Adjugates of Diophantine Quadruples

Philip Gibbs

Diophantine m-tuples with property D(n), for n an integer, are sets of m positive integers such that the product of any two of them plus n is a square. Triples and quadruples with this property can be classed as regular or irregular according to whether they satisfy certain polynomial identities. Given any such m-tuple, a symmetric integer matrix can be formed with the elements of the set placed in the diagonal and with corresponding roots off-diagonal. In the case of quadruples, Jacobi's theorem for the minors of the adjugate matrix can be used to show that up to eight new Diophantine quadruples can be formed from the adjugate matrices with various combinations of signs for the roots. We call these adjugate quadruples.

Introduction

Diophantus proposed the problem of finding triples and quadruples of rational numbers such that the product of any two is one less than a square, and found several examples [1]. Fermat considered the problem over positive integers noting the quadruple (1,3,8,120) [2]. Then Euler showed that an infinite class of quadruples including Fermat's example can be extended to rational quintuples such as (1,3,8,120, 777480/8288641) [3]. Computer based searches have more recently yielded a finite number of rational Diophantine sextuples [4,5].

Some key questions about Diophantine m-tuples remain unsettled. We do not know if there exists a Diophantine quintuple in integers or a rational Diophantine septuple. There are also stronger conjectures on the complete set of quadruples. Over the last two decades a number of approaches have produced excellent results that have come tantalisingly close to answering the first question. By using results from the theory of Diophantine approximations it has been shown that there are no Diophantine sextuples in integers and only finitely many quintuples [6]. Impressive though these methods are, it seems that they are currently limited by gap requirements that make it difficult to derive stronger results.

It is possible that further progress may follow a better understanding of the algebraic and factorisation properties of Diophantine m-tuples and their generalisations. Even if it does not, these properties are of interest in their own right. Using algebraic methods and results from the theory of elliptic curves it is known that any Diophantine triple can be extended to a quadruple [7]. Furthermore, any quadruple can be extended to a rational Diophantine quintuple [8]. These results reveal that the structure of quadruples and quintuples is governed by the existence of certain polynomials over the m-tuples with useful factorisation properties that are not fully explained. The results described here have grown out of attempts to better understand these algebraic structures.

Basic Definitions

A **Diophantine *m*-tuple with the property D(*n*)** for *n* an integer is an *m*-tuple of distinct positive integers $(a_1,...,a_m)$ such that

$$a_i a_j + n = x_{ij}^2$$

 is always an integer square for $i \neq j$. The values of a_i are called the **components** of the quadruple and the values of x_{ij} are called its **roots**. For a given quadruple the roots are not unique because the alternatives with different signs are also valid roots. When we talk of **rational Diophantine m-tuples** we mean the case where *n* is a positive square number. An **improper** Diophantine *m*-tuple is an *m*-tuple with similar properties but with the relaxed condition that the elements a_i can be any integers and need not be distinct. A **primitive** Diophantine *m*-tuple is one where there is no common factor > 1 that divides all the numbers a_i and *n*. Two Diophantine quadruples will be called **equivalent** if they are both integer multiples of the same primitive quadruple after permutations of the components.

A **regular** Diophantine triple with the property D(*n*) is a triple (*a,b,c*) with the extra condition that

$$(c - b - a)^2 = 4(ab+n)$$

This equation is symmetric under permutations of *a*, *b*, *c*.

A **regular** Diophantine quadruple with the property D(*n*) is a quadruple (*a,b,c,d*) with the extra condition that

$$n(d + c - a - b)^2 = 4(ab+n)(cd+n)$$

This is also symmetric under permutations of the variables. Since both sides of the equation must be square it follows that a Diophantine quadruple with property D(*n*) can only be regular if *n* is square, whereas regular Diophantine triples with property D(*n*) exist for all *n*. When *n* is square the quadruple formed by adding a zero to a regular triple is an improper regular quadruple. An **irregular** Diophantine *m*-tuple is one that is not regular. A **semi-regular** Diophantine quadruple is one which contains a regular triple, and a **twice semi-regular** Diophantine quadruple is one that contains two regular triples. These definitions will help us classify and understand the quadruples better.

It is also convenient to define a function $Z_4(n)$ whose value is the number (possibly infinite) of irregular Diophantine quadruple with property D(*n*). A number of conjectures concerning Diophantine quadruples can then be summarised statements about $Z_4(n)$, for example it is believed to be finite for all $n \neq 0$. In particular $Z_4(1) = 0$. Setting upper limits for $Z_4(n)$ is a hard problem but lower limits for congruence classes of *n* can be found by constructing polynomial solutions [9].

Adjugation and Jacobi's Theorem

Given a Diophantine m-tu ple $(a_1,...,a_m)$ we can form a symmetric m by m matrix S with components given by

$$S_{ii} = a_i$$

$$S_{ij} = x_{ij} \quad (i \neq j)$$

For a quadruple (a,b,c,d) the matrix would look like this

$$S = \begin{pmatrix} a & x & y & u \\ x & b & z & v \\ y & z & c & w \\ u & v & w & d \end{pmatrix}$$

A minor $M_S(I,J)$ of the matrix S is the determinant of some smaller square matrix formed by removing one or more rows and columns from S, such that I is the set of indices of the rows left and J is the set of indices of the columns left. The principal minors are the ones formed when $I = J$ Because of the D(n) property the principal 2x2 minors of S are equal to -n

$$M_S(\{i,j\},\{i,j\}) = a_i \, a_j - x_{ij}^2 = -n$$

Given S we can form the adjugate matrix T whose elements are the cofactors of S given by

$$T_{ij} = (-1)^{i+j} \, M_S(U\text{-}\{j\}, \, U\text{-}\{i\})$$

U is the set of all row or column indices.

As a consequence of Laplace's formula for the determinant of a matrix we can write the matrix equation

$$ST = |S| \, I$$

Where I is the identity matrix and $|S|$ is the determinant of S, $|S| = M_S(U,U)$.

Jacobi's theorem [10] relates the minors of T to those of S by the formula

$$M_T(I,J) = (-1)^{\Sigma(I,J)} \, M_S(U\text{-}I, \, U\text{-}J) \, |S|^{r\text{-}1}$$

Where the exponent $\Sigma(I,J)$ used to determine the sign factor is just the sum of all the indices in both sets, and $r = |I| = |J|$ is the number of rows and columns removed to form the minors.

Jacobi's theorem can be applied to the principal 2x2 minors of the symmetric matrix S for a Diophantine quadruple with property D(n) to show that the 2x2 principle minors of the adjugate matrix T all have the value $-n \, |S|$. If we write out the components of -T as follows

$$-T = \begin{pmatrix} A & X & Y & U \\ X & B & Z & V \\ Y & Z & C & W \\ U & V & W & D \end{pmatrix}$$

Then we find that the m-tuple (A,B,C,D) is a (possibly improper) Diophantine m-tuple with the property $D(n|S|)$. The negative sign is introduced because in practice we find that the Diophantine quadruple formed in this way is less likely to be improper if we reverse the signs. So we have the following definition.

Given a (possibly improper) Diophantine quadruple (a_1, a_2, a_3, a_4) with property $D(n)$ and its integer root x_{ij} such that $a_i\, a_j + n = x_{ij}^2$, an **adjugate** quadruple is defined by constructing the symmetric matrix S with components $S_{ii} = a_i$ and $S_{ij} = x_{ij}$ $(i \neq j)$ and forming its adjugate matrix T. The adjugate quadruple (A_1, A_2, A_3, A_4) and its root X_{ij} are by definition given by $A_i = -T_{ii}$ and $X_{ij} = -T_{ij}$. Note that we speak of *an* adjugate and not *the* adjugate. This is because for a given quadruple, the roots x_{ij} can be given different combinations of signs which can provide different adjugates. From this definition the following theorem follows.

Theorem 1:

(a) Given a (possibly improper) Diophantine quadruple (a_1, a_2, a_3, a_4) with the property $D(n)$, any adjugate quadruple (A_1, A_2, A_3, A_4) is a (possibly improper) Diophantine quadruple with property $D(N)$ where $N = n|S|$ and S is the symmetric matrix constructed as described above.

(b) If (A_1, A_2, A_3, A_4) is an adjugate quadruple of (a_1, a_2, a_3, a_4) then (A_1, A_2, A_3, A_4) is equivalent to an adjugate quadruple of (a_1, a_2, a_3, a_4).

(c) A quadruple has at most eight distinct adjugates.

Proof: (a) follows from the construction Jacobi's theorem as described above. (b) is a consequence from the matrix equation $ST = |S|\, I$. (c) comes from the observation that there are $64 = 2^6$ ways to do the construction with different combinations of signs for the six roots. However if the matrix is transformed by reversing the signs on one row and the same column, then the adjugate matrix is transformed in the same way without affecting the components of the quadruple. Therefore only eight = 2^3 combinations of signs for the roots can lead to distinct adjugates.

Relationship Between Adjugation and Extension of Triples

Suppose (a,b,c) is a Diophantine triple with the property $D(1)$

$$ab+1 = x^2$$

$$ac+1 = y^2$$

$$bc+1 = z^2$$

Then a fourth integer d can be added to make a $D(1)$ Diophantine quadruple (a,b,c,d) using the formula.

$$d = a + b + c + 2abc + 2xyz$$

The quadruple is regular because it satisfies the equation

$$(d + c - a - b)^2 = 4(ab+1)(cd+1)$$

This equation shows that (cd+1) must be a square because (ab+1) is square. Similar results follow from permutations of the components to show that (a,b,c,d) is indeed a D(1) quadruple. In fact there is a second way to extend a triple using the formula

$$d = a + b + c + 2abc - 2xyz$$

However this case can lead to an improper quadruple with $d \leq 0$.

This 4th degree polynomial equation for regular D(1) quadruples can be interpreted as a special case of Cayley's hyperdeterminant which is a quartic invariant of $SL(2)^3$ acting on a 2x2x2 hypermatrix A with components A_{ijk} given by the formula

$$Det(A) = (A_{000}A_{111} + A_{001}A_{110} - A_{010}A_{101} - A_{100}A_{011})^2 - 4(A_{010}A_{100} - A_{000}A_{110})(A_{101}A_{011} - A_{111}A_{001})$$

So if we set $A_{111} = -d$, $A_{001} = c$, $A_{010} = a$, $A_{100} = b$, $A_{000} = 1$, and $A_{110} = A_{011} = A_{101} = -1$,

$$A = \left(\begin{pmatrix} 1 & a \\ b & -1 \end{pmatrix} \begin{pmatrix} c & -1 \\ -1 & -d \end{pmatrix} \right)$$

then the regularity condition is just $Det(A) = 0$.

There is a relationship between the process for extending triples to regular quadruples on the one hand, and adjugation of quadruples on the other. This follows from an observation of Holtz and Sturmfels who showed that if all the principal minors of a symmetric m by m matrix are naturally arranged in a 2^m hypermatrix, then the hyperdeterminant of any 2^3 segment of the hypermatrix is equal to zero [11]. To see this take the symmetric matrix S formed from a Diophantine quadruple and its roots. Then construct a 2x2x2x2 hypermatrix with its principal minors using the definition of the adjugate quadruple as follows,

$$\begin{pmatrix} \begin{pmatrix} 1 & a \\ b & -n \end{pmatrix} & \begin{pmatrix} c & -n \\ -n & -D \end{pmatrix} \\ \begin{pmatrix} d & -n \\ -n & -C \end{pmatrix} & \begin{pmatrix} -n & -B \\ -A & |S| \end{pmatrix} \end{pmatrix}$$

There are 8 different 2x2x2 hypermatrix slices that have a zero hyperdeterminant by the result of Holtz and Sturmfels. If $n = 1$ this would mean that the 4 quadruples with components (a,b,c,D), (a,b,C,d), (a,B,c,d) and (A,b,c,d) are regular Diophantine quadruples. In other words the four components of the adjugate quadruple are formed from the components used to extend the four subtriples of the original quadruple.

This also allows us to state some relationships between properties of a quadruple and its adjugates that can be verified by constructing the possible 2x2x2x2 hypermatrices for each adjugate:

- If a quadruple is regular then four out of its eight adjugates are the regular quadruples formed by dropping one of its for components and replacing it with the other extension value.
- If a quadruple is semi-regular, i.e. it contains a regular triple, then four of its eight adjugates will be improper quadruples with a zero component. Note that for any D(n) quadruple with a zero component, the value of n must be square, but this does not need to be the case for its adjugates.

- If quadruple is improper with a zero component then all of its adjugates are semi-regular.
- If a quadruple is twice semi-regular, i.e. it contains two regular triples, then two of its adjugates have two zeros and four others have one zero component.
- If a quadruple is improper with two duplicate components then it can have at most six distinct adjugates and four of them are improper with two duplicate components.
- If quadruple is improper with two zero components then all of its adjugates are twice semi-regular, but four of them are improper with two duplicate components and there are only two other distinct adjugates.

Adjugation and the Construction of Diophantine Quadruples

Adjugation can be used to construct generic formula for $D(n)$ Diophantine quadruples . The principle is to start with a simple formula for Diophantine quadruples (that may be improper), then apply adjugation to get another formula. As an example, consider the well known regular polynomial $D(1)$ triple

$$(a,b,c) = (x\text{-}1, x\text{+}1, 4x) \ , x > 1$$

This can be extended to an improper but regular $D(1)$ quadruple by adding a fourth component $d = 0$. We find that seven of the potential adjugates are improper and the remaining one is

$$(A,B,C,D) = (9x\text{+}3, 9x\text{-}3, 4x, 4x(2x\text{+}1)(2x\text{-}1))$$

which is a $D(9 - 32x^2)$ semi-regular quadruple.

References

[1] T. L. Heath, *Diophantus of Alexandria. A Study in the History of Greek Algebra*, (Cambridge, England, 1910), Powell's Bookstore, Chicago; Martino Publishing, Mansfield Center, 2003, pp. 162-164, 177-181, 344-349.

[2] P. Fermat, *Observations sur Diophante, Oeuvres de Fermat*, Vol. 1 (P. Tannery, C. Henry, eds.), 1891, p. 303.

[3] L. Euler, *Opuscula Analytica I*, 1783, pp. 329-344.

[4] P. Gibbs, *Some rational Diophantine sextuples*, Glas. Mat. Ser. III **41** (2006), 195-203.

[5] A. Dujella, *Rational Diophantine sextuples with mixed signs*, Proc. Japan Acad. Ser. A Math. Sci. **85** (2009), 27-30.

[6] A. Dujella, *There are only finitely many Diophantine quintuples*, J. Reine Angew. Math. **566** (2004), 183-214.

[7] J. Arkin, V. E. Hoggatt and E. G. Strauss, *On Euler's solution of a problem of Diophantus*, Fibonacci Quart. **17** (1979), 333-339.

[8] A. Dujella, *On Diophantine quintuples*, Acta Arith. **81** (1997), 69-79.

[9]   A. Dujella, *A problem of Diophantus and Dickson's conjecture*, Number Theory, Diophantine, Computational and Algebraic Aspects (K. Gyory, A. Petho, V. T. Sos, eds.), Walter de Gruyter, Berlin, 1998, pp. 147-156.

[10] H. Jeffreys, B. Swirles, *Methods of mathematical physics*, Cambridge university press, p135

[11]   O. Holtz, B Sturmfels, *Hyperdeterminantal relations among symmetric principal minors*, J. Algebra 316 (2007), no. 2, 634–648.