2}\binom{2r}{j}\cdot B_j\cdot x^{2r-j}. \tag{2.6}$$

Let P be an arbitrary odd prime. By the Staudt-Clausen Theorem ([28], Ch. IX), PB_j is an integer modulo P, and if $j\neq 0$,

$$\begin{aligned} PB_j&\equiv 0 \quad (\text{mod } P) \quad \text{if} \quad j\not\equiv 0 \ (\text{mod } P-1),\\ PB_j&\equiv -1 \ (\text{mod } P) \quad \text{if} \quad j\equiv 0 \ (\text{mod } P-1). \end{aligned} \tag{2.7}$$

Consequently all the coefficients of

$$P(B_{2r}(x)-B_{2r})\equiv \sum_0^{2r-2}\binom{2r}{j}(PB_j)\,x^{2r-j}$$

are integers modulo P. Using (2.5) and applying a trivial extension of Gauss's Theorem to integers modulo P we have

$$\sum_0^{2r-2}\binom{2r}{j}(PB_j)\,x^{2r-j}\equiv x^2(x-1)^2(\bar{a}x^2-\bar{a}x+\bar{b})(\bar{c}_0x^{r-3}+\cdots+\bar{c}_{r-3})^2 \tag{2.8}$$

where $\bar{a}$, $\bar{b}$, $\bar{c}_i$ $(i=0, 1, \ldots, r-3)$ are integers modulo P. We equate coefficients and obtain $PB_0=P=\bar{a}\cdot\bar{c}_0^2$. Since $\bar{a}$ and $\bar{c}_0$ are integers modulo P we must have

$$\bar{a}\equiv 0 \ (\text{mod } P) \qquad \bar{c}_0\not\equiv 0 \ (\text{mod } P). \tag{2.9}$$

Further equating of coefficients yields

$$\binom{2r}{2}PB_2=Pr(2r-1)/6=\bar{a}(3\bar{c}_0^2+\bar{c}_1^2+2\bar{c}_0\bar{c}_2-6\bar{c}_0\bar{c}_1)+\bar{b}\cdot\bar{c}_0^2.$$

But from (2·9) it then follows that $\bar{b}\cdot\bar{c}_0^2\equiv Pr(2r-1)/6 \ (\text{mod } P)$.

If either $P\neq 3$, or $P=3$ but $r\not\equiv 1 \pmod 3$, it is clear that $\bar{b}\cdot\bar{c}_0^2\equiv 0 \pmod P$, and on account of (2.9) this implies

$$\bar{b}\equiv 0 \pmod P). \tag{2.10}$$

Together with the fact that the $\bar{c}_i$ are integers modulo P, (2.9) and (2.10) imply that all the coefficients of the left-hand member of (2.8) vanish modulo P, i.e. $\binom{2r}{j}(PB_j)\equiv 0 \pmod P$, $(j=0,1,\cdots,2r-2)$. By virtue of (2.7) this is equivalent to $\binom{2r}{f(P-1)}\equiv 0 \pmod P$ for all f such that $0<f(P-1)\leq 2r-2$. If we set $2r=\sum_0^{t(P)} r_{iP}P^i$, where $0\leq r_{iP}\leq P-1$, we must have, by Lemma 3,

$$\sum_0^{t(P)} r_{iP}\leq P-1. \tag{2.11}$$

Formula (2.11) holds whenever (2.10) holds, i.e. for all odd primes P, $P=3$ being excepted when $r\equiv 1 \pmod 3$, which means $2r\equiv 2 \pmod 3$. Therefore, taking into account (2.4), the assumptions of Lemma 4 are satisfied for $2r$, and therefore $2r$ must be one of the numbers 2, 6, 10, 30.

The case $2r=2$ is excluded by the assumption $p>1$. For $2r=10$, a simple computation yields $Q_9(y)\equiv(y-1)(2y^2-3y+3)$ which is not of the required form. The case $2r=30$ could be settled in the same way, but to avoid tedious computation the following indirect method is used.

Since $r=15$, $\binom{2r}{j}PB_j\equiv 0 \pmod P$ for all odd primes P including 3. This implies that $\binom{2r}{j}\cdot 2B_j$ is an integer for every j. From (2.5) and (2.6) we obtain

$$\sum_0^{2r-2}\binom{2r}{j}\cdot 2B_j x^{2r-j}\equiv x^2(x-1)^2(a'x^2-a'x+b')(c_0'x^{r-3}+\cdots+c_{r-3}')^2 \tag{2.12}$$

where we may assume that a', b', c_i' $(i=0,1,\ldots,r-3)$ are integers. Equating coefficients, $2B_0=2=a'c_0'^2$, and therefore

$$a'=2 \qquad c_0'^2=1. \tag{2.13}$$

It is clear from Lemma 1, a), that $c_{r-3}'\neq 0$. Comparing the next-to-last coefficients of (2.12) we obtain, after use of (2.13) and division by c_{r-3}', $c_{r-3}'=b'(c_{r-4}'-c_{r-3}')$.

This implies that b' is a factor of c_{r-3}'. Considering the last coefficient in (2.12),

$\binom{2r}{2r-2}(2B_{2r-2}) = b' c'^2_{r-3}$, we see that all its prime factors divide it more than once. However, $\binom{30}{28} \cdot 2B_{28} = -7 \cdot 3\,392\,780\,147$ and the second factor is not divisible by 7. This eliminates the case $2r = 30$.

The only remaining case is $2r = 6$, i.e. $p = 5$, and indeed $Q_5(y) \equiv 2y - 1$.

3. Numerical properties of $S_p(n)$

LEMMA 6. *Let $P(x)$ be a polynomial with integral coefficients, and let $Q(x) \equiv ax + b$, with a and b relatively prime integers, be algebraically prime to $P(x)$. There exists an integer $D(a, b, P(x))$ such that the following properties are satisfied:*

a) *For any integer n, every common factor of the numbers $P(n)$, $Q(n)$ is a factor of D.*

b) *There exists n_0 such that D divides both $P(n_0)$, $Q(n_0)$.*

PROOF: We perform the algebraic division of $P(x)$ by $Q(x)$ and obtain

$$P(x) \equiv (ax + b) \cdot T(x) + r. \tag{3.1}$$

If we apply Ruffini's Rule for the determination of r and of the coefficients of $T(x)$, we find that on multiplying (3.1) through by a^s (s the degree of $P(x)$) we obtain

$$a^s \cdot P(x) \equiv (ax + b) \cdot T'(x) + r'$$

where r' and the coefficients of $T'(x)$ are now integers.

Let D be the largest factor of r' that is relatively prime to a. Then

$$a^s \cdot P(x) \equiv (ax + b) \cdot T'(x) + r'' \cdot D. \tag{3.2}$$

We now substitute an arbitrary integer n for the variable in (3.2). Any common factor h of $P(n)$ and $an + b$ will be a factor of $r'' \cdot D$. Since h divides $an + b$, and $(a, b) = 1$ by assumption, we must have $(a, h) = 1$. By the definition of D, h must then divide D. Property *a*) of D is thus proved.

Let n_0 be a root of the congruence $an + b \equiv 0 \pmod{D}$, which is soluble since $(a, D) = 1$. On substitution of n_0 in (3.2), both terms in the right-hand member become divisible by D. Therefore D divides $a^s \cdot P(n_0)$, but since $(a, D) = 1$, D must also divide $P(n_0)$. This completes the proof.

The number $D(a, b, P(x))$ is thus uniquely defined except for the sign, which we shall assume positive always. It is a kind of "numerical GCF" of $P(x)$ and $Q(x)$·

We now apply Lemma 6 to the study of $S_p(n)$.

LEMMA 7. *The numbers* $D(1, 0, P_p(x))$, $D(1, 1, P_p(x))$, $D(2, 1, P_p(x))$ *are well-defined for all* $p>1$, *and furthermore,* $D(1, 0, P_p(x))=D(1, 1, P_p(x))=D(1, 0, Q_p(y))$.

PROOF: The first part follows from Lemma 1, a) and Lemma 6. The equalities follow from Lemma 1, b) and c), and in fact the common value of the three numbers is the constant term of $P_p(x)$ or $Q_p(y)$.

We shall henceforth invariably use the notation

$$D_p=D(1, 0, Q_p(y)) \qquad D'_p=D(2, 1, P_p(x)).$$

The following result is useful for the study of particular cases of the diophantine equation.

LEMMA 8. *Let n be an arbitrary integer, and let h be a common factor of* $P_p(n)$ *and* $2n+1$. *Then the GCF of h and* $P_p(n)/h$ *is a factor of* D'_p/h.

We omit the proof, which proceeds by considering the even polynomial $P'(z)$ obtained as $P'(2x+1)\equiv P_p(x)$.

COROLLARY. *If* D'_p *is squarefree, then for any integer n and any common factor h of* $P_p(n)$ *and* $2n+1$, *we have* $(P_p(n)/h, h)=1$.

4. The Equation $S_p(n)=m^q$. Number of Solutions

The purpose of this section is the investigation of the equation

$$S_p(n)=1^p+2^p+\cdots+n^p=m^q \tag{4.1}$$

and the determination of the cases in which the number of solutions is either finite or infinite. The answer to this question is given, with a more precise statement about the number of solutions, in Theorem 1 below.

We shall first make a few remarks of a trivial nature, which will, however, be quoted repeatedly in the sequel.

REMARK I. If $q=1$, the equation is obviously satisfied for any n and a matching m. This case will be spoken of as a trivial one.

REMARK II. For any given p, if q_1 is a factor of q_2, the values of n corresponding to solutions of (4.1) for $q=q_2$ will be among those corresponding to solutions for $q=q_1$.

REMARK III. For any values of p, q, the set $n=m=1$ is a solution of the equation. It will be referred to as the trivial solution.

REMARK IV. Since $S_3(n)=(S_1(n))^2$ for all n, the following statement holds: If q_0 is odd [even], and $n=n_0$, $m=m_0$ is a solution of (4.1) for

$$p=1,\ q=q_0 \quad [p=1,\ q=q_0/2],$$

then

$$n=n_0,\ m=m_0^2 \quad [n=n_0,\ m=m_0]$$

is a solution of (4.1) for $p=3$, $q=q_0$; and in this way all the solutions of this case may be obtained. In particular, if $p=3$, $q=2$ we have, by Remark I, a trivial case for $p=1$, $q=1$, and hence this case shall be called trivial for $p=3$ also.

We shall require the following theorems:

THEOREM A. (Nagell, Ljunggren, Domar). *The equation*

$$|Ax^q-By^q|=1$$

has at most two solutions in positive integers x, y for $q\geq 3$. If $q=3$, 4 there is at most one solution.

This special case of the Thue-Siegel Theorem is proved for $q=3$ by Nagell [24] and for $q=4$ by Ljunggren [16]. For $q\geq 5$ it is proved by Domar [9].

THEOREM B. (Landau-Ostrowski-Thue). *Let a, b, c, d, be integers such that $a(b^2-4ac)\neq 0$. If $r\geq 3$, the equation*

$$ax^2+bx+c=dy^r$$

has only a finite number of solutions in integers x, y. ([8], Th. 118, [11], Satz 695).

THEOREM C. *Let $f(x)$ be a polynomial of degree ≥ 3 with integral coefficients, and assume that all its roots are distinct. Then, if c is any integer, the equation*

$$f(x)=cy^2$$

has only a finite number of solutions in integers x, y. ([31]).

The main result of this section is the following:

THEOREM 1. *For given values of p and q, the number of solutions of* (4.1) *is infinite only in the trivial cases $q=1$ and $p=3$, $q=2$, and in the cases $p=1$, $q=2$; $p=3$, $q=4$; $p=5$, $q=2$. In all other cases the number of solutions $N(p,q)$ is finite and $N(p,q)\leq N_0(p)$, where $N_0(p)$ is a function of p alone.*

PROOF: We shall consider separately the cases $p=1$, p even, and p odd and ≥ 3.

1. $p=1$. By Lemma 1, equation (4.1) becomes $n(n+1)/2=m^q$. Splitting into relatively prime factors we have, according to the parity of n, either $n=2x^q$, $n+1=y^q$ or $n=x^q$, $n+1=2y^q$. Therefore one of the equations

$$y^q-2x^q=1 \qquad x^q-2y^q=-1 \tag{4.2}$$

must hold. If $q=2$, these are "Pellian" equations and have an infinite number of solutions. We shall give the formula for them in Section 6. If $q\geq 3$, Theorem A implies that equations (4.2) have between them at most two solutions, and so the theorem is proved in this case with $N_0(1)=2$.

2. p *even*. According to Lemma 1, (4.1) has the form

$$\frac{1}{k(p)}\cdot n(n+1)(2n+1)\cdot P_p(n)=m^q. \tag{4.3}$$

Since the left-hand member is an integer for every integral value of n, there exist, for a given n, the integers k_1, k_2, k_3, k_4 (not necessarily uniquely defined), such that $k_1k_2k_3k_4=k(p)$, and such that n/k_1, $(n+1)/k_2$, $(2n+1)/k_3$, $P_p(n)/k_4$ are all integers. The three first of these are obviously relatively prime in pairs. We now set

$$d_1=(n/k_1,\ P_p(n)/k_4) \qquad d_2=((n+1)/k_2,\ P_p(n)/k_4)$$
$$d_3=((2n+1)/k_3,\ P_p(n)/k_4).$$

By Lemmas 6 and 7 it is clear that d_1, d_2 are factors of D_p and d_3 is a factor of D_p'. Furthermore, d_1, d_2, d_3 are also obviously relatively prime in pairs. It follows that

$$n/k_1d_1 \qquad (n+1)/k_2d_2 \qquad (2n+1)/k_3d_3 \qquad P_p(n)/k_4d_1d_2d_3$$

are integers relatively prime in pairs. If we substitute these numbers in (4.3) we obtain

$$d_1^2\cdot d_2^2\cdot d_3^2\cdot\frac{n}{k_1d_1}\cdot\frac{n+1}{k_2d_2}\cdot\frac{2n+1}{k_3d_3}\cdot\frac{P_p(n)}{k_4d_1d_2d_3}=m^q. \tag{4.4}$$

We shall first consider q odd and ≥ 3. We may set

$$d_1=a_1^qb_1c_1e_1 \qquad d_2=a_2^qb_2c_2e_2 \qquad d_3=a_3^qb_3c_3e_3 \tag{4.5}$$

in such a way that:

a) $b_1c_1e_1$, $b_2c_2e_2$, $b_3c_3e_3$ are qth-power-free.

b) all prime factors of b_1 are factors of n/k_1d_1; all prime factors of b_2 are factors of $(n+1)/k_2d_2$; all prime factors of b_3 are factors of $(2n+1)/k_3d_3$.

c) All prime factors of $c_1 c_2 c_3$ are factors of $P_p(n)/k_4 d_1 d_2 d_3$.

d) $(e_1 e_2 e_3,\ n/k_1 d_1) = (e_1 e_2 e_3,\ (n+1)/k_2 d_2) = (e_1 e_2 e_3,\ (2n+1)/k_3 d_3)$
$= (e_1 e_2 e_3,\ P_p(n)/k_4 d_1 d_2 d_3) = 1.$

The decomposition thus defined is clearly unique. The b_i, c_i, e_i $(i = 1, 2, 3)$ are all relatively prime in pairs. (Remark: For the purposes of this proof, d_3 need not have been factored. However, the complete factoring is the appropriate background for the study of particular cases (Stction 5)).

We now substitute (4.5) into (4.4) and regroup the factors in such way that all except the first will certainly be relatively prime in pairs:

$$(a_1^2 a_2^2 a_3^2)^q \cdot \left(b_1^2 \cdot \frac{n}{k_1 d_1}\right) \cdot \left(b_2^2 \cdot \frac{n+1}{k_2 d_2}\right) \cdot \left(b_3^2 \cdot \frac{2n+1}{k_3 d_3}\right) \cdot \left(c_1^2 c_2^2 c_3^2 \cdot \frac{P_p(n)}{k_4 d_1 d_2 d_3}\right) \cdot e_1^2 \cdot e_2^2 \cdot e_3^2 = m^q. \quad (4.6)$$

We may divide through by a qth power and thus eliminate the first factor. All the remaining factors, being relatively prime in pairs, must be perfect qth-powers. From condition a) of their definition, and since q is odd, it follows that $e_1 e_2 e_3 = 1$. If the first two remaining factors are x^q, y^q we obtain on division by b_1, b_2 respectively

$$b_1 \cdot n = k_1 c_1 (a_1 x)^q \qquad b_2 \cdot (n+1) = k_2 c_2 (a_2 y)^q. \quad (4.7)$$

The numbers $k_1, k_2, b_1, b_2, c_1, c_2$ are factors of either $k(p)$ or D_p. The number of possible sets of values of these is therefore bounded by a bound $N'(p)$ which depends, through $k(p)$ and D_p, on p alone.

Let $f_1 = (b_1, k_1)$, $f_2 = (b_2, k_2)$. Let h_1, h_2 be the least integers such that b_1/f_1, b_2/f_2 divide h_1^q, h_2^q respectively. Since $(b_1, c_1) = (b_2, c_2) = 1$, it is clear that if (4.7) is to hold we may set $a_1 x = h_1 X$, $a_2 y = h_2 Y$. Thus

$$n = (k_1/f_1)\, c_1 (h_1^q f_1/b_1) \cdot X^q = A X^q$$
$$n + 1 = (k_2/f_2)\, c_2 (h_2^q f_2/b_2) \cdot Y^q = B Y^q$$

and therefore (4.7) implies

$$B Y^q - A X^q = 1. \quad (4.8)$$

The number of sets of values of A, B is still $\leq N'(p)$. For each set, (4.8) has, by Theorem A, at most 2 solutions. Equation (4.3) has therefore at most $2N'(p)$ solutions in this case.

We now consider the case $q = 2$. In (4.4) we may divide through by squares, and since the last four factors in the left-hand member are relatively prime in pairs they must be perfect squares. In particular

$$n = k_1 d_1 \cdot x^2 \qquad n+1 = k_2 d_2 \cdot y^2 \qquad 2n+1 = k_3 d_3 \cdot z^2$$

and combining these we have

$$4 k_1 k_2 d_1 d_2 \cdot (xy)^2 + 1 = (k_3 d_3)^2 \cdot z^4.$$

The coefficients of this equation can only take a finite number of sets of values, and for each such set the equation has, according to Theorem B, only a finite number of solutions; and so has therefore (4.3). This is for $q = 2$, but according to Remark II, this result holds for any even q, and $N(p, 2q') \leq N(p, 2)$. Combining this result with the previous one, the theorem is proved for p even and we may set $N_0(p) = \max\{2N'(p), N(p, 2)\}$.

3. $p \geq 3$, *odd*. By Lemma 1, (4.1) has now the form

$$\frac{1}{k(p)} \cdot n^2 (n+1)^2 \cdot P_p(n) = m^q. \tag{4.9}$$

Consider in the first place the case q odd and ≥ 3. In a way quite similar to that followed for p even, there exist, for every integer n, integers k_1, k_2, k_3, such that $k_1 k_2 k_3 = k(p)$ and such that n^2/k_1, $(n+1)^2/k_2$, $P_p(n)/k_3$ are integers. We then set

$$d_1 = (n^2/k_1, P_p(n)/k_3) \qquad d_2 = ((n+1)^2/k_2, P_p(n)/k_3)$$

and by Lemmas 6 and 7, d_1, d_2 are factors of D_p^2. We now factor d_1 and d_2 in a way completely similar to that established in (4.5). Substitution in (4.9) yields

$$(a_1^2 a_2^2)^q \cdot \left(b_1^2 \cdot \frac{n^2}{k_1 d_1}\right) \cdot \left(b_2^2 \cdot \frac{(n+1)^2}{k_2 d_2}\right) \cdot \left(c_1^2 c_2^2 \cdot \frac{P_p(n)}{k_3 d_1 d_2}\right) \cdot e_1^2 \cdot e_2^2 = m^q$$

where $e_1 e_2 = 1$ as before, and all factors except the first are certainly relatively prime. Therefore

$$b_1^2 \cdot n^2 = k_1 d_1 \cdot x^q \qquad b_2^2 \cdot (n+1)^2 = k_2 d_2 \cdot y^q. \tag{4.10}$$

Since the left-hand members are perfect squares, and since $q = 2q' + 1$ is odd, we must have $k_1 d_1 x = x'^2$, $k_2 d_2 y = y'^2$. (4.10) implies

$$b_1 (k_1 d_1)^{q'} \cdot n = x'^q \qquad b_2 (k_2 d_2)^{q'} \cdot (n+1) = y'^q. \tag{4.11}$$

As above, the number of sets of values of $k_1, k_2, d_1, d_2, b_1, b_2$ (factors of either $k(p)$ or D_p^2) is bounded by a number which we shall also denote by $N'(p)$ and which depends on p alone.

Let h_1, h_2 be the last integers such that $b_1 (k_1 d_1)^{q'}$, $b_2 (k_2 d_2)^{q'}$ divide h_1^q, h_2^q, and let A, B be the quotients of these divisions. If (4.11) is to hold, we may set $x' = h_1 X$, $y' = h_2 Y$. Then $n = A X^q$, $n+1 = B Y^q$, and we again obtain equation (4.8). The number of sets of values of A, B being $\leq N'(p)$, the number of solutions of (4.9) is again at most $2N'(p)$ in this case.

Consider now $q=2$. Set $k(p) = K^2 \cdot k'$, with k' squarefree. Equation (4.9) then reduces to

$$P_p(n) = Q_p(n(n+1)) = k' u^2. \tag{4.12}$$

Set $Q_p(y) \equiv (Q'(y))^2 \cdot R(y)$ where $R(y)$ has only simple roots. We may assume $Q'(y)$ and $R(y)$ to have integral coefficients (Gauss). Equation (4.12) then reduces to

$$R(n(n+1)) = k' v^2. \tag{4.13}$$

If the degree of $R(y)$ is ≥ 3, then the diophantine equation $R(w) = k' v^2$ has only a finite number of solutions in integers w, v, since $R(y)$ has only simple roots (Theorem C). The same holds a fortiori for (4.13). If the degree of $R(y)$ is 2, we examine $R(x(x+1))$ as a polynomial in x. It is easy to verify that there is a multiple root if and only if either: (i) $R(y)$ has a multiple root, which is excluded by construction, or: (ii) $x = -1/2$ is a root of $R(x(x+1))$, which is excluded by Lemma 1, a). It follows that $R(x(x+1))$ (which is of degree 4) has no multiple root, and therefore (4.13) has only a finite number of solutions (Theorem C). We conclude that, if the degree of $R(y)$ is ≥ 2, $N(p, 2)$ is finite, and by Remark II, $N(p, 2q') \leq N(p, 2)$, so that for these values of p the theorem is proved and we may set

$$N_0(p) = \mathrm{Max}\,\{2N'(p),\ N(p, 2)\}.$$

It remains to examine the cases for which the degree of $R(y)$ is 0 or 1. By Lemmas 2 and 5, this is the case only for $p=3$, $p=5$ respectively. Case $p=3$ is disposed of by Remark IV, which yields the result required by the statement of the theorem, again with $N_0(3) = 2$. As for $p=5$, $Q_5(y) \equiv 2y-1$, $k' = 3$, and (4.13) may be written

$$(2n+1)^2 - 6v^2 = 3 \tag{4.14}$$

which has an infinite number of solutions, each one providing a solution of (4.9). We shall give these solutions in Section 6. Consider now $p=5$, $q=4$. Since $D_5 = 1$ and since every fourth power is also a square we must have

$$(2n+1)^2 + 3 = 6v^4$$

and this equation has only a finite number of solutions by Theorem B. (In Section 6 we shall prove that there is none but the trivial solution). The theorem is thus proved also for $p=5$, with $N_0(5)=\max\{2N'(5),\ N(5,4)\}$, since any even number other than 2 is a multiple of 4 or of an odd number other than 1; the conclusion follows from Remark II. The proof of Theorem 1 is thus complete.

REMARK. A referee pointed out that, as far as finiteness of the number of solutions is concerned, Theorem 1 could be deduced from Siegel's theorem ([27]): *If $f(x, y)$ is a polynomial with rational coefficients which is irreducible in the field of all algebraic numbers (or in the field of complex numbers) and if the genus of the Riemann surface of $f(x, y)=0$ is positive, then there are only finitely many pairs of numbers a, b (a an integer, b rational), such that $f(a, b)=0$.*

We note that $y^q-S_p(x)$ is reducible if $p=3$ and q is even, but by Lemmas 1 and 2 is irreducible otherwise. The reducible case is disposed of by Remark IV. In the irreducible case we refer to the genus calculations in [2], pp. 231–239. From the results there obtained it follows that $y^q-S_p(x)=0$ has a Riemann surface the genus of which is 0 if and only if $q=1$ or if $S_p(x)$ is of one of the forms $(R(x))^q(x-a)^r$ or $(R(x))^q(x-a)^r(x-b)^{q-r}$ where $0\leq r<q$ and $R(x)$ is some polynomial. Thus by Lemmas 1, 2 and 5 it follows that in the irreducible cases the genus is 0 if $q=1$ or if $p=1$, $q=2$ or if $p=5$, $q=2$ but is otherwise positive. Application of the above-mentioned theorem then yields Theorem 1 as far as the finiteness of the number of solutions is concerned.

In concluding, it may be noted that, just as $2N'(p)$ could be explicitly computed from p, a similar bound can be given for $N(p, 2q')$, by an appropriate use of Theorem A, except if $q'=1$ or if p is odd and $q'=2$.

5. The Equation $S_p(n)=m^q$. Odd Values of q

5.1. Methods and theorems. In this section we shall give methods to find odd primes q for which the equation has none but the trivial solution. Apart from the trivial application of Remark II of Section 4, we point out that the same methods apply to certain composite odd numbers while failing for all their prime factors; but we shall not pursue this remark further.

The first method we shall describe is essentially one of congruences. The application to be made is similar to the method used by Dénes [5], to Fermat's Theorem. Less general theorems have been proved by Vandiver [30] and Ankeny and Erdös [1].

For any positive integer h, let Γ_h denote the set consisting of 0 and of the $2h$th roots of unity. Let $Z_{2h}(x)$ denote the cyclotomic polynomial of order $2h$ (its degree is $\varphi(2h)$.) Let $N(\eta)$ denote the norm of the algebraic number η.

Consider a set of polynomials in s variables with integral coefficients

$$P = \{P_k(x_1, x_2, \dots, x_s) : k = 1, \dots, t\}. \tag{5.1}$$

Let h be a positive integer. For every set $\{\gamma_1, \gamma_2, \dots, \gamma_s\}$ of s elements chosen in Γ_h, consider the set of numbers

$$\{N(P_k(\gamma_1, \gamma_2, \dots, \gamma_s)) : k = 1, \dots, t\} \tag{5.2}$$

The sets (5.2) form a class $S(P, h)$.

LEMMA 9. *Let P be a class of polynomials as defined by* (5.1), *and let q be an odd prime. If there exists a positive integer h such that $r = 2hq + 1$ is a prime and such that r does not simultaneously divide all the numbers of any one of the sets in $S(P, h)$, then the set of equations*

$$P_k(u_1^q, u_2^q, \dots, u_s^q) = 0 \qquad k = 1, \dots, t \tag{5.3}$$

has no solution in integers $u_1, u_2, \dots, u_s$.

PROOF: It will be sufficient to prove the lemma for the case of two variables, the proof being entirely similar in the general case.

With the exception of 0, the qth power residues modulo r form a cyclic subgroup of order $(r-1)/q = 2h$ of the multiplicative group of non-zero residues. Let g be a generator of this subgroup; this statement is equivalent to

$$Z_{2h}(g) \equiv 0 \pmod r. \tag{5.4}$$

We now consider the set of equations (5.3) modulo r and substitute u_1^q, u_2^q by their residues modulo r. We obtain one of the following sets of congruences:

$$\begin{aligned} P_k(0,0) &\equiv 0 \pmod r \quad k = 1, \dots, t \quad \text{(i)} \\ P_k(g^{j_1}, 0) &\equiv 0 \pmod r \quad k = 1, \dots, t \quad \text{(ii)} \\ P_k(0, g^{j_2}) &\equiv 0 \pmod r \quad k = 1, \dots, t \quad \text{(iii)} \\ P_k(g^{j_1}, g^{j_2}) &\equiv 0 \pmod r \quad k = 1, \dots, t \quad \text{(iv)} \end{aligned} \tag{5.5}$$

where $0 \le j_1, j_2 < 2h$. If (5.3) is to have solutions, one at least of (5.5), must hold. Assume for instance that a set of type (iv) holds for some choice of j_1, j_2. In order that it may hold simultaneously with (5.4), the algebraic resultants

$$\boldsymbol{R}(P_k(x^{j_1}, x^{j_2}),\ Z_{2h}(x)), \quad k=1, \ldots, t$$

must all vanish modulo r.

Let ξ be a primitive $2h$th root of unity, i.e. a root of $Z_{2h}(x)$. Using a well-known relation ([29], Sect. 28), the result just mentioned may be restated as

$$\boldsymbol{N}(P_k(\xi^{j_1}, \xi^{j_2}))\equiv 0 \pmod r \qquad k=1, \ldots, t.$$

Applying this method to all choices of j_1, j_2, as well as to the sets of congruences of types (i), (ii), (iii) in (5.5), we obtain precisely the sets in $S(P, h)$, and the proof of the lemma is complete.

We now define $\boldsymbol{L}_h$ to be the class of all odd primes q such that $2hq+1$ is a prime. (Note that every q belongs at least to one, and in fact to an infinite number, of these classes). Since the class of sets $S(P, h)$ depends on h, but not on q, we obtain the following alternative formulation of Lemma 9.

COROLLARY. *Let P be defined as in Lemma 9. Let h be a given positive integer. If among the sets in $S(P, h)$ there is none such that all its elements vanish, then the set of equations* (5.3) *has solutions for at most a finite number of primes q in $\boldsymbol{L}_h$, namely for those for which $r=2hq+1$ divides all the elements of some one set of $S(p, h)$.*

REMARK 1. Since in our applications one of the polynomials in P is often of the form ax_1+bx_2+1, it is often useful to apply the following result which we state without proof (for the method, see [1]; there is, however, no restriction on h such as in that paper): *If $P(x_1, x_2, \ldots, x_s)\equiv a_1x_1+\cdots+a_sx_s+k$, $k\neq 0$, then if for some h and some choice of $\gamma_1, \gamma_2, \ldots, \gamma_s$ in Γ_h we have $P(\gamma_1, \gamma_2, \ldots, \gamma_s)=0$ this same equality must already hold for some choice of the γ_i in Γ_1 (i.e. either 0 or ± 1).*

REMARK 2. In both Lemma 9 and its Corollary the fact that q is a prime is irrelevant· Although this remark may extend the field of application of this method, it was not followed up in numerical computation; neither was the simple relation $\boldsymbol{N}(P_k(\gamma_1, \gamma_2, \ldots, \gamma_s))<\sigma_k^{\varphi(2h)}$, where σ_k is the sum of the absolute values of the coefficients of P_k.

REMARK 3. In applying the Corollary of Lemma 9 to any particular set of equations, it may be possible to prove impossibility for all q in a given $\boldsymbol{L}_h$, if the exceptional values of q for which r divides all the elements of some set in $S(P, h)$ also belong to some other $\boldsymbol{L}_{h'}$, in which they are not exceptional. This remark is widely used in the applications.

We shall now require some definitions and notations. $\boldsymbol{R}$ will denote the class of all regular primes (in the sense of Kummer). Let s be any prime. We shall say that a prime $q \geq 7$ belongs to the class $\boldsymbol{A}_s$ if s belongs to an even exponent modulo q; and that q belongs to the class $\boldsymbol{B}_s$ if s belongs to either an even exponent or the exponent $(q-1)/2$ modulo q. Finally, q shall belong to the class $\boldsymbol{C}_s$ if $s^{q-1} \not\equiv 1 \pmod{q^2}$.

In terms of these notations the following lemma is a restatement of some results of Dénes [6].

LEMMA 10. *The equation $x^q + y^q = cz^q$ (c an integer prime to q) has no solution in integers x, y, z except the trivial ones (i.e. $|xyz| = 0, 1$, if x, y, z are assumed to have no common factor), in the following cases:*

a) $c = 2^{u_2}$ and $q \in \boldsymbol{R} \cap \boldsymbol{B}_2 \cap \boldsymbol{C}_2$

b) $c = 2^{u_2} \cdot 3^{u_3}$ and $q \in \boldsymbol{R} \cap \boldsymbol{A}_2 \cap \boldsymbol{A}_3 \cap (\boldsymbol{C}_2 \cup \boldsymbol{C}_3)$

c) $c = 2^{u_2} \cdot 5^{u_5}$ and $q \in \boldsymbol{R} \cap \boldsymbol{A}_2 \cap \boldsymbol{A}_5 \cap (\boldsymbol{C}_2 \cup \boldsymbol{C}_5)$

d) $c = 2^{u_2} \cdot 3^{u_3} \cdot 5^{u_5}$ and $q \in \boldsymbol{R} \cap \boldsymbol{A}_2 \cap \boldsymbol{A}_3 \cap \boldsymbol{A}_5 \cap (\boldsymbol{C}_2 \cup \boldsymbol{C}_3 \cup \boldsymbol{C}_5)$.

PROOF: Case a) is a restatement (and a trivial extension if $u_2 \neq 1$) of [6], Th. 9. Cases b), c), d) follow immediately from [6], Th. 7, under the additional assumptions

$$\text{b)}\ \frac{1}{f_2} + \frac{1}{f_3} \leq \frac{q-3}{2(q-1)} \qquad \text{c)}\ \frac{1}{f_2} + \frac{1}{f_5} \leq \frac{q-3}{2(q-1)} \qquad \text{d)}\ \frac{1}{f_2} + \frac{1}{f_3} + \frac{1}{f_5} \leq \frac{q-3}{2(q-1)} \tag{5.6}$$

respectively, where f_s denotes the exponent to which s belongs modulo q. A straightforward computation shows that (5.6) b) is satisfied for all q except 7, which does not belong to $\boldsymbol{A}_2$ (only $q \geq 7$ are considered); (5.6) c) holds for all q except 7, 31, neither of which belongs to $\boldsymbol{A}_2$; (5.6) d) holds for all q except 7, 11, 13, 31, of which 7, 31 do not belong to $\boldsymbol{A}_2$ and 11, 13 do not belong to $\boldsymbol{A}_3$. The lemma is therefore proved.

Regularity and irregularity of primes are now known for primes up to 2000 ([14]). In Appendix II we have collected the data relevant to Lemmas 9 and 10 for all regular primes less than 1000, note being taken of the fact that in the applications the Corollary of Lemma 9 was applied for $h = 1, \ldots, 6$. It is known that the only primes less than 16000 which do not belong to $\boldsymbol{C}_2$ are 1093 and 3511 ([3]).

We shall also require some results concerning equations of degrees 3 and 5. Concerning the former, we have the following restatement of part of the comprehensive results of Selmer ([26]).

THEOREM D. *If a, b, c are cubefree integers, the equation $a x^3+b y^3+c z^3=0$ has no solutions but the trivial ones (i.e. with $xyz=0$) if $|abc|$ is one of the numbers contained in Table 4^q of* [26]; *and also in the cases contained in Table 2^a of* [26]. *If $|abc|=2$, there are none but the trivial solutions $xyz=0$ and $|x|=|y|=|z|$.*

A special case of Theorem A for $q=3$ is this:

THEOREM E (Nagell). *If D is a multiple of* 3 *and has no prime factors of the form $6h+1$, the equation $x^3+Dy^3=1$ has none but the trivial solution $x=1$, $y=0$, unless $D=9$.* ([23]).

THEOREM F (Lebesgue). *The equation $x^5+y^5=cz^5$ has none but the trivial solutions (i.e. $|xyz|=0,1$ if x, y, z are assumed to have no common factor) if c has no prime factor of the form $10h+1$ and furthermore $c\not\equiv\pm1$, ±7* (mod 25). ([12]).

5.2. Cases $p=1$, $p=3$. Lemma 10 a), Theorems D and F, and Remark II in Section 4 imply that equations (4.2) have none but the trivial solutions and therefore the equation (4.1) for $p=1$ has none but the trivial solution $n=m=1$, whenever q is a multiple of 3, 5, or of any prime in $\boldsymbol{R}\cap\boldsymbol{B}_2\cap\boldsymbol{C}_2$. Remark IV then disposes of the case $p=3$ for q odd or twice an odd number (we include this case in this section for $p=3$) and at the same time a multiple of any of the primes mentioned.

5.3. Other cases. Due to lack of space, we shall not discuss the different cases in detail. After giving the general data for $p=2,\ldots,11$ (which will also serve for Section 6) we shall make some general remarks about the cases with odd q and give two examples of how the method applies.

		p even		
p	$k(p)$	$Q_p(y)$	D_p	D'_p
2	6	1	1	1
4	30	$3y-1$	1	7
6	42	$3y^2-3y+1$	1	31
8	90	$5y^3-10y^2+9y-3$	3	$3\cdot127$
10	66	$(y-1)(3y^3-7y^2+10y-5)$	5	$5\cdot7\cdot73$

For $p=8$, $Q_8(n(n+1))\equiv6$ (mod 9) for every integer n, so that it is divisible by exactly one factor 3 of $k(8)$, and thus $d_1d_2=1$, and $d_3=1$ or 127. For $p=10$ we set

$$Q_{10}(y)\equiv(y-1)\cdot S(y) \text{ and find: } D(1,0,y-1)=D(1,-1,S(y))=1;$$
$$D(1,0,S(y))=D(2,1,x(x+1)-1)=5;\ D(2,1,S(x(x+1)))=7\cdot73.$$

In all cases considered, D_p and D'_p are squarefree, so that, in (4.6), we have $a_1 a_2 a_3 = 1$. By the Corollary to Lemma 8, $c_3 = 1$.

p odd

p	$k(p)$	$Q_p(y)$	D_p
5	12	$2y-1$	1
7	24	$3y^2-4y+2$	2
9	20	$(y-1)(2y^2-3y+3)$	3
11	24	$2y^4-8y^3+17y^2-20y+10$	10

For both $p=7$, $p=11$, $Q_p(n(n+1)) \equiv 2 \pmod 4$ for all n, so that it is divisible by exactly one factor 2 of $k(p)$. Therefore for $p=7$, $d_1 d_2 = 1$; and for $p=10$, $d_1 d_2 = 1, 5$. As for $p=9$, we set $Q_9(y) \equiv (y-1) \cdot S(y)$ and it is clear that $n(n+1)-1$ and $S(n(n+1))$ are relatively prime for all n.

The general method of attack for both even and odd values of p consists in eliminating n between the various factors in (4.6) (and in the corresponding equation for p odd), which are known to be perfect qth powers. A set of equations is thus obtained for every set of values of the coefficients. This set is tested by the congruence methods of Lemma 9 and its corollary. The computational difficulties have limited us in general to $h \leq 6$; in the case $p=10$ the number of equations and the values of their coefficients were so high that the computations could not be carried out, and in the case $p=11$ they were limited to $h=1$.

In those cases in which the Corollary of Lemma 9, completed with Remark 3 following it, breaks down (as it must, since equation (4.1) possesses the trivial solution and therefore no simple congruence method can settle it completely), we apply Lemma 10 and Theorems A, D, E, F. In the cases $p=2$, $p=5$, the congruence method adds nothing to the knowledge we obtain through these theorems, and can therefore be dispensed with. Theorems A and E (for $q=3$) are required only for the cases $p=9$, 10, 11, and will therefore not appear in the given examples. The results obtained for these as well as for the other values of p considered, with q odd, are given in Section 7 (Theorem 2).

As examples we shall now discuss the cases $p=4$ and $p=7$.

Case $p=4$. According to the data above, we have $d_1 d_2 = 1$, $b_3 = d_3$. Therefore the following equations must hold:

$$n = k_1 x^q \quad n+1 = k_2 y^q \quad d_3(2n+1) = k_3 z^q \quad 3n(n+1)-1 = k_4 d_3 t^q.$$

Elimination of n provides the equations

$$k_2 y^q - k_1 x^q - 1 = 0 \quad d_3 k_1 x^q + d_3 k_2 y^q - k_3 z^q = 0 \quad 3 k_1 k_2 (xy)^q - k_4 d_3 t^q = 0. \tag{5.7}$$

For $q=3$, these equations are treated by congruences modulo 7, 9, 13, and those cases that are not incompatible are settled by means of Theorem D. Taking into account that n must be positive, this yields the trivial solution $n=m=1$ as the unique solution of (4.1). A similar conclusion is reached for $q=5$ by means of congruences modulo 11 and 25 and use of Theorem F.

In the general case ($q \neq 3, 5$) the Corollary of Lemma 9 and the subsequent Remarks 1 and 3 are applied to (5.7) for $h \leq 6$. (*Note*: In view of the fact that our result will be restricted by other considerations to $q \in \boldsymbol{R} \cap \boldsymbol{B}_2 \cap \boldsymbol{C}_2$, it was not considered necessary to check cases under Remark 3 for values of q not in this class.) The method breaks down only in the following cases:

$$\text{(i) } k_1 k_2 = 2\,; \ \text{(ii) } d_3 = k_3 = k_1 = 1\,; \ \text{(iii) } d_3 = k_3 = k_2 = 1.$$

In case (i) the first of equations (5.7) has no non-trivial solutions for $q \in \boldsymbol{R} \cap \boldsymbol{B}_2 \cap \boldsymbol{C}_2$ by Lemma 10, a). In cases (ii) and (iii) the equation obtained in eliminating y or x, respectively, between the first two equations (5.7) similarly has no non-trivial solution for the same class of values of q. Only in case (i) do the trivial solutions yield the trivial solution $n=m=1$ of the original equation; in the other two cases they yield the absurd value $n(n+1)=0$. We conclude that for $p=4$ the original equation has none but the trivial solution $n=m=1$ for $q=3$, 5, or $q \in \boldsymbol{R} \cap \boldsymbol{B}_2 \cap \boldsymbol{C}_2 \cap \bigcup_1^6 \boldsymbol{L}_h$ (or multiples of these).

Case $p=7$. From the above data we conclude $d_1 d_2 = 1$, and hence the following hold:

$$n^2 = k_1 x^q \qquad (n+1)^2 = k_2 y^q \qquad Q_7(n(n+1)) = k_3 t^q.$$

We may set $k_3 = 2k_3'$, and $k_3' = 1, 3$ as is easily seen. We thus have either of the two sets

$$\begin{aligned} n^2(n+1)^2 &= \ \ 4(xy)^q \qquad Q_7(n(n+1)) = 6t^q \\ n^2(n+1)^2 &= 12(xy)^q \qquad Q_7(n(n+1)) = 2t^q. \end{aligned} \tag{5.8}$$

In the first case, since q is odd and x, y are relatively prime, we must have $x=X^2$, $y=Y^2$, and therefore $n(n+1)=2(XY)^q$, whence either of the equations

$$Y^q - 2X^q = 1, \ X^q - 2Y^q = -1$$

holds; and these have no non-trivial solutions for $q=3$ (Theorem D), $q=5$ (Theorem F) or $q \in \boldsymbol{R} \cap \boldsymbol{B}_2 \cap \boldsymbol{C}_2$ (Lemma 11, a)). In all these cases the trivial solutions yield only $n = m = 1$.

In the second case of (5.8), the left-hand member of the first equation being a square and q odd, we must have $xy = 3(XY)^2$. This implies

$$n(n+1) = 2 \cdot 3^{(q+1)/2} \cdot (XY)^q,$$

whence one of the following equations must hold:

$$\begin{aligned} 2 \cdot 3^{(q+1)/2} \cdot Y^q - X^q &= 1 \\ 3^{(q+1)/2} \cdot Y^q - 2X^q &= 1 \end{aligned} \tag{5.9}$$

or those obtained by substituting $(-X)$, $(-Y)$ for X, Y, respectively, in these equations; since q is odd, these last two cases need not be considered separately. The first equation (5.9) has none but the trivial solution for $q = 3$ (Theorem D), $q = 5$ (Theorem F) or $q \in \boldsymbol{R} \cap \boldsymbol{A}_2 \cap \boldsymbol{A}_3 \cap (\boldsymbol{C}_2 \cup \boldsymbol{C}_3)$ (Lemma 11, b)); the trivial solution yields $n = 0$, which is excluded.

Consider the second equation (5.9). For $q = 3$ we obtain $9Y^3 - 2X^3 = 1$, which is impossible modulo 9; for $q = 5$ we have $27Y^5 - 2X^5 = 1$, which is impossible modulo 11. In the general case ($q \neq 3, 5$) we obtain, in conjunction with the second equation of the second set of (5.8),

$$\begin{aligned} 3^{(q+1)/2} \cdot Y^q - 2X^q &= 1 \\ 2 \cdot 3^{q+2} \cdot (XY)^{2q} - 4 \cdot 3^{(q+1)/2} \cdot (XY)^q + 1 &= t^q. \end{aligned}$$

The Corollary of Lemma 9 cannot be applied directly, but this set may be transformed to

$$\begin{aligned} 3(3Y^2)^q - (2X^q + 1)^2 &= 0 \\ 48 \cdot X^{2q} \cdot (3Y^2)^q - (18X^{2q} \cdot (3Y^2)^q - t^q + 1)^2 &= 0 \end{aligned} \tag{5.10}$$

to which the Corollary may be applied. We do this for $h \leq 6$. We note that 3, and therefore $3Y^2$, is a quadratic residue modulo $r = 2hq + 1$ for $h \equiv 0, 1, 5 \pmod 6$, and a non-residue otherwise; this follows from the quadratic reciprocity law and the fact that r, q are prime and $\neq 3$. This fact may be used to restrict the choice of the γ_i in (5.2) and hence the sets of $S(P, h)$ for which the assumption of Lemma 9 and its Corollary must hold. With the help of Remark 3 to the Corollary, we are able to show that (5.10) is impossible for all $q \in \bigcup_{1}^{6} \boldsymbol{L}_h$.

Combining the previous results, we conclude that for $p=7$ and $q=3, 5$, or

$$q \in \boldsymbol{R} \cap \boldsymbol{A}_2 \cap \boldsymbol{A}_3 \cap \boldsymbol{C}_2 \cap \bigcup_1^6 \boldsymbol{L}_h$$

(or multiples of these), there is no solution of the original equation other than the trivial one $n=m=1$.

6. The Equation $S_p(n)=m^q$. Even Values of q

6.1. Preliminary theorems. We shall require some facts about certain "Pellian" equations $x^2-Dy^2=a$ (D square-free). For the elementary theory of these equations, see, e.g., [28], Ch. XI. We shall be interested in particular in the equations

$$x^2-2y^2=\pm 1. \tag{6.1}$$

The non-negative solutions of (6.1) are all given by the general relation

$$x_s+y_s\sqrt{2}=(1+\sqrt{2})^s \tag{6.2}$$

for non-negative s, in such a way that

$$x_s^2-2y_s^2=(-1)^s. \tag{6.3}$$

A few trivial facts concerning these solutions are:

$$(x_s, y_s)=(x_s, x_{s+1})=(x_s, x_{s+2})=1. \tag{6.4}$$

y_s is even or odd according as s is even or odd, and

$$(y_{2r-1}, y_{2r+1})=(y_{2r}/2, y_{2r+2}/2)=1. \tag{6.5}$$

According as $r\equiv 0, 1, 2, 3 \pmod 3$, we have respectively

$$x_{2r}\equiv 1, 3, 5, 3 \pmod{12} \qquad y_{2r}/2\equiv 0, 1, 0, 5 \pmod 6. \tag{6.6}$$

A more interesting property of the x_s, y_s is as follows: from (6.2) we have

$$x_{2r}+y_{2r}\sqrt{2}=(x_r+y_r\sqrt{2})^2$$

and therefore $x_{2r}=x_r^2+2y_r^2$. Combining this result with (6.3),

$$x_{2r}=(2y_r)^2+(-1)^r. \tag{6.7}$$

One further type of "Pellian" equation which we consider is

$$x^2 - 6y^2 = 3 \tag{6.8}$$

the general solution of which is

$$x + y\sqrt{6} = (3 + \sqrt{6})(5 + 2\sqrt{6})^r \qquad r = 0, 1, 2, \dots. \tag{6.9}$$

LEMMA 11. *The equation* $9x^4 - 1 = 8y^2$ *has no solution except the trivial one* $|x| = |y| = 1$.

PROOF: By congruence modulo 16, y must be odd. Thus the only way of factoring $(3x^2 - 1)(3x^2 + 1) = 8y^2$ admissible modulo 3 is such that we obtain the equations

$$2v^2 - u^2 = 1, \quad 2v^2 + u^2 = 3x^2,$$

and according to a result of Lucas ([21]), this set implies $|u| = |v| = |x| = 1$.

LEMMA 12. *The equations*

$$x^{2s} - 2y^{2s} = \pm 1 \qquad s \neq 1 \tag{6.10}$$

have no solutions except the trivial ones $y = 0$, $x = \pm 1$ *(for the plus sign) and* $|x| = |y| = 1$ *(for the minus sign).*

(*Note:* A theorem of Liouville ([15]), implies this result for the equation with the plus sign for all s for which Fermat's Theorem holds.)

PROOF: Without loss of generality we may assume that s is a prime. For $s = 2$, the lemma is a well-known result of Fermat (see [13], Th. IV; [28], Ch. XII). We may therefore assume from now on that s is an odd prime. Consider first the equation with the minus sign. It may be put in the form

$$X^2 + 1 = 2Y^s \qquad (X = x^s, \ Y = y^2),$$

and this equation has no non-trivial solutions unless $s = 4$ (see [17]) and this is excluded.

For the equation with the plus sign, (6.10) may be considered as a case of (6.1), and therefore by (6.3) and (6.7) we may set $x^s = z^2 \pm 1$. The minus sign cannot hold, since x is odd and the left-hand side would have to be factored into perfect sth powers differing by 2. We therefore have $x^s = z^2 + 1$, and an elementary argument in the field of Gaussian integers shows that this has no non-trivial solutions (see, e.g. [4], Th. II).

LEMMA 13. *The equation* $4x^s-1=3y^{2s}$, $s\neq 1$, *has none but the trivial solution* $|x|=|y|=1$.

PROOF: We may again assume that s is a prime. If $s=2$, the first member can be factored; the only factoring compatible modulo 3 is $2x-1=u^4$, $2x+1=3v^4$, so that $3v^4-u^4=2$. This equation has none but the trivial solution $|u|=|v|=1$ (see [16]).

We then assume that s is odd. We rewrite the equation as

$$1+3Y^2=4x^s; \qquad (Y=y^s).$$

By congruence modulo 8 it follows that x must be odd. A result of Ljunggren ([18]) then implies that, if there are non-trivial solutions, s must divide the class number of $K(\sqrt{-3})$ (K the rationals), but this class number is 1.

6.2. Cases $p=1$, $p=3$. The equations for $p=1$ are (4.2). If q is even but $q\neq 2$, Lemma 12 implies that there is none but the trivial solution $n=m=1$. The remaining case is $p=1$, $q=2$, which has, according to Theorem 1, an infinite number of solutions. Instead of using (4.2), we obtain directly from $n(n+1)/2=m^2$ the equation $(2n+1)^2-8m^2=1$. We have then from (6.1), (6.2), (6.3) the result:

$$n=(x_{2r}-1)/2, \quad m=y_{2r}/2 \quad \text{for } r=1,2,\ldots.$$

As for $p=3$, it is disposed of by Remark IV; the cases with q even but double an odd number were already discussed in Section 5; the cases with q a multiple of 4 are covered by the above result for $p=1$.

6.3. Cases with p even. From the data in the preceding section, (4.4) implies, for $p=2,4,6,8$, $q=2$:

$$n=k_1x^2 \quad n+1=k_2y^2 \quad 2n+1=k_3d_3z^2 \quad Q_p(n(n+1))=k_4d_3t^2.$$

For the case $p=10$ see below.

Case $p=2$. Here $k_1k_2k_3=6$. By means of congruences modulo 3 we eliminate all the cases except

$$\text{(i)}\ k_1=1,\ k_2=2,\ k_3=3; \qquad \text{(ii)}\ k_1=6,\ k_2=k_3=1.$$

In case (i) we square the third of the above equations and obtain, substituting the first and the second, $9z^4-1=8(xy)^2$. According to Lemma 11, this equation has none but trivial solutions, which yield $n=m=1$.

In case (ii) it follows that $z^2-2y^2=-1$ and therefore by (6.1), (6.2), (6.3) we may set

$$\begin{aligned} z &= x_{2r+1} = x_{2r} + 2y_{2r} = 2y_{2r+2} - x_{2r+2} \\ y &= y_{2r+1} = x_{2r} + y_{2r} = x_{2r+2} - y_{2r+2}. \end{aligned} \tag{6.11}$$

On the other hand we must have $6x^2 = z^2 - y^2$ and using (6.11) this may be written $6x^2 = (z-y)(z+y) = y_{2r} \cdot y_{2r+2}$. Since both factors in the right-hand member are even, x must be even, and we have

$$6(x/2)^2 = (y_{2r}/2)(y_{2r+2}/2). \tag{6.12}$$

By (6.5) the factors in the right-hand member are relatively prime, and using (6.6) we see that they must be $6u^2$, v^2 in some order, where $uv = x/2$. Set $y_{2s} = 2v^2$ (either $s=r$ or $s=r+1$) and substitute in (6.3); we find $x_{2s}^2 - 1 = 8v^4$. There are only two ways of factoring this compatible with the fact that x_{2s} is odd. If

$$x_{2s} = 4a^4 + 1 = 2b^4 - 1$$

we obtain $b^4 - 2a^4 = 1$ which has only the trivial solution $a=0$ (Lemma 12) and this implies the excluded value $n=0$. Thus $x_{2s} = 2a^4 + 1 = 4b^4 - 1$ and $a^4 - 2b^4 = -1$, whence by Lemma 12 $|a| = |b| = 1$, and $x_{2s} = 3$. This implies $s=1$. If now $r = s-1 = 0$, we should have $n = 6x^2 = y_0 y_2 = 0$, which is excluded. Therefore $r = s = 1$, and

$$n = y_2 y_4 = 24.$$

We find $S_2(24) = 4900 = 70^2$, so that $m = 70$. This is thus the only non-trivial solution. Since 70 is not a perfect power, the equation for $p=2$, q even but $q \neq 2$ has none but the trivial solution.

(*Note:* Lucas [22] derived the final argument from a theorem of Gérono [10]. Cf. also [20]. Although Lucas solved the case $p=q=2$ completely in [22] (cf. also [19]) we have included a proof, mainly since the argument will be used again.)

Cases $p=4, 8$. By appropriate congruences we can eliminate all the combinations of values of k_1, k_2, k_3, k_4, d_3 except $k_1 = d_3 = 1$, $k_2 = 2$, $k_3 = 3$. This case coincides, as far as the first three equations are concerned, with the case (i) for $p=2$, and thus $n = m = 1$ is the only solution.

Case $p=6$. By appropriate congruences, the only cases remaining are:

(i) $k_1 = d_3 = 1$, $k_2 = 2$, $k_3 = 3$, which coincides with case (i) for $p=2$ and yields none but the trivial solution $n=m=1$; and (ii): $k_1=42$, $k_2=k_3=d_3=1$. Following the reasoning for case (ii) of $p=2$, we obtain, corresponding to (6.12),

$$42\,(x/2)^2 = (y_{2r}/2)\,(y_{2r+2}/2).$$

This time the factors in the right-hand member must be either $42\,u^2$ and v^2, or $6\,u^2$ and $7\,v^2$, in some order, with $uv=x/2$. In the first case the procedure is identical with that for $p=2$, but leads to $y_4=12=84\,u^2$ which is absurd. We may thus assume that $y_{2s}=12\,u^2$ ($r=s$ or $r+1=s$). Substitution in (6.3) yields $288\,u^4=x_{2s}^2-1$. There are only four ways of factoring compatible with the fact that x_{2s} is odd. Of these, only two are possible modulo 4: If $x_{2s}=144a^4+1=2b^4-1$, we get $b^4-72a^4=1$, which may be transformed to $b^4+(6a^2)^4=((6a^2)^2+1)^2$, which is of the form $x^4+y^4=z^2$ and has no non-trivial solutions (see e.g. [28], Ch. XII). This leads to $n=0$, which is excluded. If $x_{2s}=16a^4+1=18b^4-1$, we get $(3b^2)^2-8a^4=1$. This equation, as we have seen in the case $p=2$, leads to $a=0$ or $a=1$. $a=0$ implies $n=0$ which is excluded. From $a=1$ we have $b=1$, $x_{2s}=17$, $s=2$. According as $r=s$ or $r=s-1$ we obtain $y_6=70=14\,v^2$, $y=2=14\,v^2$, both of which are absurd. Case (ii) therefore yields no additional solutions.

Case $p=10$. Here we take advantage of the peculiar algebraic structure of $Q_{10}(y)$ (see Section 5). By means of appropriate congruences, all possible cases for $q=2$ are eliminated except those containing the equation $n(n+1)-1=u^2$. But this may be written $(2n+1)^2-(2u)^2=5$. It follows that we must have

$$2n+1+2u=5, \quad 2n+1-2u=1,$$

whence $n=1$, and thus $n=m=1$ is the only solution.

We have thus shown that for $p=2, 4, 6, 8, 10$ and $q=2$ there is no non-trivial solution of (4.1) except the solution $n=24$, $m=70$ for $p=2$. For q even but $q\neq 2$ there is, by Remark II of Section 4, none but the trivial solution in any of these cases.

6.4. Cases with p odd ≥ 5. We set $q=2q'$. Since, for the values of p considered, $d_1 d_2$ is squarefree, and 4 is the only square factor of $k(p)$, we may set $k(p)=4k'$ and the reasoning which led to (4.12) yields the equations

$$n(n+1)=2\,(xy)^{q'} \qquad Q_p(n(n+1))=k'\cdot t^{2q'}. \tag{6.13}$$

The first of these equations is precisely the equation we obtain in the case $p=1$, $q=q'$. Solvability of this case is thus a necessary condition for that of (6.13). The results of the discussion of the case $p=1$ in this section and the preceding one may thus be applied (see Theorem 2).

(*Note:* Simple conditions can be given for p odd in order that (6.13) should hold; we shall not, however, go into this matter).

We are, however, able to prove more than what has just been stated, at least for $p=5, 7, 9$.

Case $p=5$. The case $q'=1$ has, according to Theorem 1, an infinite number of solutions. By (4.14), (6.8) and (6.9), all the solutions are given by

$$n=(x-1)/2, \qquad m=y(3y^2+1)/4$$

where x, y are given by (6.9).

For $q' \neq 1$, we substitute the first equation of (6.13) in the second and obtain $4(xy)^{q'}-1=3t^{2q'}$, which by Lemma 13 has none but the trivial solutions for all q'; this implies $n=m=1$.

Case $p=7$. We shall only examine the case $q'=2$ in addition to the general remarks made above. In the second equation (6.13), set $n(n+1)=2z$, and we obtain $2(3z-1)^2+1=9t^4$, as is easily verified from the data in Section 5. Since t must be odd, $3z-1$ is even, say $3z-1=2w$. Thus $9t^4-1=8w^2$, and by Lemma 11 this has none but the trivial solution, which yields $n=m=1$.

Case $p=9$. Consider $q'=1$. Since $Q_9(y)\equiv(y-1)\cdot S(y)$, the second of equations (6.13) splits into

$$n(n+1)-1=k_3'u^2 \qquad S(n(n+1))=k_3''v^2$$

where $k_3'k_3''=k'=5$. If $k_3'=1$, the first of these equations may be written

$$(2n+1)^2-(2u)^2=5,$$

which clearly implies $n=1$, and hence $m=1$ also. If $k_3'=5$, $n(n+1)\equiv 1 \pmod 5$, and hence $t^2=S(n(n+1))\equiv 2 \pmod 5$, which is absurd.

The results obtained in these cases are completed by a reference to Remark II in Section 4.

7. Summary of Particular Cases and Conjectures

The results of the two preceding sections are collected in Theorem 2. The classes of primes $\boldsymbol{L}_h$, $\boldsymbol{R}$, $\boldsymbol{B}_s$, $\boldsymbol{A}_s$, $\boldsymbol{C}_s$ are defined in Section 5. If u is an integer, $[u]$ will denote the class of all multiples of u, and $[u]^*$ the class of all multiples of u exclusive of u itself. If $\boldsymbol{U}$ is a certain class of integers, $[\boldsymbol{U}]$ will denote the class of all numbers that are multiples of at least one integer in $\boldsymbol{U}$.

THEOREM 2. *All the solutions of the equation $S_p(n) = m^q$ are given in the following cases:*

a) *If $q=1$ or if $p=3$, $q=2$; every value of n provides a solution.*

b) *If $p=1$, $q=2$ or if $p=3$, $q=4$, the number of solutions is infinite; they are all given by $n=(x_{2r}-1)/2$, $m=y_{2r}/2$, where $x_r + y_r\sqrt{2} = (1+\sqrt{2})^r$, $r=1,2,3,\ldots$.*

c) *If $p=5$, $q=2$, the number of solutions is infinite; they are all given by $n=(x-1)/2$, $m=y\,(3y^2+1)/4$, where $x+y\sqrt{6}=(3+\sqrt{6})\,(5+2\sqrt{6})^s$, $s=0,1,2,\ldots$.*

d) *If $p=2$, $q=2$, the only solutions are $n=m=1$ and $n=24$, $m=70$.*

e) *In the following cases the equation has none but the trivial solution $n=m=1$:*

p	q *odd* (q *belongs to* :)	q *even*; $q=2q'$ (q' *belongs to* :)
1	$[3] \cup [5] \cup [\boldsymbol{R} \cap \boldsymbol{B}_2 \cap \boldsymbol{C}_2]$	$[1]^*$
2	$[3] \cup [5] \cup [\boldsymbol{R} \cap \boldsymbol{B}_2 \cap \boldsymbol{C}_2]$	$[1]^*$
3	$[3] \cup [5] \cup [\boldsymbol{R} \cap \boldsymbol{B}_2 \cap \boldsymbol{C}_2]$	$[2]^* \cup [3] \cup [5] \cup [\boldsymbol{R} \cap \boldsymbol{B}_2 \cap \boldsymbol{C}_2]$
4	$[3] \cup [5] \cup [\boldsymbol{R} \cap \boldsymbol{B}_2 \cap \boldsymbol{C}_2 \cap \bigcup_1^6 \boldsymbol{L}_h]$	$[1]$
5	$[3] \cup [5] \cup [\boldsymbol{R} \cap \boldsymbol{A}_2 \cap \boldsymbol{A}_3 \cap \boldsymbol{C}_2]$	$[1]^*$
6	$[3] \cup [5] \cup [\boldsymbol{R} \cap \boldsymbol{B}_2 \cap \boldsymbol{C}_2 \cap \bigcup_1^6 \boldsymbol{L}_h]$	$[1]$
7	$[3] \cup [5] \cup [\boldsymbol{R} \cap \boldsymbol{A}_2 \cap \boldsymbol{A}_3 \cap \boldsymbol{C}_2 \cap \bigcup_1^6 \boldsymbol{L}_h]$	$[2] \cup [3] \cup [5] \cup [\boldsymbol{R} \cap \boldsymbol{B}_2 \cap \boldsymbol{C}_2]$
8	$[3] \cup [5] \cup [\boldsymbol{R} \cap \boldsymbol{B}_2 \cap \boldsymbol{C}_2 \cap \bigcup_1^6 \boldsymbol{L}_h]$	$[1]$
9	$[3] \cup [5] \cup [\boldsymbol{R} \cap \boldsymbol{A}_2 \cap \boldsymbol{A}_3 \cap \boldsymbol{A}_5 \cap \boldsymbol{C}_2 \cap \bigcup_1^6 \boldsymbol{L}_h]$	$[1]$
10	$[3] \cup [5]$	$[1]$
11	$[3] \cup [5] \cup [\boldsymbol{R} \cap \boldsymbol{A}_2 \cap \boldsymbol{A}_3 \cap \boldsymbol{A}_5 \cap \boldsymbol{C}_2 \cap \boldsymbol{L}_1]$	$[2]^* \cup [3] \cup [5] \cup [\boldsymbol{R} \cap \boldsymbol{B}_2 \cap \boldsymbol{C}_2]$

Table 1 contains those primes from 7 to 997 which belong to each of the classes mentioned in Theorem 2. The table is based on the data in Appendix II.

It is interesting to find out what lowest bound we may obtain for the number of solutions in the cases not covered by Theorem 2, by means of an adequate use of Theorem A. In this connection it is convenient to sharpen Domar's result by using his own discussion of formula (8) in his paper [9]: *If we exclude a possible solution $|x| = |y| = 1$, the equation $|Ax^q - By^q| = 1$ has at most one solution in positive* *integers for* $q \geq 7$. Application of this statement yields the following bounds for the number $N(p, q) - 1$ of non-trivial solutions: ($q \geq 7$):

p	1	2	3	4	5	6	7	8	9	10	11
q odd	1	2	1	7	2	7	3	7	4	13	9
q even	0	0	1	0	0	0	1	0	0	0	1

It would seem that, except for $p = 4, 6, 8, 10$, these bounds cannot be improved by the use of Domar's result alone.

The results obtained in this paper give rise to the following conjecture:

Conjecture: *Disregarding the cases with an infinite number of solutions (specified by Theorem 1), the only non-trivial solution of the equation* $S_p(n) = m^q$ *is* $p = 2,\ q = 2,\ n = 24,\ m = 70$.

Table 1

$$\boldsymbol{R} \cap \boldsymbol{B}_2 \cap \boldsymbol{C}_2$$

```
  7   11   13   17   19   23   29   41   43   47   53   61   71   79   83
 97  107  109  113  137  139  163  167  173  179  181  191  193  197  199
211  227  229  239  241  251  269  277  281  313  317  331  349  359  367
373  383  397  419  443  449  457  479  487  499  503  509  521  563  569
571  599  641  643  661  701  709  719  733  739  743  769  787  823  829
853  857  859  863  883  907  941  947  967  977  983  991  997  (88 primes).
```

$$\boldsymbol{R} \cap \boldsymbol{B}_2 \cap \boldsymbol{C}_2 \cap \bigcup_{1}^{6} \boldsymbol{L}_h$$

```
  7   11   13   17   19   23   29   41   43   47   53   61   71   79   83
 97  107  109  113  137  139  163  173  179  181  191  193  199  211  229
239  241  251  269  277  281  313  331  349  359  367  373  383  397  419
443  449  479  487  499  503  509  569  571  599  641  643  661  709  719
733  739  743  769  787  823  829  853  857  863  883  907  941  947  977
997  (76 primes).
```

$$\boldsymbol{R} \cap \boldsymbol{A}_2 \cap \boldsymbol{A}_3 \cap \boldsymbol{C}_2$$

```
 17   19   29   41   43   53   61   97  113  137  139  163  173  193  197
211  241  269  281  317  331  349  373  397  449  457  499  509  521  569
571  641  643  661  701  739  769  787  853  857  859  883  907  941  977
997  (46 primes).
```

$$\boldsymbol{R} \cap \boldsymbol{A}_2 \cap \boldsymbol{A}_3 \cap \boldsymbol{C}_2 \cap \bigcup_{1}^{6} \boldsymbol{L}_h$$

```
 17   19   29   41   43   53   61   97  113  137  139  163  173  193  211
241  269  281  331  349  373  397  449  499  509  569  571  641  643  661
739  769  787  853  857  883  907  941  977  997  (40 primes).
```

$$R \cap A_2 \cap A_3 \cap A_5 \cap C_2 \cap \bigcup_1^6 L_h$$

17 29 41 43 53 61 97 113 137 163 173 193 241 281 349
373 397 449 509 641 643 661 769 787 853 857 883 907 977 997
(30 primes).

$$R \cap A_2 \cap A_3 \cap A_5 \cap C_2 \cap L_1$$

29 41 53 113 173 281 509 641 (8 primes).

Note: Total number of primes in interval considered: 165.
Regular primes among these: 100.

Appendix I: Proof of Lemmas 3 and 4

LEMMA 3. *Let P be a prime, n an arbitrary positive integer, and set $n = \sum_0^t n_i P^i$, where $0 \leq n_i \leq P-1$. (The n_i are the digits of n written to the base P, and are therefore uniquely determined.) Then $\binom{n}{m(P-1)} \equiv 0 \pmod P$ for all integers m such that $0 < m(P-1) < n$ if and only if $\sum_0^t n_i \leq P-1$.*

PROOF: 1. Let $r \leq n$ be a non-negative integer, and set $r = \sum_0^t r_i P^i$, where $0 \leq r_i \leq P-1$. It is well-known and easy to prove (e.g. by application of Legendre's rule for the exponent of a prime factor in a factorial) that $\binom{n}{r} \not\equiv 0 \pmod P$ if and only if $r_i \leq n_i$ for all i.

2. Assume that there exists an integer m, $0 < m(P-1) < n$, such that $\binom{n}{m(P-1)} \not\equiv 0 \pmod P$. Set $r = m(P-1)$. It follows from part 1 of the proof that $r_i \leq n_i$ for all i. Since moreover we have assumed $r < n$, equality cannot hold for all i, and therefore we obtain

$$\sum_0^t r_i < \sum_0^t n_i. \tag{A.1}$$

On the other hand, since $P \equiv 1 \pmod{P-1}$, we have

$$\sum_0^t r_i \equiv \sum_0^t r_i P^i = m(P-1) \equiv 0 \pmod{P-1}.$$

Since, however, we have assumed $r > 0$, this implies

$$\sum_0^t r_i \geq P-1 \tag{A.2}$$

and combining (A.1) and (A.2) we finally obtain $\sum_0^t n_i > P-1$, and this completes one-half of the proof.

3. Assume now that $\sum_0^t n_i > P-1$. Then there exists a "section" of the sequence of digits, say $n_j, \ldots, n_k$, such that $\sum_j^k n_i > P-1$, and such that this inequality does not hold for any sub-section. Since we have $n_i \leq P-1$ for every i, this section cannot consist of a single element. We now set

$$m_0 = P^j \cdot \left(1 + \sum_0^{k-j} n_{j+s}\left(\frac{P^s-1}{P-1}\right)\right) \neq 0. \tag{A.3}$$

Hence

$$m_0(P-1) = P^j \cdot \left(P-1 + \sum_0^{k-j} n_{j+s}(P^s-1)\right) = \left(P-1-\sum_{j+1}^{k} n_i\right)P^j + \sum_{j+1}^{k} n_i P^i. \tag{A.4}$$

Now by assumption $\sum_j^k n_i > P-1$, but $\sum_{j+1}^k n_i \leq P-1$, and therefore

$$P-1-n_j < \sum_{j+1}^{k} n_i \leq P-1,$$

whence we conclude

$$0 \leq P-1-\sum_{j+1}^{k} n_i < n_j \leq P-1. \tag{A.5}$$

If we finally set $r = m_0(P-1)$, it follows on inspection of (A.3) and (A.5) and from the fact that the determination of the digits of r is unique, that

$$r_j = P-1-\sum_{j+1}^{k} n_i < n_j; \qquad r_i = n_i \quad (i = j+1, \ldots, k);$$

and $r_i = 0 \leq n_i$ otherwise. Since we now have $r_i \leq n_i$ for all i, part 1 of the proof implies that $\binom{n}{m_0(P-1)} \not\equiv 0 \pmod{P}$; and since the inequality $r_j < n_j$ is a strict one and since $m_0 \neq 0$ by (A.3), we conclude that $0 < m_0(P-1) < n$, which completes the proof.

LEMMA 4. *Let n be a positive integer such that $n \equiv 2 \pmod 4$. If P is any odd prime, set $n = \sum_0^{t(P)} n_{iP}P^i$, where $0 \leq n_{iP} \leq P-1$. If both the following conditions are satisfied*

a) *Either $n \equiv 2 \pmod 3$ or $\sum_0^{t(P)} n_{i3} \leq 2$*

b) *For all odd primes $P > 3$, $\sum_0^{t(P)} n_{iP} \leq P-1$.*

then n must be one of the numbers 2, 6, 10, 30.

PROOF: It is obvious that the numbers mentioned satisfy a) and b). We shall now replace condition b) by the weaker one that the inequality be verified for $P=5, 7, 13$.

1. Since n is even and P is odd,

$$0\equiv n=\sum_{0}^{t(P)} n_{iP}P^i\equiv\sum_{0}^{t(P)} n_{iP} \pmod 2. \tag{A.6}$$

If $P\equiv 1 \pmod 4$ we have

$$2\equiv n\equiv\sum_{0}^{t(P)} n_{iP} \pmod 4 \tag{A.7}$$

and if $P\equiv -1 \pmod 4$

$$2\equiv n\equiv\sum_{0}^{t(P)} (-1)^i n_{iP} \pmod 4. \tag{A.8}$$

2. Applying condition b) and (A.7) to $P=5$ we obtain $n=5^c+5^d$. Applying condition a) and (A.8) to $P=3$ we distinguish the following three cases:

Case I: $n\equiv 2 \pmod 3$

Case II: $n\equiv 1 \pmod 3$; then $n=1+3^a$, $a\neq 0$, $a\equiv 0 \pmod 2$

Case III: $n\equiv 0 \pmod 3$; then $n=3^a+3^b$, $ab\neq 0$, $a\equiv b \pmod 2$.

3. *Case I.* Since $5^c+5^d\equiv 2 \pmod 3$, both c and d are even. Therefore $n\not\equiv 0 \pmod 7$. Application of condition b) and (A.6) to $P=7$ and the fact that we are in Case I yield $n=7^g+7^h$. But then $n\equiv 1, 2 \pmod 7$. In the latter case, $n=2$.

Excluding this case from now on, we have $n=1+7^h\equiv 1 \pmod 7$. Therefore $c\equiv d\equiv 2 \pmod 6$, and in particular $cd\neq 0$, so that $n\equiv 0 \pmod 5$. Therefore $h\equiv 2 \pmod 4$. On the other hand the above condition implies $n=5^c+5^d\equiv 5 \pmod 9$, so that $h\equiv 2 \pmod 3$. Thus finally $h\equiv 2 \pmod{12}$. This implies $n\equiv 11 \pmod{13}$, which contradicts condition b) and (A.7).

4. *Case II.* Since $5^c+5^d\equiv 1 \pmod 3$ it follows that c and d are odd, and therefore $n\equiv 3, 10, 0 \pmod{13}$. On the other hand, $1+3^a\equiv 2, 4, 10 \pmod{13}$. Thus we must have $n\equiv 10 \pmod{13}$. It now follows from condition b) and (A.7) for $P=13$ that $n=10$.

5. *Case III.* From $5^c+5^d\equiv 0 \pmod 3$ it follows that $c\not\equiv d \pmod 2$, and, say, c is even, d is odd.

Since $a\equiv b \pmod 2$ it follows that $n\not\equiv 0 \pmod 7$. Analysis of the combinations of values modulo 6 of c (even) and d (odd) which make this possible then shows that we must also have $n\not\equiv 0 \pmod 9$. This implies that a, b cannot both be ≥ 2.

Since neither can be 0 in Case III, one at least, say a, is 1, and consequently b also is odd.

If $b \equiv 1 \pmod 6$ it follows that $n \equiv 6 \pmod 7$, and by condition b) for $P=7$ it follows that $n=6$.

If $b \equiv 5 \pmod 6$ it follows that $n \equiv 12 \pmod{13}$, which contradicts condition b) and (A.7) for $P=13$.

Therefore, in the remaining discussion of this case, $b \equiv 3 \pmod 6$, and $n \equiv 2 \pmod 7$, $n \equiv 4 \pmod{13}$.

We now recall that c is even and d odd. If $c=0$, then $n=1+5^d \equiv 6, 9 \pmod{13}$, which contradicts the preceding. Thus $c \neq 0$ and $n \equiv 0 \pmod 5$. It follows that $b \equiv 3 \pmod 4$, and hence $n=3+3^b \equiv 14 \pmod{16}$.

Application of condition b) and (A.6) to $P=7$ and the fact that we are in Case III and that $n \equiv 2 \pmod 7$ yield $n=2+7^g+7^h+7^j+7^k$. Then $n \equiv 14 \pmod{16}$ implies that g, h, j, k are all odd. It is easy to verify that there is then no combination of these numbers which will make $n \equiv 0 \pmod{25}$. Therefore, since $c \geq 2$, we must have $d=1$. Taking into account $b \equiv 3 \pmod 6$ we may set $b=3b'$; and since $c=2c'$ is even we must have $n=3+3^{3b'}=5+5^{2c'}$. Therefore, setting $x=3^{b'}$, $y=5^{c'}$ we have $x^3-y^2=2$; but this diophantine equation has the unique solution $x=3$, $y=\pm 5$, as is well known (see, e.g., [28], Ch. XII). Therefore $b'=c'=1$, and $n=30$. The proof is thus complete.

Appendix II: Data concerning Primes

Of the 165 primes between 7 and 997, 65 are irregular:

37 59 67 101 103 131 149 157 233 257 263 271 283 293 307
311 337 347 353 379 389 401 409 421 433 461 463 467 491 523
541 547 557 577 587 593 607 613 617 619 631 647 653 659 673
677 683 691 727 751 757 761 773 797 809 811 821 827 839 877
881 887 929 953 971

The table in this appendix contains the following information concerning the regular primes q between 7 and 997:

a) The values of h such that $q \in \boldsymbol{L}_h$, for $h \leq 6$. If there is no such value, the least h is given in brackets.

b) The fact whether q belongs to $\boldsymbol{B}_2$, $\boldsymbol{A}_2$, $\boldsymbol{A}_3$, $\boldsymbol{A}_5$ (indicated by x in the appropriate column).

Note: Dénes [6] states that 2 belongs to exponents 35 modulo 281 and 281 modulo 563, whereas actually 2 belongs to exponents 70 modulo 281 and 562 modulo 563. In particular, [6], Th. 9 is also valid for 281.

q	h	B_2	A_2	A_3	A_5	q	h	B_2	A_2	A_3	A_5
7	2 3 5	x		x	x	251	1	x	x		
11	1 3 4	x	x			269	4 6	x	x	x	
13	2 3 5 6	x	x		x	277	2 3	x	x		x
17	3 4	x	x	x	x	281	1 6	x	x	x	x
19	5 6	x	x	x		313	3	x	x		x
23	1 3 6	x			x	317	(13)	x	x	x	x
29	1 4 6	x	x	x	x	331	3	x	x	x	
31	5 6			x		349	5	x	x	x	x
41	1	x	x	x	x	359	1	x			
43	2 5	x	x	x	x	367	3 5	x		x	x
47	3	x			x	373	2 3	x	x	x	x
53	1	x	x	x	x	383	6	x			x
61	3 6	x	x	x	x	397	3	x	x	x	x
71	4 6	x				419	1	x	x		
73	2 3 6			x	x	431	1 4				
79	2	x		x		439	5			x	
83	1 3 6	x	x		x	443	1 3	x	x		x
89	1 6			x	x	449	4	x	x	x	
97	2 5	x	x	x	x	457	(15)	x	x	x	x
107	3 4	x	x		x	479	4 6	x			
109	5	x	x			487	2 5	x		x	x
113	1	x	x	x	x	499	2	x	x	x	
127	2			x	x	503	3 6	x			x
137	3 4	x	x	x	x	509	1 4	x	x	x	x
139	2 6	x	x	x		521	(16)	x	x	x	x
151	3 5			x		563	(7)	x	x		x
163	2	x	x	x	x	569	6	x	x	x	
167	(7)	x			x	571	5	x	x	x	
173	1 3	x	x	x	x	599	4	x			
179	1 4	x	x			601	3 5 6				x
181	3 5	x	x	x		641	1 3	x	x	x	x
191	1 6	x				643	6	x	x	x	x
193	2 5	x	x	x	x	661	3 6	x	x	x	x
197	(9)	x	x	x	x	701	(9)	x	x	x	x
199	2 6	x		x		709	2	x	x		x
211	5	x	x	x		719	1 6	x			
223	6			x	x	733	5	x	x		x
227	(12)	x	x		x	739	2	x	x	x	
229	6	x	x		x	743	1	x			x
239	1 4	x				769	5	x	x	x	x
241	3 5	x	x	x	x	787	3	x	x	x	x

Table (count.)

q	h	B_2	A_2	A_3	A_5	q	h	B_2	A_2	A_3	A_5
823	5	x		x	x	919	2			x	
829	5 6	x	x			937	3 5			x	x
853	2 3	x	x	x	x	941	3 4	x	x	x	
857	4	x	x	x	x	947	3 4	x	x		x
859	(11)	x	x	x		967	(8)	x		x	x
863	3 6	x			x	977	4	x	x	x	x
883	2 5 6	x	x	x	x	983	(7)	x			x
907	3	x	x	x	x	991	(9)	x		x	
911	1					997	2	x	x	x	x

References

[1]. N. G. Ankeny and P. Erdös, The insolubility of classes of diophantine equations. *Am. Journ. Math.*, 76 (1954), 488–496.

[2]. Appell et Goursat, *Théorie des fonctions algébriques.* Paris 1929.

[3]. N. G. W. H. Beeger, On the congruence $2^{p-1} \equiv 1 \pmod{p^2}$ and Fermat's Last Theorem. *Nieuw Arch. Wiskunde*, 20 (1939), 51–54.

[4]. J. W. S. Cassels, On the equation $a^x - b^y = 1$. *Am. Journ. Math.* 75 (1953), 159–162.

[5]. P. Dénes, An extension of Legendre's criterion in connection with the first case of Fermat's last theorem. *Publ. Math. Debrecen*, 2 (1951), 115–120.

[6]. ——, Über die diophantische Gleichung $x^l + y^l = c z^l$. *Acta Math.*, 88 (1952), 241–251.

[7]. L. E. Dickson, *History of the Theory of Numbers*, Vol. II.

[8]. ——, *Introduction to the Theory of Numbers.* 1929.

[9]. Y. Domar, On the diophantine equation $|A x^n - B y^n| = 1$. *Math. Scand.*, 2 (1954), 29–32.

[10]. M. Gérono, Solution de la Question 1177. *Nouv. Ann. Math.* (2), 16 (1877), 230–234.

[11]. E. Landau, *Vorlesungen über Zahlentheorie.* 1927.

[12]. V. A. Lebesgue, Théorèmes nouveaux sur l'équation indéterminée $x^5 + y^5 = a z^5$. *Journal de Math.* (1), 8 (1843), 49–70.

[13]. A. M. Legendre, *Théorie des Nombres*, IV, N° 1. 1830.

[14]. D. H. Lehmer, E. Lehmer and H. S. Vandiver, An application of high-speed computing to Fermat's Last Theorem. *Proc. Nat. Acad. Sci. USA*, 40 (1954), 25–33.

[15]. J. Liouville, Sur l'équation $Z^{2n} - Y^{2n} = 2x^n$. *Journal de Math.* (1), 5 (1840), 360.

[16]. W. Ljunggren, Über die Lösung einiger unbestimmten Gleichungen vierten Grades. *Avhdl. Norske Vid. Akad.* Oslo (1935), 1–35.

[17]. ——, Zur Theorie der Gleichung $x^2 + 1 = D y^4$. *Avhdl. Norske Vid. Akad.* Oslo. I 5 (1942).

[18]. ——, Über die Gleichungen $1 + D x^2 = 2 y^n$, $1 + D x^2 = 4 y^n$. *Norske Vid. Selsk., Forhdl.*, 15 (1953), 115–118.

[19]. ——, New solution of a problem proposed by E. Lucas. *Norsk Math. Tidskr.*, 34 (1952), 65–72.

[20]. É. Lucas, Sur la résolution du système des équations $x^2 - 6 y^2 = u^2$, $x^2 + 6 y^2 = v^2$. *Nouv. Ann. Math.* (2), 15 (1876), 466–470.

[21]. ——, Sur la résolution du système des équations $2 v^2 - u^2 = w^2$ et $2 v^2 + u^2 = 3 z^2$ en nombres entiers. *Nouv. Ann. Math.* (2), 16 (1877), 409–416.

[22]. É. Lucas, Solution de la Question 1180. *Nouv. Ann. Math.* (2), 16 (1877), 429–432.

[23]. T. Nagell, Über die Einheiten in reinen kubischen Zahlkörpern. *Skrifter Vid. Selsk. Christiania* (1922).

[24]. ——, Solution complète de quelques équations cubiques à deux indéterminées. *Journal de Math.* (9), 4 (1925), 209–270.

[25]. N. E, Nörlund, Mémoire sur les polynômes de Bernoulli. *Acta Math.*, 43 (1922), 121–196.

[26]. E. S. Selmer, The diophantine equation $ax^3 + by^3 + cz^3 = 0$. *Acta Math.*, 85 (1951), 203–362.

[27]. C. L. Siegel, Über einige Anwendungen diophantischer Approximationen. *Abh. preuss. Akad. Wiss., phys.-math. Kl.* 1929, N° 1, 1–70.

[28]. J. V. Uspensky and M. A. Heaslet. *Elementary Number Theory.* 1939.

[29]. B. L. van der Waerden, *Modern Algebra.* 1949.

[30]. H. S. Vandiver, On classes of diophantine equations of higher degrees which have no solutions. *Proc. Nat. Acad. Sci. USA.*, 32 (1946), 101–106.

[31]. "X". Letter to L. J. Mordell. *Journal London Math. Soc.*, I (1926), 66–68.