Mathematics in Ancient India

3. Brahmagupta's Lemma: The Samasabhavana

Amartya Kumar Dutta



Amartya Kumar Dutta is an Associate Professor of Mathematics at the Indian Statistical Institute, Kolkata. His research interest is in commutative algebra.

Number Theory for its own sake, as a great intellectual challenge, has a long history, particularly here in India. Already in the 7th century, Brahmagupta made important contributions to what is now known (incorrectly) as Pell's equation.: Michael Atiyah ([1], p.913)

In number theory, the grandest achievements of ancient Indian mathematicians had been in finding integer solutions of Diophantine equations. Recall[1] that equations with integer coefficients are called `Diophantine equations' when one is interested in finding their integer[2] solutions.

Indian algebraists were the first to evolve and describe algorithms for finding all integer solutions of Diophantine equations. In Part 2 of this series, we had discussed the Indian solutions of the linear Diophantine equation in two variables pioneered by Aryabhata (b. 476 CE). From the time of Brahmagupta (b. 598 CE), Indians began attempting the harder problem of solving various types of Diophantine equations of second degree. Among these equations, the most well-known and significant is the so-called Pell's equation[3]:

$$Dx^2 + 1 = y^2:$$

This equation has major applications in modern number theory some of which we shall mention in the next instalment.

As early as 628 CE, Brahmagupta gave a partial solution to the problem of solving $Dx^2 + m = y^2$ (D; m integers). In the Preface of his famous treatise on history of number theory, L E Dickson makes a special mention of this work ([2], p.xi):

[1] Part 1, An overview, *Resonance*, Vol.7, No.4, pp.4-19, 2002.
Part 2. Diophantine Equations: The Kuttaka, *Resonance*, Vol.7, No.10, pp.6-22, 2002.

[2] Sometimes Diophantine equations also refer to equations to be solved in rational numbers. See pp. 7-8 of the October 2002 issue and the opening paragraph of the Preface in [2].

[3] In a modern number theory text, Pell's equation is usually denoted as $x^2 - Dy^2 = 1$. We shall initially denote it by $Dx^2+1=y^2$ so as to be more consistent with ancient Indian descriptions of the equation.

\It is a remarkable fact that the Hindu Brahmegupta in the seventh century gave a tentative method of solving $ax^2 + c = y^2$ in integers, which is a far more di± cult problem than its solution in rational numbers."

If $D < 0$, then it is easy to see that there are at most ¯nitely many integral solutions of the equation $Dx^2 + m = y^2$. Again, if D is a perfect square and m a non-zero integer, then, by factoring $y^2 ¡ Dx^2$, it is easy to see that the equation has only ¯nitely many integral solutions and one can easily determine them. For instance, $(0; § 1)$ are the only integral solutions of $Dx^2 + 1 = y^2$ when D is a perfect square. Thus one is interested only in those values of D which are positive integers but not perfect squares.

Now, for small values of D, a solution of $Dx^2 + 1 = y^2$ can be found by inspection { for instance, when $D = 2$, $(x; y) = (2; 3)$ is a solution. But this is misleadingly simple. For, if $D = 61$, the smallest positive integral solution is $(x; y) = (226153980; 1766319049)$ indicating the unexpected intricacy of the general problem.

We shall discuss Brahmagupta's results which enable one to solve certain di± cult cases like $D = 83$ or $D = 92$. Brahmagupta had remarked that a person who is able to solve these two cases within a year is truly a mathematician ([3], p.364).

Brahmagupta's methods, once stated, are easy to understand and implement. To have a richer appreciation of these techniques, young readers could ¯rst spend some time in attempting to devise their own methods for ¯nding integer solutions of the equations $Dx^2 + 1 = y^2$ for special values of D. The cases $D = 83$ or $D = 92$ would, of course, be too di± cult at this stage (still, why not make an attempt?) but, before proceeding further, the students could at least try the following simpler exercise:

Exercise 1. Consider $11x^2 + 1 = y^2$. By trial-and-error,

Brahmagupta had remarked that a person who is able to solve the equations $83x^2 + 1 = y^2$ and $92x^2 + 1 = y^2$ within a year is truly a mathematician.

Keywords
Varga-Prakriti or Pell's equation, Brahmagupta's Lemma, Samasabhavana, binary composition, binary quadratic form.

Box 1. The Varga-Prakriti

The term varga-prakriti (square-natured) was used by ancient Indians for equations of the type $Dx^2 + m = y^2$ (D, m integers). The coefficient D was termed as gunaka (multiplier or qualifier) or prakriti (nature or type), while the quantity m was called ksepa, praksepa or praksepaka (additive or interpolator). The (integer) solutions corresponding to x and y were defined by Brahmagupta as adya-mula (initial or first root) and antya-mula (final or second root) respectively; later writers sometimes termed them as kanistha-pada (junior or lesser root) and jyestha-pada (senior or greater root) respectively. The Indian results on varga-prakriti have been discussed by Datta-Singh in ([7], 141-180).

the reader can easily arrive at the smallest positive integral solution $(3, 10)$. Find a larger solution.

Brahmagupta's Lemma (628 CE)

Suppose that a, b are natural numbers such that $Da^2 + 1 = b^2$, i.e., $b^2 - Da^2 = 1$. Squaring both sides, we have, $(b^2 + Da^2)^2 - D(2ba)^2 = 1$. Thus from the solution (a, b) of $Dx^2 + 1 = y^2$, we produce a bigger solution $(2ab, b^2 + Da^2)$. We can continue this process to generate infinitely many distinct solutions.

Brahmagupta (628 CE) made a more general and crucial observation – the celebrated `Brahmagupta's Lemma' ([4], Chapter 18, Verses 64-65). Using modern notations, the statement can be formulated as follows:

Lemma 1. (Brahmagupta's Lemma)

If (x_1, y_1) is a solution of $Dx^2 + m_1 = y^2$ and (x_2, y_2) is a solution of $Dx^2 + m_2 = y^2$, then $(x_1y_2 + x_2y_1, y_1y_2 + Dx_1x_2)$ and $(x_1y_2 - x_2y_1, y_1y_2 - Dx_1x_2)$ are solutions of $Dx^2 + m_1m_2 = y^2$.

In other words, we have two identities (now called Brahmagupta's identities)

$$(y_1^2 - Dx_1^2)(y_2^2 - Dx_2^2) = (y_1y_2 \pm Dx_1x_2)^2 - D(x_1y_2 \pm x_2y_1)^2.$$

The sheer beauty apart, Brahmagupta's identity has now become a standard and useful result in modern al-

Box 2. Brahmagupta's Lemma

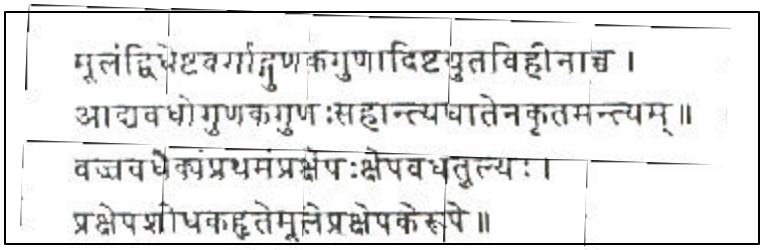
Brahmagupta's language, though not as cryptic as Aryabhata's, is still quite terse. His results have been explained more lucidly by Bhaskara II (1150). Below we give translations, adapted from Datta-Singh ([7], pp.146-148), of the verses of Brahmagupta and Bhaskara II on Brahmagupta's Lemma. For the convenience of the reader, modern notations have been inserted in parentheses [ ].

Version of Brahmagupta: \Of the square of an optional number [x_i] multiplied by the gunaka [D] and increased or decreased by another optional number [jm_ij], extract the square root [y_i]. Proceed twice [i.e., take $i = 1; 2$]. The product of the ¯rst roots [x_1x_2] multiplied by the gunaka [D] together with the product of the second roots [y_1y_2] will give a (new) second root [$Dx_1x_2 \S y_1y_2$]; the cross-products [$x_1y_2; x_2y_1$] taken together will give the (corresponding) ¯rst root [$x_1y_1 \S x_2y_1$]. The (new) interpolator will be equal to the product of the (previous) interpolators [m_1m_2]."

Version of Bhaskara II : \Set down successively the lesser root, greater root and interpolator [$x_1; y_1; m_1$]; and below them should be set down in order the same or another [$x_2; y_2; m_2$]. From them, by the Principle of Composition, can be obtained numerous roots. Therefore, the Principle of Composition will be explained here. (Find) the two cross-products of the two lesser and the two greater roots [$x_1y_2; x_2y_1$]; their sum is a lesser root. Add the product of the two lesser roots multiplied by the prakriti [D] to the product of the two greater roots; the sum will be a greater root. In that (equation) the interpolator will be the product of the two previous interpolators. Again the di®erence of the two cross-products is a lesser root. Subtract the product of the two lesser roots multiplied by the prakriti from the product of the two greater roots; (the di®erence) will be a greater root. Here also, the interpolator is the product of the two (previous) interpolators."

gebra. It plays a crucial role in problems on quadratic forms. (See [5], p.14, 83, 204, 236, 332 for discussions on applications of this identity.)

In his research monograph ([6]), Manuel Ojanguren begins a chapter (Chapter 5, p.54) by quoting Brahmagupta's original Sanskrit verses. The chapter itself is titled `Also sprach Brahmagupta'[4] and the ¯rst result


मूलंद्विघ्नेष्टवर्गाद्गुणकगुणाद्दिष्टयुतविहीनाच्च ।
आद्यवधोगुणकगुणःसहान्त्यघातेनकृतमन्त्यम् ॥
वज्रवधैक्यंप्रथमंप्रक्षेपःक्षेपवधतुल्यः ।
प्रक्षेपशोधकहृतेमूलेप्रक्षेपकेरूपे ॥

From:
Also sprach Brahmagupta

[4] In English :'Thus Spake Brahmagupta' !

in the chapter (Lemma 5.1) has also been labelled by M Ojanguren as `Brahmagupta's Lemma'! As we shall see in the last section, the result Lemma 5.1 (in [6]) is a reformulation of Brahmagupta's identity in the language of quadratic forms.

Brahmagupta's Lemma was rediscovered by the great Swiss mathematician L Euler (1707-1783) around 1758 CE. Euler highlighted the result in his writings as theorema eximium (a theorem of capital importance), theorema elegantissimum (a most elegant theorem), etc.

What makes Brahmagupta's Lemma so special? Why do renowned historians and mathematicians { especially algebraists and number-theorists { pay glowing tributes to it? The lemma has a delightful charm as well as technical power { a glimpse of this power can be felt from the way it can be used to solve a di± cult equation like $92x^2 + 1 = y^2$ in a few simple steps. And, what is more striking, implicit in the lemma are several subtle fundamental concepts of modern algebra. There is an originality and sophistication in the very attitude towards an algebraic problem that gave rise to the lemma and its ingenious applications. The techniques involved were far ahead of the times { only a rare algebraic genius could have thought along such lines in the seventh century.

Sometimes the brilliance of an algebraic research lies in its opening up of new and unexpected horizons with immense possibilities through surprisingly simple innovations. But, ironically, the very simplicity of the work makes it di± cult for later generations to fathom its greatness![5] Further, once a reader gets accustomed to an original idea, the familiarity often hinders a proper appreciation of its true worth. For cultivation of the right perspective, it is desirable that results are also seen in their historical contexts.

[5] See the remarks of Laplace in side-box of page 13 of *Resonance*, April 2002.

Let us ¯rst analyse a few consequences of Brahmagupta's

Lemma pertaining to the equation $Dx^2 + m = y^2$. Before proceeding further, the reader is invited to find integer solutions for $83x^2 + 1 = y^2$ and $92x^2 + 1 = y^2$ using Brahmagupta's Lemma.

The Samasabhavana and Applications

For a given positive integer D, Brahmagupta's Lemma enables one to define a multiplicative structure on the set of integral solutions of the equations $Dx^2 + m = y^2$. For convenience, let us denote by $(p; q; m)$ a triple of integers satisfying $Dp^2 + m = q^2$. Brahmagupta's Lemma gives two laws of binary composition (which we denote by $\circ$):

$$(p; q; m) \circ (r; s; n) = (ps \pm qr; qs \pm Dpr; mn).$$

These laws came to be known as the bhavana (`production' or `composition') rules: the law obtained by taking the positive sign was called the samasabhavana (additive composition)[6] and the rule obtained by taking the negative sign was called the antarabhavana (subtractive composition). In the special case of equal roots and interpolators, the rule was called tulyabhavana (composition of equals). (See [7], p 148).

[6] From Vedic times, addition has been called *samasa* ('putting together') and the sum obtained *samasta* ('whole', 'total', etc).

Thus, Brahmagupta's Lemma provides, in particular, laws of composition on the set of integral solutions of the specific equation $Dx^2 + 1 = y^2$. The samasabhavana is perhaps the first known instance of an involved abstract algebraic thinking. We shall discuss this aspect in a subsequent section.

The samasabhavana enables one to generate infinitely many integral solutions to the equation $Dx^2 + 1 = y^2$ from a given non-trivial integral solution. If $p; q$ are positive integers satisfying $Dp^2 + 1 = q^2$, then define $(p_0; q_0) = (p; q)$ and $(p_{i+1}; q_{i+1}) = (p; q) \circ (p_i; q_i)$, where $\circ$ is the samasabhavana. It is easy to see that $p_{i+1} > p_i > \cdots > p_1 > p_0$ and $q_{i+1} > q_i > \cdots > q_1 > q_0$, i.e., the solutions are distinct and increasing. One can thus generate arbitrarily large solutions!

Exercise 2. Use this trick to solve Exercise 1. Can you determine whether the solution you get (by applying samasabhavana) is the least possible solution greater than the pair (3; 10)? (This may not be easy { we shall discuss the question in a later instalment.)

Exercise 3. Show that the equation $3x^2 + 2 = y^2$ does not have any integral solution.

In general, when the equation $Dx^2 + m = y^2$ does have an integral solution, the samasabhavana can use that solution and a non-trivial integral solution of $Dx^2 + 1 = y^2$ to generate in¯nitely many integral solutions of $Dx^2 + m = y^2$ (as the reader can verify). This was stated by Brahmagupta (verse[7] 66) as follows ([7] p.173):

[7] Henceforth we shall be referring to verses in Chapter 18 of [4].

From two roots (of a square-nature) with any given additive or subtractive, by making (combination) with the roots for the additive unity, other ¯rst and second roots of (the equation having) the given additive or subtractive (can be found).

As explicitly mentioned by Sripati (1039) and Bhaskara II (1150), and implicit in Brahmagupta (verses 65-66), the samasabhavana also gives a method for ¯nding in¯nitely many solutions in rational numbers to the equation $Dx^2 + 1 = y^2$ ([7], pp.151{153). As before, we need to ¯nd one non-trivial rational solution. But this is quite easy. Choose any positive integer p and any positive integer q such that $q^2 > Dp$. Put $m = q^2 - Dp^2$. We have a triple $(p; q; m)$. Applying samasabhavana on the triple $(p; q; m)$ with itself, we have the triple $(2pq; Dp^2 + q^2; m^2)$. This gives a rational solution $x = 2pq=m$; $y = (Dp^2 + q^2)=m$ to the equation $Dx^2 + 1 = y^2$.

But the question remains: How does one obtain a non-trivial integral solution to $Dx^2 + 1 = y^2$? Again, using the samasabhavana, Brahmagupta derived integral solutions to the equation $Dx^2 + 1 = y^2$ from any triple $(p; q; m)$ where $m \in \{-1; \pm 2; \pm 4\}$. His results (verses

67-68) may be summarised as follows[8]:

(p; q; § 1)) (2pq; 2q² ¨ 1; 1).

(p; q; § 2)) (pq; q² ¨ 1; 1).

(p; q; § 4)) (pq=2; q²=2 ¨ 1; 1) if p even.

(p; q; + 4)) (p(q² ¡ 1)=2; q(q² ¡ 3)=2; 1) if p odd.

(p; q; ¡ 4)) (pq(q² + 1)(q² + 3)=2; (q² + 2)
[(q² + 1)(q² + 3) ¡ 2]=2; 1) if p odd.

The reader can easily deduce all the above formulae by repeated use of the samasabhavana rule and necessary simpli¯cations. (Note that Dp² + q² is replaced by 2q² ¡ m which simpli¯es calculations during applications.) For m = § 1 or § 2, it is enough to apply samasabhavana on (p; q; m) with itself once. Similarly for m = § 4 when p is even. If p is odd, then for m = 4, one has to compose (p; q; m) with itself twice, i.e., consider (p; q; m) ¯ (p; q; m) ¯ (p; q; m); for m = ¡ 4, one applies the composition ¯ve times { or better, composes (p; q; m) ¯ (p; q; m) with itself twice.

Now Brahmagupta's techniques can be used to solve the equation Dx² + 1 = y² in a variety of cases, including the cases D = 83 and D = 92 mentioned earlier.[9] The least positive integral solutions in these cases are (9; 82) and (120; 1151) respectively.

However, for general D, one still needs an algorithm for ¯nding some triple (p; q; m) where m 2 f§ 1; § 2; § 4g. Till then, the above results can be applied only to those speci¯c values of D for which one gets such a triple through inspection or clever manipulations. Even when such a triple becomes available for a special D, Brahmagupta's methods lead to some positive integral solution of Dx² + 1 = y² { but that need not be the minimum; and therefore the samasabhavana will fetch only

[8] A notation like '$(p, q; -2) \Rightarrow (pq, q^2 + 1; 1)$' would mean 'If $Dp^2 - 2 = q^2$, then $D(pq)^2 + 1 = (q^2 + 1)^2$.'.

[9] Note: $83 \times 1^2 - 2 = 9^2$; $92 \times 1^2 + 8 = 10^2$. For $D = 92$, (1,10;8) can be composed with itself to obtain (5, 48;4). Another approach: As it is enough to solve $92x^2 + 4 = y^2$ and hence $23x^2 + 1 = z^2$, use $23 + 2 = 5^2$.

in¯nitely many integral solutions, but not necessarily all integral solutions.

But then, as we shall discuss in a later instalment, Brahmagupta's novel ideas also contain the key to the discovery of the subsequent chakravala algorithm which is a perfect method (free from trial-and-error) for obtaining, for any D, the minimum positive integral solution of $Dx^2 + 1 = y^2$. In fact, his results also aid the chakravala in rapidly arriving at this minimum solution. The samasabhavana then generates all integral solutions from the minimum one.[10] Thus Brahmagupta's partial solution, apart from being a remarkable landmark by itself, was also a signi¯cant step towards the grand climax { the chakravala !

[10] The statement needs proof – it will be discussed in a later instalment.

Brahmagupta's Lemma and Modern Abstract Algebra

Let Z denote the set of integers and $S = \{(x, y, m) \in Z \times Z \times Z \mid Dx^2 + m = y^2\}$. By Brahmagupta's Lemma, the operation $\circ$ de¯ned by $(p, q, m) \circ (r, s, n) = (ps + qr, Dpr + qs, mn)$ is a binary composition on the set S. Recall that the operation $\circ$ is precisely the samasabhavana and that `bhavana' means composition. This sophisticated idea of constructing a binary composition on an abstractly de¯ned but unknown set is the quintessence of modern `abstract algebra'. It is a wonder that, in an attempt to solve an equation, a seventh-century mathematician thought of constructing an intricate abstract structure on the solution set of a system of equations. This is an original attitude to mathematics the like of which was not to be seen for the next 1000 years.

Brahmagupta's Lemma in Historical Context

Brahmagupta is the ¯rst known mathematician to have systematically investigated the problem of ¯nding in¯nitely many integral solutions of the equation $x^2 - Dy^2 = 1$. This equation has a rich and interesting history which

we shall brie° y outline in the next instalment. We mention here that, after Brahmagupta's partial solution in 628 CE, a complete solution (chakravala algorithm) was described by an unknown Indian mathematician named Jayadeva[11] around 10th century CE (or earlier). A similar method was also described by Bhaskara II (1150 CE). The examples worked out by Bhaskara to illustrate the chakravala include the case D = 61 with least positive integral solution (226153980; 1766319049). Several centuries later, Fermat (1657) raised the problem of solving $x^2 - Dy^2 = 1$ in integers and Brouncker gave a general method of solution.[12]

[11] Not to be confused with the Vaishnava poet of Geeta-Govinda fame.

[12] In a text of 1693, J Wallis described Brouncker's solution and also mentioned the work of John Pell. Euler probably confused their contributions and named the equation $x^2 - Dy^2 = 1$ as Pell's equation although Pell had nothing to do with *this* equation. Since then, the name of Pell has got strongly linked with the equation.

The Indian achievements on the Pell's equation between 7th and 10th century appear all the more striking when contrasted with the general evolution of algebraic thought. Till the 16th century CE, Arab and European mathematicians had to struggle with problems involving equations of the type ax + b = c (a; b; c positive integers) as shown by the prevalence of the cumbrous `rule of false position' (see Box 3)! As D E Smith remarked:

Box 3. The Rule of False Position

One form of the rule may be stated in our current algebraic language as follows: to solve a problem involving a simple linear equation of the type ax + b = c, one guesses a value, say u, for the unknown x; computes d = au + b, and then applies the rule x = u + (c ¡ d)=a or x = u ¡ (d ¡ c)=a, depending on whether c > d or d > c. The rule may appear weird now, but it used to be applied in a mathematical atmosphere where one did not have notations for the unknown, avoided negative numbers, and had not developed the culture of framing and solving algebraic equations. Another form (double false position) for solving the equation f(x) = c, where f(x) = ax + b, was to guess two values for x, say u and v, compute f(u) = p and f(v) = q, determine the errors $e_u = c ¡ p$ and $e_v = c ¡ q$, and then apply the rule x = $(ve_u ¡ ue_v)=(e_u ¡ e_v)$. The rule was popular among the Arab and European mathematicians during the Middle Ages prior to the 16th century Renaissance. It is referred as elchataym by Fibonacci (13th century), el cataym by Pacioli (1494), Regola Helcataym by Tartaglia (1556), Regole del Cattaino by Pagani (1591), etc. As late as 1542 CE, the prominent arithmetician Robert Recorde thought highly of this rule. Smith remarked (p.439), \Awkward as this seems, the rule was used for many centuries, a witness to the need for and value of a good symbolism." For more details, see Datta-Singh ([7], 37-38), D E Smith (History of Mathematics II, Dover 1953, pp.437-442) and F Cajori (History of Mathematics, AMS Chelsea NY 2000, pp.103, 110).

To the student of today, having a good symbolism at his disposal, it seems impossible that the world should ever have been troubled by an equation like $ax + b = 0$. Such, however, was the case, ... (History of Mathematics II, p.437).

When we think about the general level of algebraic maturity attained by the pre-Renaissance mathematical community, the algebraic depth of Brahmagupta as reflected in the samasabhavana, looks astonishing.

Brahmagupta was born in an era when symbolic algebra was still at its infancy. He himself established some of its basic features. He took the important step of introducing zero as an integer in algebra and formulating the rules of arithmetic operations involving negative numbers and zero. Brahmagupta also contributed to the evolution of good notations and terminology (like the use of distinct letters for several unknowns), the formation and handling of equations; and so on.[13]

[13] In a subsequent article, we shall elaborate on Brahmagupta's role in the advancement of basic symbolic algebra in Indian mathematics.

Possible Genesis of Brahmagupta's Lemma

It would be instructive and interesting to explore, in retrospect, how a great mathematician could possibly have arrived at his discovery. Even if the actual thought-process of Brahmagupta had been completely different, a meaningful speculation could provide additional insight into the problem. So let us indulge in this game. (See [8] for an interesting discussion on the same idea.)

Now, in most ancient civilisations { especially the Babylonian, Chinese and Vedic Indian { practical construction problems had led to the construction of what are called Pythagorean triples, i.e., integer triple $(x; y; z)$ satisfying $x^2 + y^2 = z^2$. Pythagorean triples continued to fascinate subsequent ancient number-theorists like Euclid (300 BCE), Diophantus (250 CE) and Brahmagupta (628 CE). They explicitly described the general solution of the Pythagorean triple. Now, it is very

likely that while playing with Pythagorean triples, the minds of such number-theorists would have been led to the question: When is a positive integer N (not necesarily a square) expressible as a sum of two squares ($a^2 + b^2$; $a < b$)?[14]

The smallest such numbers are clearly $5 = 1^2 + 2^2$ and $13 = 2^2 + 3^2$. It can be easily seen that, in these two cases, the decomposition is unique. But then a mathematical explorer would observe that $65 [= 5 £ 13 = (1^2+ 2^2)(2^2+ 3^2)]$ can be expressed as sums of two distinct squares in two di®erent ways: namely, $65 = 1^2 + 8^2 = 4^2 + 7^2$. A mature algebraic mind would realise (maybe, after observing a few more of such examples) that the non-uniqueness in the decomposition of 65 is no accident { it is a consequence of the algebraic identity

$$(x^2 + y^2)(z^2 + t^2) = (xz + yt)^2 + (xt ¡ yz)^2 =$$

$$(xz ¡ yt)^2 + (xt + yz)^2: \quad (¤)$$

It seems possible that, while handling Pythagorean triples, ancient Indians would have arrived at this identity.[15]

Brahmagupta, who explicitly gave[16] the integer solution $(2mn; m^2 ¡ n^2; m^2 + n^2)$ of the equation $x^2 + y^2 = z^2$, might have been led to the identity (¤) or, equivalently, the now well-known fact that $m = x^2 + y^2$ and $n = z^2 + t^2$ imply $mn = (xz § yt)^2 + (xt ¨ yz)^2$. If so, then, while considering $Dx^2 + m = y^2$, he might have been on the lookout for analogous identities amenable to application in his situation. Given his skill, he would have noticed the relevant algebraic patterns to arrive at the appropriate generalisations.

Note that, using complex numbers, Brahmagupta's identities readily follow from (¤) by replacing y by $y\sqrt{¡D}$ and t by $t\sqrt{¡D}$. But, as Weil points out ([5], p 14), "this could not have been fully realized until the eighteenth century".[17]

[14] The problem can now be fairly easily solved by analysing it in the ring of Gaussian integers. See Chapter 11 of the text *Algebra* by M Artin.

[15] The identity occurs explicitly in Fibonacci (1225 CE) and implicitly in Diophantus (see [5], pp. 10-11).

[16] See ([4] : Chapter 12, Verse 33).

[17] Complex numbers began to appear in mathematics only in the 16th century CE – its vigorous use can be seen from the 18th century.

A slick proof of Brahmagupta's identity $(y^2 - Dx^2)(t^2 - Dz^2) = (yt + Dxz)^2 - D(yz + tx)^2$ may be obtained by splitting the terms $y^2 - Dx^2, t^2 - Dz^2$ and observing the identity $(y + x\sqrt{D})(t + z\sqrt{D}) = (yt + Dxz) + (yz + xt)\sqrt{D}$. Multiplying this identity by the conjugate identity $(y - x\sqrt{D})(t - z\sqrt{D}) = (yt + Dxz) - (yz + xt)\sqrt{D}$, one gets Brahmagupta's identity. This was the approach of Euler. Had Brahmagupta's thought-process (both the discovery as well as the proof of his main result) taken a similar route?

Brahmagupta's Lemma and Binary Quadratic Forms

Results on the Pell's equation are of great importance in the theory of binary quadratic forms. An expression of the form $Ay^2 + 2Byx + Cx^2$ is called a binary quadratic form with discriminant $B^2 - AC$. In particular, $y^2 - Dx^2$ is a binary quadratic form with discriminant D. Thus, in the language of quadratic forms, Brahmagupta's identity says that two such forms (say $y^2 - Dx^2; v^2 - Du^2$) can be `composed' to yield another such form with discriminant $D$ in a new pair of variables $(xv \pm yu; yv \pm Dxu)$. Again recall that the word `bhavana' means `composition'! We mention here that the theory of composition of quadratic forms is an important and rich topic initiated by Gauss and Dirichlet in the 19th century and is still a very active area of research.

One does not know the initial motivation of Brahmagupta in investigating equations like $y^2 - Dx^2 = 1$. But, a thousand years later, Fermat's researches in number theory led him to a deep study of the binary quadratic form $y^2 - 2x^2$ which must have resulted in his realisation of the far-reaching importance of the study of the equation $y^2 - Dx^2 = 1$. (See [5] for more details.)

Before mentioning another useful modern version of Brahmagupta's Lemma, we define a few terms. Two quadratic forms f and g are said to be equivalent if there exists

a homogeneous linear change of variables which takes the form f to the form g. More precisely, the quadratic forms f(x;y) and g(x;y) are equivalent if there exists a non-singular (i.e., invertible) matrix A such that g(x) = f(Ax) where x denotes the vector $(x;y)^T$. Thus, if the quadratic forms are de¯ned over a `¯eld' K containing the rational numbers, then f and g are equivalent if there exists a;b;c;d in K with ad ¡ bc 6= 0 such that g(x;y)= f(ax + by;cx + dy). For instance, f = xy is equivalent to g = x^2 ¡ y^2 since g(x;y) = f(u;v) where u = x + y; v = x ¡ y.[18]

A number c is said to be represented by a binary form f(x;y) if the value c is attained by f, i.e., if there exist numbers a;b (in the ¯xed ¯eld or ¯xed integral domain K) such that c = f(a;b). For instance, if we restrict ourselves to the ¯eld of rational numbers, or even the ¯eld of real numbers, then ¡1 is not represented by the form $x^2 + y^2$. A quadratic form f is said to be strongly multiplicative if f is equivalent to cf for every non-zero c represented by f.

Let f denote the binary form y^2 ¡ Dx^2 and c be a non-zero number represented by f. Then Brahmagupta's Lemma tells us that f is equivalent to cf (i.e., y^2 ¡ Dx^2 is strongly multiplicative). For, if c = b^2 ¡ Da^2 and g = cf, then g(x;y) = (b^2 ¡ Da^2)(y^2 ¡ Dx^2). Now Brahmagupta's identity prescribes the substitution that has to be made to obtain g(x;y) = f(u;v), namely, the bijective homogeneous linear transformation given by u = bx + ay; v = Dax + by. (Note that the determinant of this transformation is c which is non-zero). The equivalence of f and cf is essentially the `Lemma 5.1' referred by Ojanguren in ([6], pp.54{55) as `Brahmagupta's Lemma'. This result was generalised in 1965 by A P¯ster using, what are now called, `P¯ster forms'.[19] P¯ster's discovery opened up new directions in the theory of quadratic forms. For an introductory exposition on P¯ster's theory, see ([9], [10]). Incidentally, some

[18] To minimise technicality, we avoided being too precise in our definitions. The coefficients A, B, C of a quadratic form belong to a fixed field or a fixed integral domain K. In general the condition for equivalence of f and g is that $ad–bc$ must be a 'unit' in K. The equivalence of $x^2–y^2$ and xy holds over fields containing the rational numbers; but it does not hold over integral domains where 2 does not have inverse. (For instance, it does not hold over the domain of integers or over fields 'of characteristic 2'.)

[19] For readers familiar with the relevant terminology, Lemma 5.1 in ([6], p54) states that if K is a field of characteristic different from 2, and c is a non-zero element of K represented by the quadratic space $\langle 1, a\rangle$, then $\langle 1, a\rangle$ is isometric to $\langle c\rangle\langle 1, a\rangle$. The generalisation of Pfister (Lemma 5.2 in [6], p.55) states that Pfister forms are multiplicative.

Indian mathematicians have made signi¯cant contributions in the area of quadratic forms during the second half of the 20th century.

Suggested Reading

[1] M Atiyah, Mathematics as a basic science, *Current Science*, Vol. 65, No.12, 1993.

[2] L E Dickson, *History of the Theory of Numbers*, Chelsea Publishing Co. NY, Vol.III, 1952.

[3] H T Colebrooke, *Algebra, with Arithmetic and Mensuration, from the Sanscrit of Brahmegupta and Bhascara*, John Murray, London, 1817.

[4] Brahmagupta, *Brahma Sphuta Siddhanta* (628). The Sanskrit text, edited by R S Sharma, has been published by the Indian Institute of Astronomical Research, 1966.

[5] A Weil, *Number Theory: An approach through history from Hammurapi to Legendre*, Birkhauser, 1984.

[6] M Ojanguren, *The Witt Group and The Problem of Luroth*, Dottorato di ricerca in Mathematica, ETS EDITRICE PISA, University of Pisa, 1990.

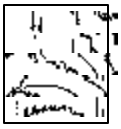
[7] B Datta and A N Singh, *History of Hindu Mathematics: A Source Book*, Part II, *Algebra*, Motilal Banarasidass, Lahore, 1935; Asia Publishing House, Bombay, 1962.

[8] R Sridharan, Ancient Indian contributions to Quadratic Algebra in *Science in the West and India*, eds B V Subbarayappa and N Mukunda, Himalaya Publishing House, Bombay, 1995.

[9] N Jacobson, *Basic Algebra*, Hindustan Pub. Corp., Delhi, Vol. 2, 1991.

[10] T Y Lam, *The Algebraic Theory of Quadratic Forms*, Benjamin, 1973.

Address for Correspondence
Amartya Kumar Dutta
Stat-Math Unit
Indian Statistical Institute
203, B.T. Road
Kolkata 700 108, India.
Email: amartya@@isical.ac.in



The road to wisdom? – Well, it's plain
and simple to express:
Err
and err
and err again
but less
and less
and less

Piet Hein