# When are Multiples of Polygonal Numbers again Polygonal Numbers?

## Jasbir S. Chahal, Michael Griffin and Nathan Priddis

*To the memory of S. Srinivasan*

**Abstract.** Euler showed that there are infinitely many triangular numbers that are three times other triangular numbers. In general, it is an easy consequence of the Pell equation that for a given square-free $m > 1$, the relation $\Delta = m\Delta'$ is satisfied by infinitely many pairs of triangular numbers $\Delta$, $\Delta'$.

After recalling what is known about triangular numbers, we shall study this problem for higher polygonal numbers. Whereas there are always infinitely many triangular numbers which are fixed multiples of other triangular numbers, we give an example that this is false for higher polygonal numbers. However, as we will show, if there is one such solution, there are infinitely many. We will give conditions which conjecturally assure the existence of a solution. But due to the erratic behavior of the fundamental unit of $\mathbb{Q}(\sqrt{m})$, finding such a solution is exceedingly difficult. Finally, we also show in this paper that, given $m > n > 1$ with obvious exceptions, the system of simultaneous relations $P = mP'$, $P = nP''$ has only finitely many possibilities not just for triangular numbers, but for triplets $P$, $P'$, $P''$ of polygonal numbers, and give examples of such solutions.

**Keywords.** polygonal numbers, Pell equation, triangular numbers, elliptic curves, Diophantine equations

**2010 Mathematics Subject Classification.** primary:11D45, secondary:11G05

## 1. Introduction

For an integer $\ell \geq 3$, the $r$-th *polygonal number* or $r$-th $\ell$-gonal number $P(\ell, r)$, $r \geq 1$, is defined by

$$P(\ell, r) = \frac{(\ell - 2)r^2 - (\ell - 4)r}{2}.$$

It is the total number of dots that are used to enlarge recursively a single dot, representing the first $\ell$-gonal number, to a regular $\ell$-gon with each side having $r$ dots. In the process the first dot remains the only common vertex of successive $\ell$-gons with each side having $r$ dots (cf. Figure 1).
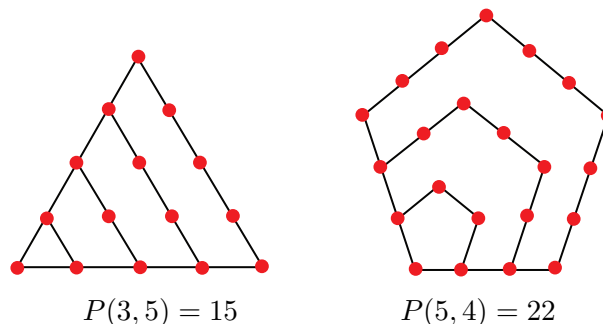


$$P(3, 5) = 15 \qquad P(5, 4) = 22$$

Figure 1: Representation of polygonal numbers for $\ell = 3$ and $\ell = 5$.

Thus

$$P(3, r) = \frac{r(r+1)}{2} = 1, 3, 6, 10, 15, \ldots$$

are the *triangular numbers*,

$$P(4, r) = r^2 = 1, 4, 9, 16, 25, \ldots$$

are the (perfect) squares, whereas

$$P(5, r) = \frac{r(3r-1)}{2} = 1, 5, 12, 22, 35, \ldots$$

are the *pentagonal numbers*, and so on.

These numbers, especially the triangular and the pentagonal numbers, have been studied since antiquity (cf. [Dic71]). In 1638 Fermat stated without proof his Polygonal Number Theorem: *Every positive integer is a sum of at most $\ell$ $\ell$-gonal numbers*. The case $\ell = 4$ is a well-known theorem of Lagrange (*every positive integer is a sum of at most four squares*), proved by Jacobi and independently by Lagrange in 1772. Gauss discovered it for $\ell = 3$ as noted in his diary on 10 July 1796. Fermat's Polygonal Number Theorem for all $\ell$ was finally proved by Cauchy in 1813.

Euler determined all triangular numbers that are three times another triangular number. Given an integer $m > 1$, it is interesting to study which triangular numbers are $m$ times another triangular number. In this paper, we recall the answer to this question (see [ChaD93]) and determine, more generally, which $\ell$-gonal numbers are $m$ times another $\ell$-gonal number.

It is an easy consequence of the Pell equation, as we recall, that for any given square-free $m > 1$, the relation $\Delta = m\Delta'$ is satisfied by infinitely many pairs of triangular numbers $\Delta$ and $\Delta'$. However, this is not true for higher $\ell$-gonal numbers. We will give an example such that $P = mP'$ has no solution in $\ell$-gonal numbers (see Example 3). Indeed, we will state a condition that, when satisfied, determines infinitely many solutions. We conjecture that no solutions exist when the stated condition fails.

In contrast, we also prove that, given $m > n > 1$, the simultaneous relations

$$\begin{cases} P = mP' \\ P = nP'' \end{cases}$$

have only finitely many possibilities, not just for triangular numbers but for triplets $P$, $P'$, $P''$ of $\ell$-gonal numbers for all $\ell \geq 3$ except when $\ell = 4$ and $m$ and $n$ are both perfect squares. Table 2 gives several non-trivial examples of this phenomenon for small $\ell$, $m$, and $n$.

## 2. The Pell equation and polygonal numbers

The *diophantine equations* (after Diophantus of Alexandria, a third century AD Greek mathematician and the author of a series of books called *Arithmetica*) are polynomial equations with integer coefficients. The solutions sought are integers or sometimes rationals. One of the most famous diophantine equations is the so–called Pell equation.

$$x^2 - my^2 = 1. \tag{2.1}$$

Because the square factors of $m$ can be absorbed by $y^2$, the integer $m \neq 0$ is generally assumed to be square-free. We will not assume this in this article. We only assume that $m$ is not a perfect square.

This equation is named after the Englishman John Pell (1611–1685), who contributed nothing to its study. Due to an error by Euler, the name Pell was given to this diophantine equation, and, according to Weil ([Wei84, p. 174]), "traditional designation [of equation (2.1)] as Pell's equation is unambiguous and convenient."

Table 1: Fundamental solution to the Pell equation for small $m$

| $m$ | $(x,y)$ | $m$ | $(x,y)$ | $m$ | $(x,y)$ |
|---|---|---|---|---|---|
| 2 | (3,2) | 10 | (19,6) | 46 | (24335,3588) |
| 3 | (2,1) | 11 | (10,3) | 47 | (48,7) |
| 5 | (9,4) | 12 | (7,2) | 94 | (2143295,221064) |
| 6 | (5,2) | 13 | (649,180) | 95 | (39,4) |
| 7 | (8,3) | 30 | (11,2) | | |
| 8 | (3,1) | 31 | (1520, 273) | | |

The Pell equation has a very long and rich history going at least as far back as Archimedes (cf. [Len00], [Nel80], [Wei84]). His complicated "cattle problem" reduces to the Pell equation (2.1) with $m = 4,729,494$. Its first nontrivial solution (i.e. with $y \neq 0$) was found by computer search (cf. [Nel80]) not too long ago (in 1980).

If we write (2.1) as

$$(x + y\sqrt{m})(x - y\sqrt{m}) = 1,$$

and assume that $m$ is square–free, then solving the Pell equation is equivalent to finding the units of $\mathbb{Z}[\sqrt{m}]$, a special case of the Dirichlet unit theorem for the ring of integers of a number field. (Actually, this is true only if $m \equiv 0, 2, 3 \pmod 4$, if $m \equiv 1 \pmod 4$, it needs slight modification (cf. [Cha88], pp. 78–89]) but is not an issue here.)

The solution $(x,y)$ with smallest $x = x_1 > 0$ (hence the smallest $y = y_1 > 0$) is called the *fundamental solution* of (2.1). Correspondingly, $x_1 + y_1\sqrt{m}$ is called the *fundamental unit* of $\mathbb{Z}[\sqrt{m}]$ or by abuse of language, that of the real quadratic field $\mathbb{Q}(\sqrt{m})$.

Finding the fundamental solution of (2.1) is still a very challenging problem, with no apparent pattern to it (cf. [Var97, Wei84]). The most obvious way of finding it is to put $y = 1, 2, 3, \ldots$ in $1 + my^2$ and stop as soon as it becomes a perfect square. For example, if $m = 2$, $x_1 = 3$, $y_1 = 2$ and if $m = 3$, $x_1 = 2$, $y_1 = 1$. Likewise, if $m = 11$, $x_1 = 10$, $y_1 = 3$. Already for $m = 13$, this method is not very efficient. Table 1 shows the erratic behavior of the fundamental solution for certain integers.

Brahmagupta (598–670 AD), the first to solve the quadratic equation $ax^2 + bx + c = 0$ the way we do it today, Jayadeva (9th century AD), and Bhaskara II (1114–1185 AD) were the first to study the Pell equation systematically. They showed that (for $m > 1$) infinitely many solutions can be obtained from a given nontrivial solution by using the so-called Brahmagupta identity (the product of two numbers of the form $a^2 + mb^2$ is itself a number of this form). The Fibonacci identity (the set of the sums of two squares is closed under multiplication), which already occurs in Diophantus' *Arithmetica*, is a special case of the Brahmagupta identity.

This school of Indian mathematicians devised a method (cf. [Var97, pp. 25–38]) they called chakravala (or circular), which they used to solve (2.1) for many values of $m$. For example, for $m = 61$ they found the smallest solution $x = 1766319049$, $y = 226153980$. The efficiency and the simplicity of this method impressed even André Weil, one of the greatest number theorists of the 20th century, who wrote (cf. [Wei84, p. 24]), "to have developed *chakravala* and to have it applied successfully to such difficult numerical cases as $N = 61$ or $N = 67$ had been no mean achievement." (His $N$ is our $m$.)

The Indians assumed that a nontrivial solution always exists. Lagrange was the first to prove the existence of a nontrivial solution for all $m > 1$. We now have several proofs of this fact based on different disciplines of number theory. The most common (cf. [NiZuMo91, pp. 336–356]) given in first courses in number theory uses the techniques from diophantine approximations and continued fractions (cf. [Nag64]).

Although by Lagrange's theorem we know that sooner or later $1 + my^2$ becomes a perfect square, the random size of $x_1$, $y_1$ makes it very difficult to predict how far we must go for arbitrarily given $m$.

For example, if $m = 63$, $x_1 = 8$, $y_1 = 1$, whereas, for $m = 61$, in the smallest solution $(x_1, y_1)$ above, $y_1$ runs into nine (decimal) digits. Although there are better methods available—such as the method of continued fractions—there is still no last word on solving the Pell equation, or equivalently, on finding the fundamental unit of a real quadratic field (cf. [Len00], [Wil02]).

It is easy to check that the set $G$ of integer solutions of (2.1) with $x > 0$ forms an abelian group under the binary operation

$$(x, y) * (x', y') = (xx' + myy', xy' + x'y) \tag{2.2}$$

with $(1, 0)$ as its identity and $(x, -y)$ the inverse of $(x, y)$. The group law (2.2) is suggested by multiplying $(x + y\sqrt{m})(x' + y'\sqrt{m}) = X + Y\sqrt{m}$ and comparing the rational (respectively irrational) parts in this equation. By the Dirichlet theorem, $G$ is a cyclic group generated by the fundamental solution $g = (x_1, y_1)$.

If $(x_n, y_n) = g^n = \underbrace{g * \cdots * g}_{n \text{ times}}$, it is easy to see that the integers $y_1 < y_2 < y_3 < \cdots$ increase quadratically and soon $y_n$ is so large that $1/y_n^2$ is almost zero. Thus $(x_n/y_n)^2$ is almost equal to $m$, giving a very good rational approximation to $\sqrt{m}$.

**Example 1.** If $m = 2$, $g = (x_1, y_1) = (3, 2)$ and it takes less than a minute to compute by hand and see that $(x_5, y_5) = (3363, 2378)$. It is amazing that the approximation $x_5/y_5 = 3363/2378$ to $\sqrt{2}$ is the same as given by a handheld calculator.

## 2.A. Triangular numbers

As an application of the above discussion of the Pell equation, we recall from [ChaD93] the following generalization of Euler's work regarding which triangular numbers are three times some other triangular numbers.

**Theorem 1.** *For a non-square integer $m > 1$, the equation*

$$\Delta' = m\Delta \tag{2.3}$$

*is satisfied by infinitely many triangular numbers $\Delta$, $\Delta'$.*

*Proof.* We first remark that if the *norm form equation*

$$(x + y\sqrt{m})(x - y\sqrt{m}) = d \tag{2.4}$$

has a solution $(x, y)$, infinitely many solutions are obtained by multiplying $\alpha = x + y\sqrt{m}$ with the units of the form $x' + y'\sqrt{m}$ in $\mathbb{Z}[\sqrt{m}]$. Equation (2.4) is called a norm form equation because the quadratic form $x^2 - my^2$ is the norm $N(\alpha) = \alpha\bar{\alpha}$ of $\alpha = x + y\sqrt{m}$ in $\mathbb{Z}[\sqrt{m}]$, $\bar{\alpha} = x - y\sqrt{m}$ being the *conjugate* of $\alpha$.

Since the triangular numbers are the numbers $\Delta = \frac{r(r+1)}{2}$, $r = 1, 2, 3, \ldots$, the equation (2.3) is the same as

$$s(s + 1) = mr(r + 1)$$

which again on completing squares is the same as

$$(2s + 1)^2 - m(2r + 1)^2 = 1 - m.$$

So we have to find infinitely many solutions of

$$X^2 - mY^2 = 1 - m \tag{2.5}$$

with $X$, $Y > 0$ both odd. One such solution, namely $(1,1)$, is obvious; this, however, does not give us a solution to (2.3). But we can use this solution to find others.

If $(x_n, y_n)$ is a solution of the Pell equation (2.1), then it can be checked that $x_n$, $y_n$ are of opposite parity (i.e. one odd the other even). Moreover, in case $m$ is even, it is $x_n$ that is odd. Therefore, $(X_n, Y_n) = (x_n, y_n) * (1,1) = (x_n + my_n, x_n + y_n)$ is a solution of (2.5) with both $X_n$, $Y_n$ odd. Thus solutions of (2.3) can be obtained from $(X_n, Y_n)$ with $n > 0$.

**Remark 1.** There is another solution to (2.5) that will yield solutions to (2.3) different from those mentioned in the proof, namely $(-1, 1)$ as we will see later. In fact for certain $m$ (depending on the class number of $m$), one can show that these are the only solutions to (2.3).

Suppose $a > b \geq 1$ are square-free integers which are mutually coprime. A slight modification of the above argument with $m = ab$ in the Pell equation (2.1) yields the following stronger result. We omit its proof.

**Theorem 2.** *The equation*

$$a\Delta = b\Delta'$$

*has infinitely many solutions in triangular numbers $\Delta$, $\Delta'$.*

## 2.B.   Generalization to $\ell$-gonal numbers

Equation (2.3) becomes more interesting if $\Delta$, $\Delta'$ in it are replaced by higher polygonal numbers resulting in the equation

$$P(\ell, r) = mP(\ell, s) \tag{2.6}$$

with $\ell \geq 5$. In this more general setting, the existence of solutions of (2.6) depends on the existence of solutions of the Pell equation (2.1) satisfying certain congruence equations, which may or may not happen. In fact, whether the conditions are satisfied or not seems to happen randomly (cf. [ChaPri11, Pri09]). Before we describe these conditions, we need the following preparatory lemma.

**Lemma 1.** *If $(x, y)$ is a solution to (2.1) with $x > 0$ and $y > 0$, then $x > y$ and $my > x$.*

*Proof.* Since $x^2 = 1 + my^2$ and $m \geq 2$ it is clear that $x > y$. Furthermore, $m^2y^2 + 1 > my^2 + 1 = x^2$. Hence $m^2y^2 > x^2$.

For every solution $(x, y)$ to (2.1) with $x > 0$ and $y > 0$, we also have solutions $(\pm x, \pm y)$ in any combination of positive and negative. If we compose these solutions with $(1, 1)$ we obtain

$$(1,1) * (\pm x, \pm y) = (\pm x \pm my, \pm x \pm y).$$

From the lemma, we see that only $(x + my, x + y)$ has both entries positive. We can do something similar with $(-1, 1)$ and we see that of the four possibilities only

$$(-1, 1) * (x, y) = (-x + my, x - y)$$

has both entries positive. We could do something similar with $(-1, -1)$ and $(1, -1)$, but these are simply the negatives of what we have already done.

**Theorem 3.** *Given $m > 1$ not a perfect square and $\ell \geq 5$ there exists a solution to (2.6) if there exists a solution to (2.1) with*

$$\left. \begin{array}{l} x + my \equiv -1 \pmod{q} \\ x + y \equiv -1 \pmod{q} \end{array} \right\} \tag{2.7}$$

*or*

$$\left.\begin{aligned} my - x &\equiv -1 \pmod{q} \\ x - y &\equiv -1 \pmod{q} \end{aligned}\right\}. \tag{2.8}$$

*Here $q = 2\ell - 4$, $\ell - 2$, and $\ell/2 - 1$ according as $\ell \equiv 1, 3 \pmod 4$, $2 \pmod 4$, and $0 \pmod 4$, resp. Moreover, if one solution exists, then there are infinitely many.*

*Proof.* We consider only the case $\ell \equiv 1, 3 \pmod 4$. The other two cases are dealt with similarly. Writing exactly what the two sides of (2.6) stand for and completing squares, we obtain the generalized Pell equation

$$X^2 - mY^2 = (1 - m)(\ell - 4)^2 \tag{2.9}$$

with

$$X = (2\ell - 4)\, r - (\ell - 4)$$

and

$$Y = (2\ell - 4)\, s - (\ell - 4).$$

Clearly (2.6) has a solution if and only if the generalized Pell equation (2.9) has a solution with $X$, $Y \equiv -(\ell - 4) \mod (2\ell - 4)$ and $X, Y > 0$.

One obvious solution to (2.9) is $(X, Y) = (\ell - 4, \ell - 4)$. We may obtain further solutions by composing this solution with the solutions $(x, y)$ of the Pell equation (2.1):

$$X = (\ell - 4)(x + my)$$

and

$$Y = (\ell - 4)(x + y).$$

Since $\ell \equiv 1, 3 \pmod 4$, $\ell - 4$ and $2\ell - 4$ are coprime, so $\ell - 4$ is a unit $\pmod{2\ell - 4}$. Hence the requirement $X, Y \equiv -(\ell - 4) \pmod{2\ell - 4}$ for the solutions of (2.9) leads to the conditions

$$x + my \equiv -1 \pmod{2\ell - 4}$$

and

$$x + y \equiv -1 \pmod{2\ell - 4}$$

for a solution $(x, y)$ to (2.1).

Based on the discussion above, we consider $(-(\ell - 4), \ell - 4)$ also a solution to (2.9). Composing with $(x, y)$ we obtain

$$X = (\ell - 4)(-x + my)$$

and

$$Y = (\ell - 4)(x - y).$$

By Lemma 1, $X, Y > 0$. This leads to conditions (2.8).

As soon as we have one solution $(X_0, Y_0)$ to (2.9) satisfying one of the stated congruence relations, we can find infinitely many solutions. In fact, the cyclic group of solutions to (2.1) modulo $q$ becomes a finite cyclic group with identity the class of solutions to (2.1) with $x \equiv 1 \pmod q$ and $y \equiv 0 \pmod q$ (cf. [ChaPri11]). There are infinitely many such solutions. Let $(x_s, y_s)$ be such a solution with $x_s, y_s > 0$. Then $(X_0, Y_0) * (x_s, y_s)$ is a solution to (2.9) satisfying the required congruence relations. Each of these yields a solution to (2.6).

**Remarks:**

**1.** One can see from its proof, that the converse of Theorem 3 is also true if, for a given $m > 1$, any two solutions to (3) are related by a unit (and therefore a solution to (2.1)). This is related to the class number problem. In this case, we can recover all polygonal numbers which satisfy (2.6). This is the case, for example, with $\ell = 5$, $m = 2$ as we will see in Example 2.

**2.** We can reformulate (2.7) in the following way.

$$(m-1)x \equiv -(m-1) \pmod{q}$$

and

$$(m-1)y \equiv 0 \pmod{q}.$$

Let $d = \gcd(m - 1, q)$. If $d$ is odd, we see there is only one solution to (2.7), namely $x \equiv -1 \pmod{q}, y \equiv 0 \pmod{q}$. If $d$ is even, one can check, there is an additional possible solution (modulo $q$) satisfying (2.1), which is $x \equiv \frac{q}{2} - 1 \pmod{q}$ and $y \equiv \frac{q}{2} \pmod{q}$. Only one of these is possible, and these are the only possibilities satisfying (2.7).

**3.** In [ChaPri11, Pri09] the authors investigated $G_{m,q}$, the group modulo $q$ of solutions to (2.1). It is a finite cyclic group and its order is denoted $g_m(q)$. Solutions to (2.7) are closely related to the order of this group. Indeed from the previous remark, we see that solutions to (2.7) correspond with elements of $G_{m,q}$ of order 2. Thus for example, we have no solutions to (2.7) if $g_m(q)$ is odd.

We now give some examples to show that the Equations (2.7) and (2.8) are often satisfied but not always. We emphasise we differentiate between solutions to (2.7) or (2.8) from the theorem and solutions to the original problem in (2.6). When no solution to (2.7) or (2.8) exists, it does not imply the same about the original problem. Verifying there are no solutions to (2.6) can be much more involved.

In the following examples, we focus mostly on solutions to (2.7) and (2.8), but in Example 3, we see in fact that there are no solutions to the original problem (2.6). Also in Example 2 we show that for certain choices of $\ell$ and $m$, Theorem 3 yields all solutions to (2.6).

**Example 2.** Consider $\ell = 5$ (so $q = 6$). These correspond to pentagonal numbers. For $m = 2$, the fundamental solution to (2.1) is $(3, 2)$. This does not satisfy (2.7) or (2.8). However if we look at powers of this fundamental solution, we see that the next solution is $(17, 12)$, which satisfies (2.7) and the third solution is $(99, 70)$, which satisfies (2.8). Hence there are infinitely many pentagonal numbers which are two times another pentagonal number. In fact, if we consider the ring $\mathbb{Z}[\sqrt{2}]$, then the pentagonal numbers which are twice another pentagonal number correspond to solutions to

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

which in turn are units in $\mathbb{Z}[\sqrt{2}]$. The units in $\mathbb{Z}[\sqrt{2}]$ are powers of $(1+\sqrt{2})$—which in the notation of the Pell equation we would write as $(1, 1)$ as in the proof of the theorem—negatives, and conjugates of such powers. Hence, we have actually found all solutions to (2.6) with $\ell = 5$ and $m = 2$.

With $\ell = 5$, we can do similar computations for $m = 3, 4, 5, 6, 7$ finding infinitely many solutions to (2.6) via the conditions in (2.7). With $m = 12$, there is no solution to (2.7); however, the fundamental solution $(7, 2)$ satisfies (2.8), and so we obtain infinitely many solutions in this case as well.

For $m = 10, 11, 13$, one can easily check that there are no solutions to (2.7) or (2.8) as set out in the theorem. Indeed, in the notation introduced in the Remark above, $g_{10}(5) = 1$ and $g_{13}(5) = 1$. That means that every solution to (2.1) is congruent to $(1, 0) \pmod{q}$. Furthermore, $g_{11}(5) = 2$, so we only need to check the conditions on the fundamental solution. Again, this does not necessarily mean there are no solutions to (2.6), although we conjecture that there are not.

**Example 3.** Consider $\ell = 6$ (hence $q = 4$). With $m = 2$. This Pell equation has fundamental solution $(3, 2)$, and as we have seen the next solution is $(17, 12)$. Neither of these solutions satisfies either (2.7) or (2.8). Since $(17, 12)$ is congruent to $(1, 0) \pmod q$, (i.e. $g_2(4) = 2$) these are the only solutions we must consider. In fact we will now demonstrate that there are no hexagonal numbers which are twice another hexagonal number.

In this case, we look for solutions to

$$X^2 - mY^2 = (1 - m)(\tfrac{\ell-4}{2})^2$$

with $X, Y \equiv -\frac{\ell-4}{2} \pmod q$, which becomes

$$X^2 - 2Y^2 = -1.$$

Any solution to this equation corresponds to a unit in $\mathbb{Z}[\sqrt{2}]$ with norm $-1$—that is to say a unit with norm 1 multiplied by either $(1 + \sqrt{2})$ or $(-1 + \sqrt{2})$. But these are exactly the solutions to (2.1) multiplied by either $(1, 1)$ or $(-1, 1)$ as we have seen. Hence there are no solutions.

With $\ell = 6$ we can find solutions to (2.7) or (2.8) with $m = 3, 6, 7, 8, 11$, but not for $m = 2, 5, 10, 12, 13$. Again, we conjecture that there are no solutions for these last choices of $m$.

**Example 4.** Finally, consider $\ell = 8$ (hence $q = 3$). In this case we have solutions to (2.7) or (2.8) when $m = 2, 3, 5, 6, 7, 8, 12$, but not when $m = 10, 11, 13$. (Again, this does not necessarily mean there are no solutions to (2.6) for these choices of $m$.)

## 3.   Elliptic Curves and Polygonal Numbers

In what follows, by an elliptic curve we mean a diophantine equation

$$dy^2 = x^3 + ax^2 + bx + c \tag{3.10}$$

with $a$, $b$, $c$, $d$ in $\mathbb{Z}$, $d \geq 1$ and the right-hand side of (3.10) having no repeated root. The rational solutions of (3.10), more precisely the set $E(\mathbb{Q})$ of rational points on the elliptic curve $E$ defined by (3.10) together with the point $O$ at infinity is, by the Mordell-Weil theorem (cf. [Cha88, p. 125]), a finitely generated abelian group with $O$ as its identity, under the group law given by $P + Q + R = O$ if the points $P$, $Q$, $R$ on (3.10) are collinear. Thus the torsion subgroup (i.e. the subgroup of points of finite order) of $E(\mathbb{Q})$ is finite. By the Lutz-Nagell theorem (cf. [Cha88, p. 136]), a torsion point can have only integer coordinates. However, a point with integer coordinates need not be a torsion point. *A priori* it is possible for (3.10) to have infinitely many integer solutions. But the next theorem (a special case of Siegel's theorem) from the theory of diophantine equations (cf. [Mor69, p. 255]) states that this is not possible.

**Theorem 4.** *The elliptic curve* (3.10) *has only finitely many points on it with integer coordinates.*

However, (3.10) may or may not have infinitely many rational solutions. In fact, both the cases are believed to occur with equal probability (cf. [Sil01]).

We now prove the following fact about polygonal numbers.

**Theorem 5.** *Given $\ell \geq 3$ and $m > n > 1$ (m or n square-free in case $\ell = 4$), there are only finitely many triplets $r$, $s$ and $t$ such that*

$$P(\ell, r) = mP(\ell, s) = nP(\ell, t). \tag{3.11}$$

*Proof.* We assume $\ell \neq 4$ (the trivial case). The relation (3.11) is the same as the diophantine equations

$$(\ell - 2)r^2 - (\ell - 4)r = m((\ell - 2)s^2 - (\ell - 4)s)$$
$$= n((\ell - 2)t^2 - (\ell - 4)t).$$

Setting $a = 2(\ell - 2)$ and $b = (\ell - 4)$ and completing squares, these equations become

$$\left. \begin{array}{l} (ar - b)^2 - m(as - b)^2 = -(m - 1)b^2 \\ (ar - b)^2 - n(at - b)^2 = -(n - 1)b^2. \end{array} \right\} \tag{3.12}$$

Let

$$u = ar - b, \quad v = as - b, \quad w = at - b,$$

and

$$X = m^2 n v^2. \tag{3.13}$$

Then (3.12) implies

$$X - A = mnu^2, \quad X - B = mn^2 w^2 \tag{3.14}$$

where $A = mn(m - 1)b^2$ and $B = mn(m - n)b^2$.

Now set $Y = m^2 n^2 uvw$. Multiplying (3.13) with both equations in (3.14), we find

$$Y^2 = X(X - A)(X - B). \tag{3.15}$$

By our assumption on $m$, $n$ and $\ell$, (3.15) is an elliptic curve with integer coefficients. So by 4, it has only finitely many points with integer coordinates. Consequently, (3.11) has only finitely many possibilities.

**Example 5.** Consider $\ell = 5$, $m = 6$ and $n = 3$. We have seen that there are infinitely many solutions to each of $P(r, 5) = 6P(s, 5)$ and $P(r, 5) = 3P(t, 5)$. However, following the proof of Theorem 5, finding simultaneous solutions to both can be reduced to finding integer points on the elliptic curve

$$Y^2 = X(X - 90)(X - 54).$$

This curve has several integer points, however in order to correspond to an integer solution to (3.11), we must have $m^2 n = 108$ divide $X$, and $m^2 n^2 = 324$ divide $Y$. Only three such points exist: $(0, 0)$, $(108, 324)$, and $(90828, 27351756)$. The first point gives $v^2 = 0$, which does not yield an integer value for $s$. The second point gives $v^2 = u^2 = t^2 = 1$, which yields only the trivial solution $(r, s, t) = (0, 0, 0)$. The third point gives $v = \pm 29, u = \pm 71$, and $w = \pm 41$, which yields only the solution $(r, s, t) = (12, 5, 7)$. Hence the only simultaneous solution in pentagonal numbers to $P = 6P' = 3P''$ is $P = P(5, 12) = 210$, $P' = P(5, 5) = 35$, and $P'' = P(5, 7) = 70$.

Table 2 gives several other examples. In each case listed, the solution is unique for the given $\ell$, $m$ and $n$.

**Remark 2.** Relations (3.12) are a variation of equations considered by Fibonacci in his book on squares [Fib1225]. The reader with some knowledge of algebraic geometry may also see conceptually that such a pair of equations always defines an elliptic curve. The simultaneous equations

$$\left. \begin{array}{l} x^2 + ny^2 = z^2 \\ x^2 - ny^2 = t^2 \end{array} \right\} \tag{3.16}$$

considered by Fibonacci are related to the congruent number problem (cf. [Cha88]). The pair of equations (3.16) defines an elliptic curve with its Weierstrass equation $y^2 = x^3 - n^2 x$.

Table 2: Solutions to $P = mP'$ and $P = nP''$

| $\ell$-gonal numbers | $P$ | $P'$ | $P''$ | $P = mP' = nP''$ |
|---|---|---|---|---|
| $\ell = 3$, triangular | 6 | 1 | 3 | $P = 6P' = 2P''$ |
| | 630 | 105 | 210 | $P = 6P' = 3P''$ |
| | 105 | 15 | 21 | $P = 7P' = 5P''$ |
| $\ell = 5$, pentagonal | 210 | 35 | 70 | $P = 6P' = 3P''$ |
| $\ell = 6$, hexagonal | 120 | 6 | 15 | $P = 20P' = 8P''$ |
| $\ell = 7$, heptagonal | 12852 | 1071 | 6426 | $P = 12P' = 2P''$ |

# References

[Cha88]    Chahal, J. S., *Topics in Number Theory*, Plenum-Birkhäuser-Springer, (1988).

[ChaD93]   Chahal, J.S. and D'Sousa Harry, Some remarks on triangular numbers, *Number Theory with emphasis on the Markov Spectrum*, Lecture Notes in Pure Math, Dekker, New York (1993), 61–67.

[ChaPri11] Chahal, J. S. and Priddis, N., Some Congruence Properties of the Pell equation, *Ann. Sci. Math. Québec*, **35** (2011), 175–184.

[Dic71]    Dickson, L. E., *History of the Theory of Numbers* **2**, Chelsea, (1971).

[Fib1225]  Fibonacci, *Liber Quadratorum*, 1225.

[Len00]    Lenstra Jr., H.W., Solving the Pell Equation, *Notices AMS*, **49** (2000), 182–192.

[Mor69]    Mordell, L. J., *Diophantine Equations*, Academic Press, London and New York (1969).

[Nag64]    Nagell, T., *Introduction to Number Theory*, Chelsea, New York (1964).

[Nel80]    Nelson, H. L., A solution to Archimedes' cattle problem, *J. Recreational Math.*, **13** (1980–81), 162–176.

[NiZuMo91] Niven, I., Zuckerman, H. S., Montgomery, H. L., *An Introduction to the Theory of Numbers*, 5th Ed., John Wiley & Sons, New York (1991).

[PinVar11] Pintér, Á. and Varga, N., Resolution of a non-trivial Diophantine equation without reduction methods, *Pub. Math. Debrecen*, **79** (2011), 605–601.

[Pri09]    Priddis, N., *Some Congruence Properties of Pell's Equation*, master's thesis, Brigham Young University (2009).

[Sil01]    Silverberg, A., *Open questions in arithmetic algebraic geometry*, IAS/Park City Math. Series **9**, AMS, Providence, RI (2001), 85-142.

[Var97]    Varadarajan, V. S., *Algebra in Ancient and Modern Times*, Hindustan Book Agency, Delhi (1997).

[Wei84]    Weil, A., *Number Theory – An Approach through History*, Birkhäuser, Boston (1984).

[Wil02]    Williams, H. C., Solving the Pell Equation, *Number Th. for the Millennium*, Ed. M. A. Bennett, et al, A. K. Peters, Notick, Mass. (2002), vol III, 397–455.

**Jasbir S. Chahal**
Department of Mathematics
Brigham Young University
Provo, UT 84602, USA
*e-mail*: jasbir@math.byu.edu

**Michael Griffin**
Department of Mathematics
Brigham Young University
Provo, UT 84602, USA
*e-mail*: mjgriffin@math.byu.edu

**Nathan Priddis**
Institut für Algebraische Geometrie
Leibniz Universität Hannover
Hannover, Germany
*e-mail*: priddis@mathematics.byu.edu