ON CERTAIN COMBINATORIAL DIOPHANTINE EQUATIONS AND THEIR CONNECTION TO PYTHAGOREAN NUMBERS

ROBERT S. COULTER, MARIE HENDERSON, AND FELIX LAZEBNIK

1. Introduction

The binomial knapsack problem is easily stated: determine all $(m+2)$-tuples of positive integers $n > r > r_1 \geq r_2 \geq \ldots \geq r_m$ for which

$$\binom{n}{r} = \sum_{i=1}^{m} \binom{n}{r_i}.$$

We call any $(m+2)$-tuple $(n, r, r_1, \ldots, r_m)$ satisfying this equation a *binomial knapsack*. The problem first came to the authors' attention when considering a problem on symmetric functions, but the name is derived from the connection to knapsack-type problems. This article considers the simplest case of this problem. That is, we consider the problem of determining all 4-tuples (n, r, s, t) satisfying

$$\binom{n}{r} = \binom{n}{s} + \binom{n}{t} \tag{1}$$

with $n > r > s \geq t \geq 0$.

The list of results on Diophantine equations involving factorials and binomial coefficients is long. Many such results, and related references, can be found in Guy [12], Hajdu and Pintér [13], Grytczuk [11] and Goetgheluck [10]. It is not surprising that some of these results should be quite close to, or overlap, the binomial knapsack problem. However, there does not appear to be a complete resolution of the problem at hand, and the results of this paper, to our knowledge, are new.

As with many classes of Diophantine equations, the problem splits naturally into a finite case, where (1) has only finitely many solutions, and an infinite case, where (1) has infinitely many solutions. In Section 2 we show that the number of solutions of (1) is infinite if $1 \leq r-t \leq 2$, and in Section 3 we present a complete description of the solutions of (1) in these cases. In Section 4 we restrict ourselves to the case $s = t$ with $r-t \geq 3$. We conjecture that in this case there can be only one or two solutions, with all such solutions described. In support of our conjecture, we show that, for $s = t = r - 3$, the only solution is $(n, r, t, t) = (8, 5, 2, 2)$. The case $s = t = r - 4$ was resolved by Cohn in [8]: the only solution of (1) is $(n, r, t, t) = (11, 7, 3, 3)$. One of our infinite cases is intimately related to *Pythagorean numbers*, that is, integers which represent areas of right triangles with integer sides. In the final section we use our results for this case to derive several results on Pythagorean numbers.

2000 *Mathematics Subject Classification.* 11D09, 11D41, 11G45, 11D59.

2. Separating the finite and infinite solution cases

In this section we show how the problem of determining all 4-tuples of binomial knapsacks splits into two distinct cases. The main techniques for proving finiteness of a solution set of Diophantine equations stem from the work of Runge [20] and Thue [26]. Many of these results can be found in the classical text of Mordell [19]. We are interested in integer points of curves $F(x,y)=0$ over $\mathbb{Z}$. The result best suited for our purposes is one by Davenport and Lewis.

Lemma 2.1. *Let $f,g\in\mathbb{Z}[x,y]$ be polynomials of degree n and m, respectively. The equation $f(x,y)=g(x,y)$ has only a finite number of integer solutions if $n>2$, $m<n$ and f is an irreducible form.*

This lemma appears as Theorem 22 on page 278 of [19] where it is also mentioned that it is a consequence of a result of Schinzel [21]. The attribution to Davenport and Lewis is made clear by Schinzel in [21] where he obtains the result as a corollary.

Set $r-s=m$ and $r-t=k$ with $k\geq m>0$. For any non-negative integer c, define the polynomial $f_c(x)\in\mathbb{Z}[x]$ by

$$f_c(x)=\prod_{i=0}^{c-1}(x-i).$$

It follows that a solution of (1) exists if and only if

$$f_k(a)=f_m(r)f_{k-m}(a)+f_k(r),$$

where $a=n-t=n+k-r$, or equivalently, if and only if

$$F_{k,m}(x,y)=f_k(x)-f_k(y)-f_m(y)f_{k-m}(x)=0 \tag{2}$$

has a solution $(x,y)\in\mathbb{Z}\times\mathbb{Z}$ with $y\geq 1$.

Lemma 2.2. *Let k,m be positive integers, $k>m$ and $k\geq 3$. If the trinomial $x^k-x^{k-m}-1$ is irreducible over $\mathbb{Q}$, then (2) has only a finite number of integer solutions (x,y).*

Proof. Expanding each product in (2), we can rewrite the equation as

$$x^k-x^{k-m}y^m-y^k=g_k(x,y),$$

where g_k is a polynomial of degree at most $k-1$. Since $x^k-x^{k-m}y^m-y^k$ is homogeneous, it is irreducible over $\mathbb{Z}$ if and only if the trinomial $z^k-z^{k-m}-1$ is. Applying Lemma 2.1 completes the proof. □

The reducibility of trinomials over various fields has been a focal point of several papers. The general problem of determining whether a given trinomial x^n+ax^m+b is irreducible over a finite field remains open, even for $\mathbb{F}_2$ and $\mathbb{F}_3$ (see von zur Gathen [9] on the $\mathbb{F}_3$ case). A more complete answer, due to Schinzel [22], exists for algebraic number fields and function fields in one variable. Many results deal with special cases, either in the characteristic of the field, or the form of the trinomial, or both. One of the most celebrated papers on the subject is by Swan [24] where, among other results, the number of irreducible factors of a trinomial x^n+x^m+1 over $\mathbb{F}_2$ is studied. For a good exposition of Swan's paper and many additional details, see also Berlekamp [2], Section 6.6 and the problems at the end of Chapter 6. For later related results see, for example, Mills and Zierler [17], Carlitz [7], Vishne [28], Loidreau [16], and Bluher [4]. For the reducibility of the trinomial $x^k-x^{k-m}-1$

over $\mathbb{Q}$, a complete description was obtained by Ljunggren [15] and Tverberg [27]. An application of Theorem 3 of [15] yields the following.

Lemma 2.3. *Let $a > b$ be positive integers and $f(x) = x^a - x^b - 1$. Set $d = (a, b), a_1 = \frac{a}{d} \pmod 6$ and $b_1 = \frac{b}{d} \pmod 6$. The trinomial $f(x)$ is reducible over $\mathbb{Q}$ if and only if $(a_1, b_1) \in \{(1, 2), (5, 4)\}$.*

Combining this result with Lemma 2.2, we obtain the following theorem.

Theorem 2.4. *Let k, m be integers satisfying $k \geq m > 0$. Set $d = (k, m)$, $k_1 = \frac{k}{d} \pmod 6$ and $m_1 = \frac{m}{d} \pmod 6$. If $k \geq 3$ and $(k_1, m_1) \notin \{(2, 1), (5, 4)\}$, then the equation*

$$\binom{n}{r} = \binom{n}{r-m} + \binom{n}{r-k}$$

has only finitely many solutions in n, r. If $k \leq 2$, then the equation has infinitely many solutions.

The case $k \leq 2$ is covered in the next section. The case $k \geq 3$ follows from the previous two lemmas.

Conjecture 2.5. *With notation as above, there are only finitely many solutions to (1) in the case where $k \geq 3$ and $(k_1, m_1) \in \{(2, 1), (5, 4)\}$.*

3. The infinite solutions case

Throughout this section $r - t = k \leq 2$. There are three possible 4-tuples which give binomial knapsacks under this restriction: $(n, r, r-1, r-1)$, $(n, r, r-1, r-2)$, and $(n, r, r-2, r-2)$. The first case is easily dealt with. The following theorem is easily established and is also mentioned in [10, Section 2].

Theorem 3.1. *For every positive integer r, a binomial knapsack of the form $(n, r, r-1, r-1)$ exists if and only if $n = 3r - 1$.*

The second and third cases both reduce to examples of Pell's equation with additional conditions. Since the methods involved are similar, we exhibit the method for one of the two cases, and simply state the results for the other case.

Consider the equation

$$\binom{n}{r} = \binom{n}{r-1} + \binom{n}{r-2}.$$

Expanding we obtain the equation

$$n^2 + 3n(1 - r) + (r^2 - 4r + 2) = 0$$

and using the quadratic formula yields

$$2n = 3r - 3 \pm \sqrt{5r^2 - 2r + 1}.$$

Now $n > r$ and $3r - 3 - \sqrt{5r^2 - 2r + 1} < 2r - 3$ for $r \geq 1$. It follows that we can only have $2n = 3r - 3 + \sqrt{5r^2 - 2r + 1}$.

It remains to establish when this equation yields integer solutions. If r is an integer such that $5r^2 - 2r + 1$ is a perfect square, then $3r - 3 + \sqrt{5r^2 - 2r + 1}$ is always even, so we need only determine when $5r^2 - 2r + 1$ is a perfect square.

Theorem 3.2. *The 4-tuple $(n, r, r-1, r-2)$ is a binomial knapsack if and only if*

$$2n = 3r - 3 + \sqrt{5r^2 - 2r + 1}$$

where r is any member of the sequence defined by $r_1 = 6, r_2 = 40$ and

$$r_{i+2} = 7r_{i+1} - r_i - 1. \tag{3}$$

Proof. We first find the set of all positive r for which the Diophantine equation

$$5r^2 - 2r + 1 = y^2$$

has a solution. Solving with respect to r, we get

$$r = \frac{1 \pm \sqrt{5y^2 - 4}}{5} = \frac{1 \pm x}{5}, \tag{4}$$

where $x = \sqrt{5y^2 - 4}$. Hence r is a positive integer if and only if $x = \sqrt{5y^2 - 4}$ is a positive integer congruent to 4 modulo 5. So we need to find all positive integers $x \equiv 4 \pmod 5$ for which the Diophantine equation

$$x^2 - 5y^2 = -4 \tag{5}$$

has a solution. Finding the solutions to (5) is a non-trivial but well studied problem, see for example LeVeque [14], Theorem 8.7, and there are classical methods for giving all solutions to this Pell-like equation in terms of recurrence sequences. We omit the details. □

Similar methods can be employed to prove the following.

Theorem 3.3. *The 4-tuple $(n, r, r-2, r-2)$ is a binomial knapsack if and only if*

$$2n = 2r - 3 + \sqrt{8r^2 - 8r + 1}$$

where r is any member of the sequence defined by $r_1 = 3$, $r_2 = 15$ and

$$r_{i+2} = 6r_{i+1} - r_i - 2.$$

4. The finite solutions case with $s = t$

We now consider (1) with $s = t$. If we assume $k = r - t \geq 3$, then (1) has only finitely many solutions by Theorem 2.4.

The results of the last section for the cases $k = 1$ and $k = 2$ are also relevant in the current context. To begin, it follows from Theorem 3.1, that for any integer $k \geq 3$, we must always have one solution to

$$\binom{n}{r} = 2\binom{n}{r-k}; \tag{6}$$

namely $n = 3k - 1$, $r = 2k - 1$. Also, any integer $r > 3$ from the sequence in Theorem 3.3 generates a solution to (6) for

$$k = \frac{1 - 2r + \sqrt{8r^2 - 8r + 1}}{2}.$$

Set

$$S_k = \{(x, y) \in \mathbb{Z} \times \mathbb{Z} \mid f_k(x) = 2f_k(y) \text{ and } x > y \geq k\}.$$

We make the following conjecture:

Conjecture 4.1. *Let $k \geq 3$. Then $|S_k| = 1$, unless*

$$k = \frac{1 - 2r + \sqrt{8r^2 - 8r + 1}}{2}$$

for some integer $r > 3$ of the sequence in Theorem 3.3, in which case $|S_k| = 2$.

The case $k = 4$ was established in [8]: the only solution to (6) with $k = 4$ is $n = 11$, $r = 7$. We now establish the conjecture for $k = 3$.

Theorem 4.2. *The only integers $n > r \geq 3$ which satisfy*

$$\binom{n}{r} = 2\binom{n}{r-3}, \tag{7}$$

are $n = 8$ and $r = 5$.

Proof. Expanding and simplifying we obtain

$$(n - r + 3)(n - r + 2)(n - r + 1) = 2r(r - 1)(r - 2).$$

Set $x = n - r + 2$ and $y = r - 1$, so that our equation becomes $x^3 - 2y^3 = x - 2y$. If we set $t = x - 2y$, then this equation can be rewritten as $(t + 2y)^3 - 2y^3 - t = 0$ or

$$6y^3 + 12ty^2 + 6t^2y + (t^3 - t) = 0. \tag{8}$$

We will show that no solution to (8) exists for $|t| > 3$. Exhaustively checking for those solutions with $|t| \leq 3$, we see that there are precisely 11 solutions (t, y) of (8) under this restriction:

$$\begin{array}{ccccccc} (0,0), & (-3,1), & (-3,4), & (-2,1), & (-1,0), & (-1,1), \\ & (3,-1), & (3,-4), & (2,-1), & (1,0), & (1,-1). \end{array}$$

Since $(n, r) = (t + 3y - 1, y + 1)$ and $r \geq 3$, the only solution of (7) generated from this list is $(n, r) = (8, 5)$.

It remains to show that for $|t| > 3$, there are no solutions to (8). We note $t^3 - t$ is divisible by 6 for all integers t. For any integers j, k with $k \geq 2$, we denote the k-order of j by $\mathrm{ord}_k(j)$. That is, $\mathrm{ord}_k(j)$ is the largest power of k dividing j. We divide the problem with $|t| \geq 4$ into three cases: $(t, 6) = 1$; $\mathrm{ord}_w(t) \geq 2$, where $w = 2$ or 3; and $t = ct_1$, where $c = 2, 3$, or 6, and $(t_1, 6) = 1$.

Firstly, suppose $|t| \geq 4$ and $(t, 6) = 1$. In this case t must be divisible by a prime $p \geq 5$. Set $a = \mathrm{ord}_p(t)$ and $b = \mathrm{ord}_p(y)$. Note $a = \mathrm{ord}_p(t^3 - t)$. Since t divides y^3, we must have $a \leq 3b$. If $a < 3b$, then reducing both sides of (8) by p^a, we obtain a contradiction: the resulting equation cannot be solved modulo p. So $a = 3b$ and $t = l^3$ for some integer $l \geq p \geq 5$ with $(l, 6) = 1$. Hence $y = ml$ for some integer m. We must have $(m, l) = 1$, as otherwise reducing both sides of (8) by t gives a contradiction: the resulting equation cannot be solved modulo (m, l). Substituting $y = ml$ into (8), then reducing by l^3 and setting $s = l^2$, gives

$$f(m, s) = 6m^3 + 12m^2s + 6ms^2 + s^3 = 1. \tag{9}$$

The binary cubic form $f(m, s)$ in (9) is irreducible over $\mathbb{Z}$. This follows, for instance, by an application of Eisenstein's criterion using the prime 2 in the ring $\mathbb{Z}[m][s]$. We have thus reduced our equation to a Thue-type equation. Efficient methods exist for finding all solutions for such an equation, see Bilu and Hanrot [3] for example. The Magma algebra package, [6], immediately yields the solutions $(m, s) = (0, 1)$ or $(m, s) = (-1, 1)$ for this equation. In either case we get $l^{2b} = 1$, contradicting the condition $l \geq p \geq 5$. (The computational results were checked using the Maple

package, which uses a different algorithm, and an effective bound of 10^{42415} for the maximal absolute value of m in the solutions (m, s) of (9). This bound was calculated using the results of Walsh [29].)

Now suppose $|t| \geq 4$ and $\mathrm{ord}_w(t) \geq 2$, where $w = 2$ or 3. In this case we have w divides y. Reducing (8) by $w^{\mathrm{ord}_w(t)}$, we obtain a contradiction: the resulting equation cannot be solved modulo w.

Finally, suppose $|t| \geq 4$ and $t = ct_1$, where $c = 2, 3$, or 6, and $(t_1, 6) = 1$. For each of these values of t, an argument similar to the one used in Case 1, gives $t = 6$, or $t = cl^3$, where $l \geq 5$ and $(l, 6) = 1$. Continuing as in Case 1, we again end without a solution of (8).

We have exhausted all the possibilities and the proof is complete. □

The proof just given reduces the equation $x^3 - 2y^3 = x - 2y$ to a more complicated appearing Thue-type equation, and then uses an algebra package to determine all solutions. Given the simple form of the original, this might appear somewhat puzzling to the reader. The reason we proceeded this way is as follows. Many results on Diophantine equations of the form $F(x) = G(y)$ give bounds on the maximal absolute value of either x or y for those cases where the equation is known to have a finite number of solutions. Unfortunately, these bounds are generally very large. One of the best bounds is given by Tengely [25]. However, the result requires both F and G to be monic, and so cannot be applied to our situation. As noted by the referee, the equation under consideration is an elliptic equation. Theory for solving such equations is well established and developed, see the article by Stroeker and de Weger [23], and it could also be used to solve our equation.

5. Connections to Pythagorean numbers

Recall that a *Pythagorean triangle* is a right triangle with all sides of integer length. A Pythagorean triangle is called *primitive* if the side lengths are relatively prime. A *Pythagorean number* is an integer which represents the area of a Pythagorean triangle. A *primitive Pythagorean number* is an integer which represents the area of a primitive Pythagorean triangle. This is equivalent to the weaker requirement that at least one pair of the side lengths is relatively prime. In Theorems 3 and 4 of [18], Mohanty and Mohanty showed that there are infinitely many primitive Pythagorean numbers which are the products of three consecutive integers, and asked the question about the existence of infinitely many primitive Pythagorean numbers that are the products of two consecutive integers. They answered the question by giving an explicit construction, derived from their results on products of three consecutive integers and using several properties of Fibonacci numbers. They also give two essentially different explicit constructions of infinite sequences of not primitive Pythagorean numbers that are the products of two consecutive integers.

One goal of this section is to show that these results (but for different sequences) follow immediately from our proof of Theorem 3.2. These sequences are more natural in the following sense: to find a Pythagorean number $r(r-1)$, one may attempt to construct Pythagorean triangles with legs of length $r-1$ and $2r$, or r and $2(r-1)$. Another goal of this section is to generalise these results to Pythagorean numbers of the form $r(r-k)$.

Indeed, consider the right triangle with legs of length $r-1$ and $2r$, and hypotenuse of length y, so that

$$5r^2 - 2r + 1 = y^2.$$

In the proof of Theorem 3.2 we established that the triangle is Pythagorean if and only if $r = r_i$, $i \geq 1$, and the sequence $\{r_i\}$ is defined by the recurrence (3). These triangles yield the Pythagorean numbers $r_i(r_i - 1)$. If r_i is even, the numbers $r_i - 1$ and $2r_i$, are relatively prime, which implies that $r_i(r_i-1)$ is a primitive Pythagorean number. Finally, we observe that infinitely many members of $\{r_i\}$ are even: r_i is even if and only if $i \not\equiv 0 \pmod 3$.

In light of the above argument, it is also natural to consider Pythagorean triangles with legs of length r and $2(r-1)$, since their areas are the Pythagorean numbers $r(r-1)$. Denoting the length of the hypotenuse by y, we get the Diophantine equation $5r^2 - 8r + 4 = y^2$. Note that

$$5r^2 - 8r + 4 = 5(1-r)^2 - 2(1-r) + 1.$$

This reduces the problem to the one we dealt with in Theorem 3.2. We leave the details to the reader and summarise our results in the following statement.

Theorem 5.1. *The integer $r(r-1)$ is a Pythagorean number obtained from a right triangle with legs of length $r-1$ and $2r$ if and only if r is a member of the sequence defined by $r_1 = 6, r_2 = 40$ and*

$$r_{i+2} = 7r_{i+1} - r_i - 1.$$

For this sequence, r_i is even if and only if $i \not\equiv 0 \pmod 3$, and all such terms give rise to primitive Pythagorean numbers.

The integer $r(r-1)$ is a Pythagorean number obtained from a right triangle with legs of length r and $2(r-1)$ if and only if r is a member of the sequence defined by $r_1 = 3$, $r_2 = 15$ and

$$r_{i+2} = 6r_{i+1} - r_i - 2.$$

For this sequence, r_i is odd if and only if $i \not\equiv 2 \pmod 3$ and all such terms give rise to primitive Pythagorean numbers.

We now consider the following generalisation of the question asked in [21], namely, for a given positive integer k, are there infinitely many Pythagorean numbers of the form $r(r-k)$? An obvious solution is to consider the Pythagorean triangles with legs of length $r' - 1$ and $2r'$, or r' and $2(r'-1)$ and to take similar triangles with coefficient of similarity k, i.e., $r = kr'$. It turns out that for some k *all* Pythagorean triangles with legs of length $r-k$ and $2r$, or r and $2(r-k)$ can be obtained this way.

For a positive integer d, let

$$dP_k = \{(dr, dy) \mid (2r)^2 + (r-k)^2 = y^2,\ r, y \in \mathbb{N}\}, \text{ and}$$
$$dQ_k = \{(dr, dy) \mid (2(r-k))^2 + r^2 = y^2,\ r, y \in \mathbb{N}\}.$$

We write P_k and Q_k for $1P_k$ and $1Q_k$, respectively. It is easy to check that, for every divisor k' of k, we have

$$k'P_{k/k'} \subseteq P_k, \text{ and } k'Q_{k/k'} \subseteq Q_k.$$

The following theorem describes these relations completely.

Theorem 5.2. *Let k_1, k_2 be positive integers, and let $k = k_1k_2$. Then $P_k = k_2P_{k_1}$ and $Q_k = k_2Q_{k_1}$ if and only if k_2 has no prime factor congruent to $\pm 1 \pmod{10}$.*

Proof. Substituting $k-r$ for r in $(2r)^2+(r-k)^2$, we obtain $(2(r-k))^2+r^2$. This reduces the statement for Q_k to the one for P_k, and so, in what follows we concentrate only on the latter.

Since $k_2P_{k_1} \subseteq P_k$ for every divisor k_2 of k, we first must show that every Pythagorean triangle with legs of length $r-k$ and $2r$ is similar to a Pythagorean triangle with legs of length $\frac{r}{k_2}-k_1$ and $2\frac{r}{k_2}$ with the coefficient of similarity k_2. This is equivalent of saying that every solution of

$$(r-k)^2+(2r)^2 = 5r^2-2rk+k^2 = y^2$$

can be obtained from a solution of

$$\left(\frac{r}{k_2}-k_1\right)^2+\left(2\frac{r}{k_2}\right)^2 = 5\left(\frac{r}{k_2}\right)^2-2k_1\frac{r}{k_2}+k_1^2 = \left(\frac{y}{k_2}\right)^2$$

by multiplying the latter by k_2. For these Diophantine equations, quadratic in r or r/k_2, to have a solution, their discriminants must be squares. Therefore the last statement is equivalent to saying that every solution of

$$x^2-5y^2 = -4k^2 \tag{10}$$

is obtained from a solution of

$$x'^2-5y'^2 = -4k_1^2. \tag{11}$$

by multiplying both x' and y' by k_2.

Let (x,y) be a solution of (10), and p be a prime divisor of k_2. If $p=2$, then $x^2-5y^2=0 \pmod{16}$ if and only if both x and y are even, which can be checked by a direct computation. Hence p divides both x and y. If $p=5$, then $x^2-5y^2=0 \pmod{25}$. This implies that 5 divides x^2, and hence p divides both x and y again.

Now suppose $p \neq 2,5$. Consider the ring $R=\mathbb{Z}[\omega]$ of algebraic integers where $\omega = \frac{1+\sqrt{5}}{2}$. With respect to the usual norm, R is a Euclidean domain, see, for example Baker [1, Chapter 7, Section 5] for a short proof. Hence it is a unique factorization domain and there is no distinction between irreducibles and primes in R. The prime decompositions of rational integers in this ring, as well as in other rings of algebraic integers of fields $\mathbb{Q}(\sqrt{D})$, $D \in \mathbb{Z}$, is well understood, see Borevich and Shafarevich [5, Chapter 8, Section 1].

The discriminant of the binary form x^2-5y^2 is 20 and since our prime p does not divide 20, it does not ramify in R. So it remains prime in R if and only if $\left(\frac{20}{p}\right) = \left(\frac{5}{p}\right) = \left(\frac{p}{5}\right) = -1$. Note that the last condition is equivalent to the prime p satisfying $p \equiv \pm 3 \pmod{10}$.

If $p \equiv \pm 3 \pmod{10}$, then since p^2 divides $(x-y\sqrt{5})(x+y\sqrt{5})$, it follows that p divides one of the factors, say the first. Hence $x-y\sqrt{5} = p(u+v\omega)$ for some integers $2u$ and $2v$. Hence p (being odd) divides both x and y. We have therefore shown that for every prime divisor p of k which is 2, 5, or congruent to $\pm 3 \pmod{10}$, $pP_{k/p} = P_k$. This implies $k_2P_{k_1} = P_k$.

To complete the proof of the theorem, we must show that if p is a prime divisor of k_2 such that $\left(\frac{p}{5}\right)=1$, then $k_2P_{k_1} \neq P_k$. We do this by showing that for such p there exists a solution (x,y) of (10) with $(p,x)=(p,y)=1$.

Let $k=K_1K_2$, where now K_2 is the product of *all* prime divisors of k which are 2, 5, or congruent to $\pm 3 \pmod{10}$, and K_1 is the product of all prime divisors of k congruent to $\pm 1 \pmod{10}$.

We now invoke the following result on representation of integers by binary quadratic forms: a number n is represented by some binary quadratic form f of discriminant d, $n = f(x, y)$ with $(x, y) = 1$, if and only if d is a quadratic residue modulo $4n$, [1, Chapter 5, Section 3]. We now apply this result with $d = 20$ and $n = -4K_1^2$. Note that 20 is a quadratic residue modulo $-16K_1^2$ if and only if 5 is a quadratic residue modulo $4K_1^2$. Since $\left(\frac{5}{4}\right) = 1$ and $\left(\frac{5}{K_1^2}\right) = \left(\frac{K_1^2}{5}\right) = 1$, it follows that 5 is a quadratic residue modulo $4K_1^2$. As the discriminant of $x^2 - 5y^2$ is 20 and the class number $h(\sqrt{5}) = 1$, see [5, page 481], the equation $x^2 - 5y^2 = -4K_1^2$ has an integer solution (x, y) with x and y being relatively prime. Since $P_k = K_2 P_{K_1}$, and K_2 is not divisible by p, we have therefore established the existence of a solution (x, y) of (10) with $(p, x) = (p, y) = 1$. □

Note that for $k = 1$, we get (5) from the proof of Theorem 3.2. Hence we have the following corollary.

Corollary 5.3. *Let k be any any positive integer. Then $P_k = kP_1$ and $Q_k = kQ_1$ if and only if k has no prime factor congruent to $\pm 1 \pmod{10}$.*

Acknowledgements

The authors wish to thank Szabolcs Tengely for useful discussions on topics related to this paper and bringing the article [13] to our attention, and Claus Fieker for a detailed explanation of the algorithmic methods used by the Magma algebra package to solve Thue equations. We also wish to thank the anonymous referee whose thoughtful suggestions helped to improve our original presentation.

References

1. A. Baker, *A Concise Introduction to the Theory of Numbers*, Cambridge University Press, Cambridge, 1984.
2. E.R. Berlekamp, *Algebraic Coding Theory*, McGraw-Hill, New York - Toronto, 1968.
3. Y. Bilu and G. Hanrot, *Solving Thue equations of high degree*, J. Number Th. **60** (1996), 373–392.
4. A.W. Bluher, *A Swan-like theorem*, Finite Fields Appl. **12** (2006), 128–138.
5. Z.I. Borevich and I.R. Shafarevich, *Theory of Numbers*, 2nd ed., Nauka, Moscow, 1972, (in Russian).
6. W. Bosma, J. Cannon, and C. Playoust, *The Magma algebra system I: The user language*, J. Symbolic Comput. **24** (1997), 235–265.
7. L. Carlitz, *Factorization of a special polynomial over a finite field*, Pacific J. Math. **32** (1970), 603–614.
8. J.H.E. Cohn, *The Diophantine equation $Y(Y+1)(Y+2)(Y+3) = 2X(X+1)(X+2)(X+3)$*, Pacific J. Math. **37** (1971), 331–335.
9. J. von zur Gathen, *Irreducible trinomials over finite fields*, Math. Comp. **72** (2003), 1987–2000.
10. P. Goetgheluck, *Infinite families of solutions of the equation $\binom{n}{k} = 2\binom{a}{b}$*, Math. Comp. **67** (1998), 1727–1733.
11. A. Grytczuk, *On a conjecture of Erdös on binomial coefficients*, Studia Sci. Math. Hungar. **29** (1994), 241–244.
12. R.K. Guy, *Unsolved Problems in Number Theory*, 3rd ed., Problem Books in Mathematics, Springer-Verlag, New York, 2004.
13. L. Hajdu and Á. Pintér, *Combinatorial Diophantine equations*, Publ. Math. Debrecen **56** (2000), 391–403.
14. W.J. LeVeque, *Topics in Number Theory*, vol. 1, Addison-Wesley, Reading, 1956.
15. W. Ljunggren, *On the irreducibility of certain trinomials and quadrinomials*, Math. Scand. **8** (1960), 65–70.

16. P. Loidreau, *On the factorization of trinomials over* $\mathbb{F}_3$, Tech. Report 3918, Institut national de recherche en informatique et en automatique (INRIA), 2000, http://www.inria.fr/rrrt/rr-3918.html.
17. W.H. Mills and N. Zierler, *On a conjecture of Golomb*, Pacific J. Math. **28** (1969), 635–640.
18. S. Mohanty and S.P. Mohanty, *Pythagorean Numbers*, Fibonacci Quarterly **28** (1990), 31–42.
19. L.J. Mordell, *Diophantine Equations*, Pure and Applied Mathematics, vol. 30, Academic Press, London - New York, 1969.
20. C. Runge, *Über ganzzahlige Lösungen von Gleichungen zwischen zwei Veränderlichen*, J. Reine Angew. Math. **100** (1887), 425–435.
21. A. Schinzel, *An improvement of Runge's theorem on Diophantine equations*, Comment. Pontificia Acad. Sci. **2** (1969), 1–9.
22. ———, *On reducible trinomials*, Dissertationes Math.(Rozprawy Mat.) **329** (1993), 83 pp.
23. R.J. Stroeker and B.M.M. de Weger, *Solving elliptic Diophantine equations: the general cubic case*, Acta Arith. **87** (1999), 339–365.
24. R.G. Swan, *Factorization of polynomials over finite fields*, Pacific J. Math. **12** (1962), 1099–1106.
25. Sz. Tengely, *On the Diophantine equation* $F(x) = G(y)$, Acta Arith. **110** (2003), 185–200.
26. A. Thue, *Über Annäherungswerte algebraischer Zahlen*, J. Reine Angew. Math. **135** (1909), 284–305.
27. H. Tverberg, *On the irreducibility of the trinomials* $x^n \pm x^m \pm 1$, Math. Scand. **8** (1960), 121–126.
28. U. Vishne, *Factorization of trinomials over Galois Fields of characteristic* 2, Finite Fields Appl. **3** (1997), 370–377.
29. P.G. Walsh, *A quantitative version of Runge's theorem on Diophantine equations*, Acta Arith. **62** (1992), 157–172, Erratum, Acta Arith. **75** (1995), 397–398.

(R.S. Coulter, F. Lazebnik) Department of Mathematical Science, Ewing Hall, University of Delaware, Newark, DE, 19716, U.S.A.
E-mail address: {coulter,lazebnik}@math.udel.edu

(M. Henderson) 310/60 Willis Street, Te Aro, 6001, New Zealand
E-mail address: marie.henderson@ssc.govt.nz