Since the expression is zero for $\ell < k - s$ and for $1 > k - i$,

$$\therefore \quad P_k(x) = -\sum_{i=0}^{k}\sum_{m=0}^{k} i!\binom{k}{k-m} S_{(m,i)} F_{i+1} x^{k-m}$$

$$= \sum_{i=0}^{k}\sum_{m=0}^{k}\binom{k}{m} S_{(m,i)}\, i! F_{i+1} x^{k-m}.$$

*****

A CLASS OF DIOPHANTINE EQUATIONS*

S. P. MOHANTY
Indian Institute of Technology, Kanpur, India 208016

ABSTRACT

In this paper, we prove a theorem: If $k \equiv 5 \pmod 8$ and $f \not\equiv 2^{3t-1} \pmod{2^{3t}}$ for all positive integers t, then $c(3a^2b + kb^3) + d(a^3 + 3kab^2) = 16f$ has no solutions in integers $ab \neq 0$ if c and d are both odd integers. Then it is shown how this theorem enables us to solve the diophantine equations $y^2 - k = x^3$, $k \equiv 5 \pmod 8$. In the end, we give solutions for $k = 109, 116, 125, 133, 149, 157, 165, 173, 180$, and 181.

The Mordell equation $y^2 - k = x^3$, the simplest of all nontrivial diophantine equations of degree greater than 2, has interested mathematicians for more than three centuries, and has played an important role in the development of Number Theory.

We already know the complete solutions for $y^2 - k = x^3$, $|k| \leq 100$. The author in his doctroal dissertation (UCLA, 1971) has treated the range $100 < k \leq 200$. The present paper treats 10 particular cases in the above range.

First we prove two lemmas to prove the theorem.

Theorem 1: If $k \equiv 5 \pmod 8$, $f \not\equiv 2^{3t-1} \pmod{2^{3t}}$ for all positive integers t, then $c(3a^2b + kb^3) + d(a^3 + 3kab^2) = 16f$ has no solution in integers $ab \neq 0$ if c and d are both odd integers.

Lemma 1: Let $k \equiv 5 \pmod 8$ and c and d be odd integers. Then $c(3a^2b + kb^3) + d(a^3 + 3kab^2) = 0$ has only solution $a = 0$ and $b = 0$ in integers.

Proof: Suppose $a \neq 0$, $b \neq 0$ is a solution of

(1) $$c(3a^2b + kb^3) + d(a^3 + 3kab^2) = 0$$

in integers. ($a = 0$ implies $b = 0$, and conversely.) We see from (1) that $a \neq b$ and $a \equiv b \pmod 2$. Then $3a^2b + kb^3 = b(3a^2 + kb^2) \equiv 0 \pmod 8$ and $a^3 + 3kab^2 = a(a^2 + 3kb^2) \equiv 0 \pmod 8$, since $k \equiv 5 \pmod 8$.

Hence, $c(3a^2b + kb^3) + d(a^3 + 3kab^2) \equiv (3a^2b + kb^3) + (a^3 + 3kab^2) \pmod{16}$ as both c and d are odd integers. Then, from (1), we deduce that

(2) $$(3a^2b + kb^3) + (a^3 + 3kab^2) \equiv 0 \pmod{16}.$$

But

(3) $$a^3 + 3a^2b + kb^3 + 3kab^2 = (a + b)^3 + (k - 1)b^2(a + b) + 2(k - 1)ab^2.$$

Inserting $a + b = 2r$ and $k = 8\ell + 5$ in (3), we obtain

$$\begin{aligned} a^3 + 3a^2b + kb^3 + 3kab^2 &\equiv 8r(r^2 + b^2) + 8ab^2 \pmod{16} \\ &\equiv 8 \pmod{16} \text{ when both } a \text{ and } b \text{ are odd;} \\ &\equiv 0 \text{ or } 8 \pmod{16} \text{ when both } a \text{ and } b \text{ are even.} \end{aligned}$$

Then (2) implies that a and b are both even. Since $a \neq b$, suppose $a = 2^p m$ and $b = 2^q n$ where m and n are odd integers.

Now (a,b) is a solution of (1) implies that (a_1,b_1) is a solution of

$$c(3a_1^2b_1 + kb_1^3) + d(a_1^3 + 3ka_1b_1^2) = 0,$$

*AMS(MOS) subject classifications (1970) Primary 10B10. The preparation of this paper was partly supported by NSF grant G.P. 23113.

where $a_1 = 2^{p-1}m$ and $b_1 = 2^{q-1}n$. Arguing as before, we have both a_1 and b_1 even. If

(i) $p < q$, then $a_p = m$, $b_p = 2^{q-p}n$;

(ii) $p = q$, then $a_p = m$, $b_p = n$;

(iii) $p > q$, then $a_p = 2^{p-q}m$, $b_p = n$.

In all these cases we see that a_p and b_p are not both even. So we have a contradiction.

Lemma 2: Suppose $k \equiv 5 \pmod 8$ and c and d are odd integers. Then the necessary condition for the equation $c(3a^2b + kb^3) + d(a^3 + 3kab^2) = 16f$ to be solvable in integers is

$$f \equiv 2^{3t-1} \pmod{2^{3t}} \text{ or } f \equiv 0 \pmod{2^{3t}}.$$

Proof: In the proof of Lemma 1 we have shown that

$$c(3a^2b + kb^3) + d(a^3 + 3kab^2) \equiv 8 \pmod{16} \text{ when } a \text{ and } b \text{ are odd,}$$
$$\equiv 0 \text{ or } 8 \pmod{16} \text{ when } a \text{ and } b \text{ are even.}$$

From

(4) $$c(3a^2b + kb^3) + d(a^3 + 3kab^2) = 16f$$

we see that a and b are even. Suppose $a = 2a_1$ and $b = 2b_1$. Then we have

(5) $$c(3a_1^2b_1 + kb_1^3) + d(a_1^3 + 3ka_1b_1^2) = 2f.$$

The necessary condition for (5) to be solvable in integers is $f \equiv 0$ or $4 \pmod 8$, for in (5) $a_1 \equiv b_1 \pmod 2$, i.e., $f = 8f_1$ or $4 + 8f_1$. Hence, the lemma is true for $t = 1$. If $f \not\equiv 4 \pmod 8$ then $f = 8f_1$ and

(5') $$c(3a_1^2b_1 + kb_1^3) + d(a_1^3 + 3ka_1b_1^2) = 16f_1.$$

Arguing as before, $f_1 \equiv 0$ or $4 \pmod 8$, whence $f \equiv 0$ or $32 \pmod{64}$ and the proof follows by induction.

Proof of Theorem 1: By Lemma 2, the necessary condition for equation (4) to be solvable in integers is either $f \equiv 2^{3t-1} \pmod{2^{3t}}$ or $f \equiv 0 \pmod{2^{3t}}$. By hypothesis $f \not\equiv 2^{3t-1} \pmod{2^{3t}}$ for all positive integers t. Now $f \neq 0$ for $f = 0$ implies $a = b = 0$. Then there exists t_1 such that $f \not\equiv 0 \pmod{2^{3t_1}}$ for $f \equiv 0 \pmod{2^{3t}}$ for all t implies $f = 0$. Again, by hypothesis $f \not\equiv 2^{3t_1-1} \pmod{2^{3t_1}}$. Hence the equation is insoluble in integers $ab \neq 0$. If $f = 0$, then the equation has no solution in integers.

We need the following theorem, due to Hemer [1].

Theorem 2: If $2f$ has no prime factor which splits into two different prime ideals in the field $Q(\sqrt{k})$, then all the integer solutions of the equation $y^2 - kf^2 = x^3$ can be obtained by solving the $(3^{e+1} + 1)/2$ equations $N(\beta_i)\ (\pm y + f\sqrt{k}) = \eta \cdot \beta_i \cdot \alpha^3$ where (β_i) $(i = 1, 2, \ldots, 3^e)$ are the cubes of arbitrary ideals, one from each of the 3^e classes c_i with the property $c_i^3 = (1)$, α is an integer in $Q(\sqrt{k})$ and $\eta = 1$ or ε, where ε is the fundamental unit of $Q(\sqrt{k})$ (or an arbitrary unit which is not a cube). Here e is the basis number for 3 in the group of ideal classes.

If the class number h of $Q(\sqrt{k})$ is not divisible by 3, we have $e = 0$ and we get $\pm y + f\sqrt{k} = \eta \cdot \alpha^3$ where $\eta = 1$ or ε, if $k > 1$ and $\eta = 1$ if $k < 0$ and $\eta = \sqrt{-1}$ and $(1 + \sqrt{-3})/2$ if $k = -1$ or -3, respectively. Again we have $e = 1$ if the group of ideal classes is cyclic and if $h \equiv 0 \pmod 3$.

Now consider

(6) $$y^2 - kf^2 = x^3.$$

For $100 < k \leq 200$, k square free, only $Q(\sqrt{142})$ has class number $h \equiv 0 \pmod 3$. If we take $f = 1$, $k \equiv 5 \pmod 8$, then $2f = 2$ does not split into two different primes in $Q(\sqrt{k})$. Hence, by Theorem 2, all the integer solutions of (6) [$f = 1$, $k \equiv 5 \pmod 8$] can be obtained from

$$\pm y + \sqrt{k} = \left(\frac{a + b\sqrt{k}}{2}\right)^3$$

$$\pm y + \sqrt{k} = \left(\frac{c + d\sqrt{k}}{2}\right)\left(\frac{a + b\sqrt{k}}{2}\right)^3$$

where the fundamental unit $\eta = \dfrac{c + d\sqrt{k}}{2}$ and $\dfrac{a + b\sqrt{k}}{2}$ is an integer in the field.

Now $c \equiv d \pmod 2$ and $a \equiv b \pmod 2$ for $k \equiv 1 \pmod 4$. On equating irrational parts, we get, respectively,

(7) $$b(3a^2 + kb^2) = 8,$$

and

(8) $$c(3a^2b + kb^3) + d(a^3 + 3kab^2) = 16.$$

Equation (7) can be completely solved for a given k. In particular, if $k \equiv 5 \pmod 8$, $k > 0$, $k \neq 5$, then (7) has no solution in integers. If c and d are odd, then by Theorem 1, (8) has no solution in integers. Whence (6) is not solvable in integers.

In particular, $y^2 - k = x^3$ is without integer solutions for the following k's:

$$k = 109,\ \eta = (261 + 25\sqrt{109})/2$$
$$k = 133,\ \eta = (173 + 15\sqrt{133})/2$$
$$k = 149,\ \eta = (61 + 5\sqrt{149})/2$$
$$k = 157,\ \eta = (213 + 17\sqrt{157})/2$$
$$k = 165,\ \eta = (13 + \sqrt{165})/2$$
$$k = 173,\ \eta = (13 + \sqrt{173})/2$$
$$k = 181,\ \eta = (1305 + 97\sqrt{181})/2$$

Below we consider three cases where $f \neq 1$.

Case 1:

(9) $$y^2 - 116 = x^3$$

The equation can be written as $y^2 - 2^2 \cdot 29 = x^3$. Here $k = 29 \equiv 5 \pmod 8$ and $f = 2$. The fundamental unit of $Q(\sqrt{29})$ is $\eta = (5 + \sqrt{29})/2$ and $h[Q(\sqrt{29})] = 1$. Since 2 remains a prime in $Q(\sqrt{29})$, by Theorem 2, all the solutions of (7) can be obtained from

(10) $$\pm y + 2\sqrt{29} = \left(\frac{a + b\sqrt{29}}{2}\right)^3,$$

and

(11) $$\pm y + 2\sqrt{29} = \left(\frac{5 + \sqrt{29}}{2}\right)\left(\frac{a + b\sqrt{29}}{2}\right)^3.$$

On equating irrational parts, we have, respectively,

(12) $$b(3a^2 + 29b^2) = 16,$$

and

(13) $$5(3a^2b + 29b^3) + (a^3 + 3 \cdot 29ab^2) = 16 \cdot 2.$$

(12) is easily seen to be insoluble in integers and (13) has no solution in integers by Theorem 1.

Case 2:

(14) $$y^2 - 180 - x^3$$

Here $k = 5$ and $f = 6$ in $y^2 - kf^2 = x^3$. The fundamental unit of $Q(\sqrt{5})$ is $\eta = (1 + \sqrt{5})/2$ and $h[Q(\sqrt{5})] = 1 \not\equiv 0 \pmod 3$. Again $2f = 12$ has 2 prime divisors 2 and 3. Since $(2) = (2)$ and $(3) = (3)$ in $Q(\sqrt{5})$, we need examine the following two equations by Theorem 2.

(15) $$\pm y + 6\sqrt{5} = \left(\frac{a + b\sqrt{5}}{2}\right)^3,$$

and

(16) $$\pm y + 6\sqrt{5} = \left(\frac{1 + \sqrt{5}}{2}\right)\left(\frac{a + b\sqrt{5}}{2}\right)^3.$$

From (15) and (16), we obtain, respectively,

(17) $$b(3a^2 + 5b^2) = 48,$$

and

(18) $$(a^3 + 3 \cdot 5ab^2) + (3a^2b + 5b^3) = 96.$$

From (17), we see that $b \equiv 0 \pmod 3$. Then $b(3a^2 + 5b^2) \equiv 0 \pmod 9$, while $48 \equiv 3 \pmod 9$. Hence (17) has no solution in integers. Again (18) has no solution in integers by Theorem 1.

Case 3:

(19) $$y^2 - 125 = x^3$$

By Theorem 2, we gat all the solutions of (19) from

(20) $$3a^2b + 5b^3 = 40,$$

and

(21) $$(a^3 + 15ab^2) + (3a^2b + 5b^3) = 80.$$

It is easy to see that (20) has only one solution given by $a = 0$ and $b = 2$. From this solution we find $x = (1/4)/(a^2 - 5b^2) = -5$ and hence $y = 0$. Since, by Theorem 1, (21) has no solution in integers, we have exactly one integral solution for $y^2 - 125 = x^3$, namely

$$x = -5,\ y = 0.$$

REFERENCES

1. O. Hemer. "On the Diophantine Equation $y^2 - k = x^3$." Unpublished doctoral dissertation, Uppsala, 1952.
2. S. P. Mohanty. "On the Diophantine Equation $y^2 - k = x^3$." Unpublished doctoral dissertation, UCLA, 1971.
3. L. J. Mordell. "The Diophantine Equation $y^2 - k = x^3$." *Proc. London Math. Soc.* (2) 13 (1913):60-80.

*****

A DIVISIBILITY PROPERTY CONCERNING BINOMIAL COEFFICIENTS

JÁNOS SURÁNYI

University Eötvös 1, H-1088 Budapest, Múzeum krt 6/8

I

The following observation was made by P. Erdős. The exponent of 2 in the canonical decomposition[1] of

$$\binom{2^{n+1}}{2^n} - \binom{2^n}{2^{n-1}}$$

is $3n$ for $n \geq 2$. He conjectured that this is always true.[2] I succeeded in proving his conjecture, which raised the analogous question for odd primes instead of 2.

For the solution of this problem, I can prove the following.

Theorem: The exponent of the prime number p in the canonical decomposition of the difference

$$\binom{p^{n+1}}{p^n} - \binom{p^n}{p^{n-1}}$$

is

(i) $3n$ for $p = 2$,
(ii) $3n + 1$ for $p = 3$,
(iii) at least $3n + 2$ for $p > 3$.

More generally, I will investigate, for integers K, M divisible by p ($K = kp$, $M = mp$), the difference

$$A = A_p(K, M) = \binom{K}{M} - \binom{k}{m}.$$

By an algebraic transformation, we will be led to the following question: If p is a prime and $m(p - 1)$ is even, which power of p divides the sum

$$\sum_{j=1,\, p\nmid j}^{m(p-1)/2} \frac{\prod_{r=1,\, p\nmid j}^{(mp-1)/2} r(mp - r)}{j(mp - j)}?$$

---

[1] I.e., the decomposition into the product of powers of different prime numbers.

[2] Oral communication, July 1976.