Algebraic Methods in Plane Geometry

2. Cubic Curves

Shailesh A Shirali

In Part 1 of this article we explored some connections between plane geometry and the algebra of conics. Now we bring cubic curves into the picture. We offer another algebraic proof of Pascal's theorem, and show how a group operation may be defined on the points of a cubic curve. We also show how these ideas help in finding taxicab numbers of the kind made famous by the "1729" incident featuring Hardy and Ramanujan.

Shailesh Shirali heads a Community Mathematics Center at Rishi Valley School (KFI). He has a deep interest in teaching and writing about mathematics at the high school/post school levels, with particular emphasis on problem solving and the historical aspects of the subject.

1. The Family of Cubic Curves

In Part 1 of this article we showed how the fact that the set of second degree curves is a five-parameter family leads to the result that if $\mathcal{K}_1$ and $\mathcal{K}_2$ are two second degree curves passing through four distinct points A, B, C, D, having equations $p_1(x, y) = 0$ and $p_2(x, y) = 0$, respectively, then the equation of any other second degree curve $\mathcal{K}_3$ passing through A, B, C, D may be written in the form $rp_1(x, y) + sp_2(x, y) = 0$, where r, s are real constants, not both zero. This result led to nice proofs of results like Pascal's Hexagram Theorem and the Butterfly Theorem.

Part 1. The Use of Conic Sections, *Resonance*, Vol.13, No.10, pp.916–928, 2008.

Now we extend this principle to cubic curves. The general equation of a cubic curve is

$$a_1x^3 + a_2x^2y + a_3xy^2 + a_4y^3 + a_5x^2$$

$$+a_6xy + a_7y^2 + a_8x + a_9y + a_{10} \;=\; 0,$$

where $a_1, a_2, \ldots, a_9, a_{10}$ are real constants; there are now ten constants because $\binom{4}{1} + \binom{3}{1} + \binom{2}{1} + \binom{1}{1} = 10$. (Naturally, a_1, a_2, a_3, a_4 must not all be 0.) If we multiply all the a_i's by a non-zero constant we get the same cubic. By applying some normalizing condition (like "the sum

Keywords
Cubic curves, addition of points on a cubic curve, associativity of addition, elliptic curve, abelian group, taxicab number, Carmichael number.

The family of cubic curves passing through eight given points is a one-parameter family.

of the squares of the a_i is 1") we infer that the family of cubic curves is a nine-parameter family. Therefore, the family of cubics passing through *eight* given points in general position is a one parameter family; and so, if $\mathcal{K}_1$ and $\mathcal{K}_2$ are two cubics passing through eight distinct points $\mathrm{A}_1, \mathrm{A}_2, \ldots, \mathrm{A}_8$, having equations $p_1(x, y) = 0$ and $p_2(x, y) = 0$, respectively, then the equation of any cubic curve $\mathcal{K}_3$ passing through these eight points may be written in the form $rp_1(x, y) + sp_2(x, y) = 0$, where r, s are real constants, not both zero.

This seems simple enough – but it turns out to be just what we need to explain the *associativity of addition on cubic curves*. This has exciting implications, for it allows the possibility of a *group* being defined on the points of a cubic curve. In Section 4 we show how this can be done.

2. Sketching a Cubic Curve

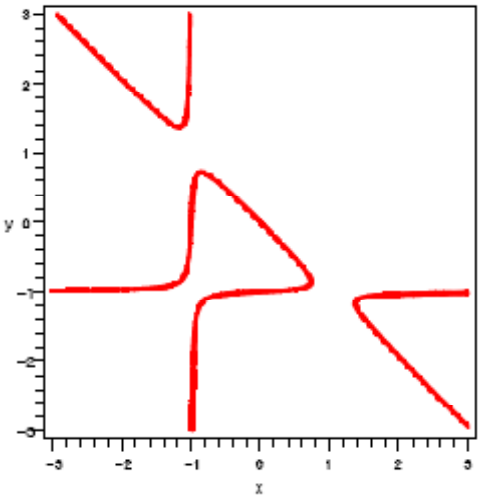
Cubic curves come in a bewildering variety of shapes, and to sketch them can be problematic. In the case of conics this is not a problem, as conics can be parametrized using rational functions; but cubic curves need *elliptic functions*, which are non-elementary and numerically rather difficult to handle. In *Figure* 1, we show some cubics, drawn using the MAPLE command `contourplot`.

3. Addition of Points on a Cubic Curve

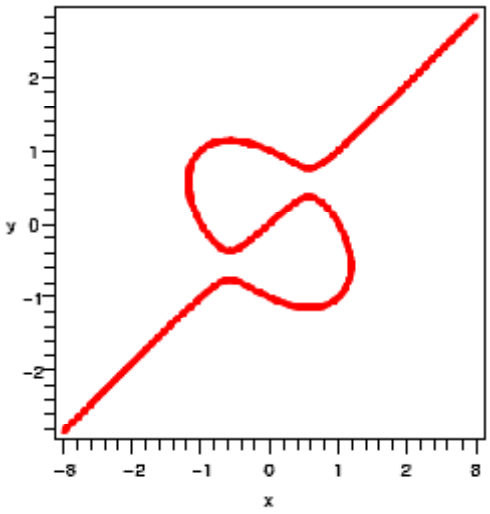
We now show that it is possible to define a binary operation $\oplus$ on the points of a cubic curve $\mathcal{K}$ in such a way that $(\mathcal{K}, \oplus)$ is a group. We shall assume that:

Conics can be parametrized using rational functions, but cubic curves need non-elementary functions.

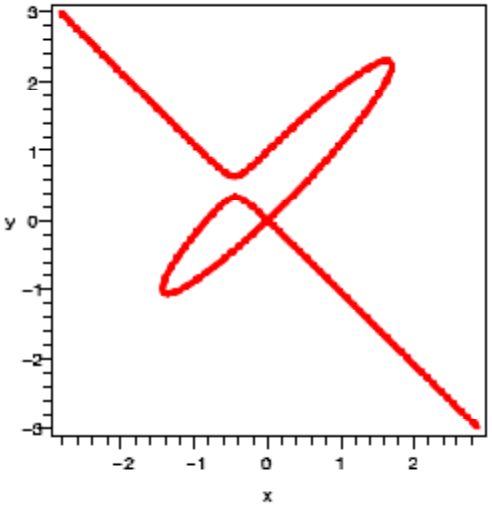
- $\mathcal{K}$ is not the union of a conic and a straight line, nor the union of three straight lines (i.e., $\mathcal{K}$ is *irreducible*). Two examples where this condition is violated are shown in *Figure* 2.
- $\mathcal{K}$ does not possess *singular points*. Examples of cubics that possess singular points are: $y^2 = x^3$,



(1) Graph of (x+y+1) (xy+y+x)–1.05xy = 0.



(2) Graph of x(x–1) (x+1)–1.2y(y+1)(y–1) = 0.



(3) $y^3 - y^2x - y^2 - x^2y + 1.2x^3 + x^2 = 0$.

Figure 1.

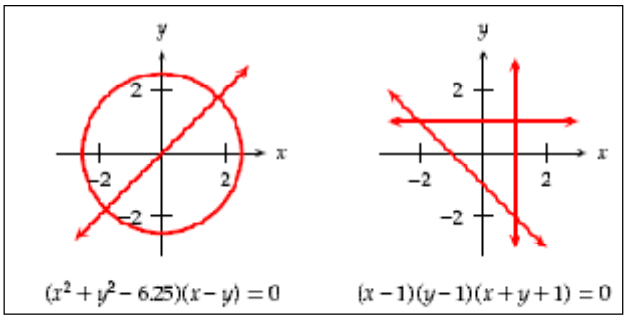


Figure 2. Examples of cubic curves that are not irreducible.

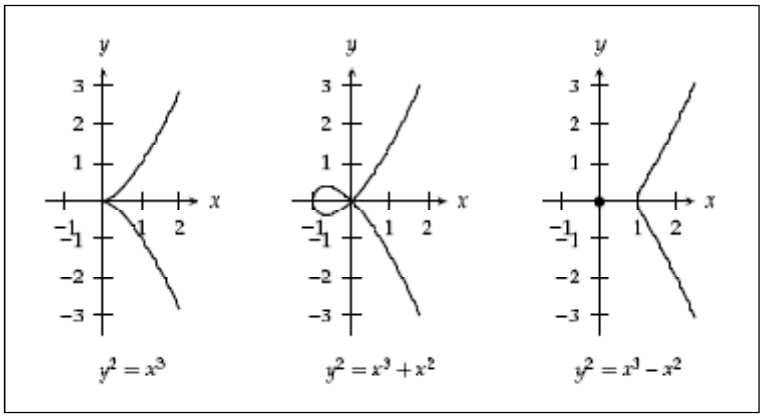


Figure 3. Examples of cubic curves with singular points.

$y^2 = x^3 + x^2$, and $y^2 = x^3 - x^2$. Each of these has a singularity at the origin (the first one has a *cusp*, the second one has a *double point*, and the third one has an *isolated point*). Their graphs are shown in *Figure* 3.

For simplicity we consider only a special kind of cubic curve: one whose equation has the form

$$y^2 = ax^3 + bx^2 + cx + d, \qquad (1)$$

where a, b, c, d are real numbers ($a \neq 0$); as y occurs only in its squared form, the curve is symmetric under reflection in the x-axis. It so happens that every cubic curve can be transformed to a curve of this type, using a suitable change in variables (this observation goes back to Isaac Newton), so there is no loss in this restriction. *Figure* 4 shows two curves of this family.

A straight line which intersects a cubic curve twice must intersect it a third time.

The possibility of defining a binary operation on such a curve $\mathcal{K}$ arises from the fact that if a, b, c, d are real numbers with $a \neq 0$, then the cubic equation $ax^3 + bx^2 + cx + d = 0$ has *three* roots over the complex domain $\mathbb{C}$; and if it has two real roots then it necessarily has a third real root (not necessarily distinct from the first two). Therefore, *a straight line which intersects a cubic curve twice must do so a third time.* To avoid needing to make exceptions to this rule, we must include in $\mathcal{K}$ those of its points which lie "at infinity". So a valid binary

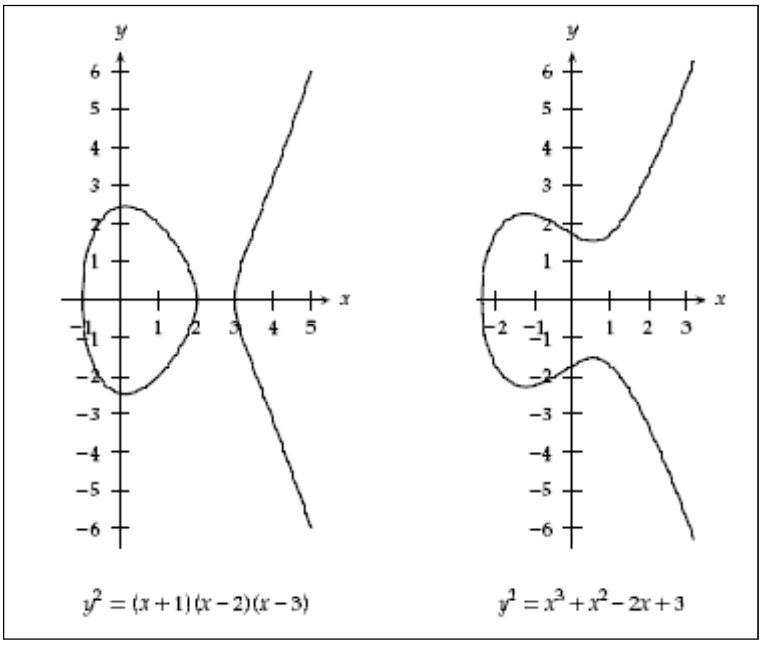


Figure 4. Two 'typical' irreducible cubic curves.

operation $*$ defined on the points of $\mathcal{K}$ is the following: if P, Q are points on $\mathcal{K}$, then we find R where $\overleftrightarrow{PQ}$ cuts $\mathcal{K}$ again, and write $P * Q = R$. The construction is shown in *Figure* 5. The rule may be described in brief thus: *Points* P, Q, R *on* $\mathcal{K}$ *are related by* $*$ *if* P, Q, R *are collinear*. Note that this means that if $P * Q = R$, then $Q * R = P$, and $P * R = Q$.

Points P, Q, R on a cubic curve are related by $*$ if they are collinear.

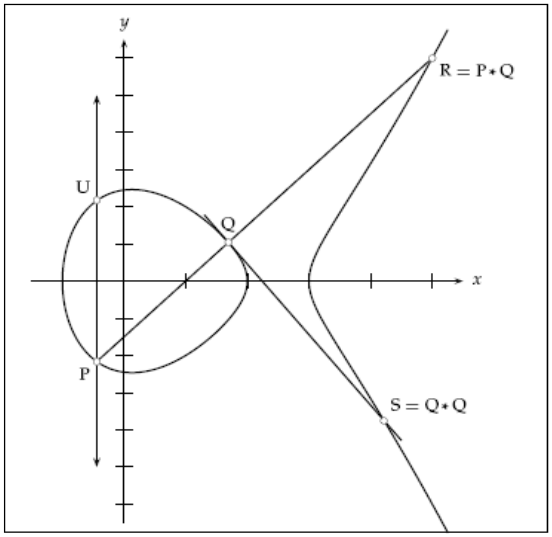


Figure 5. Illustrating how '$*$' works: $P * Q = R$, $Q * Q = S$, and $P * U$ lies at infinity.

(K, $*$) falls short of being a group by a wide margin.

This construction is well defined for every pair of points on the curve. Thus, if $\overleftrightarrow{PU}$ is parallel to the y-axis, then $P * U$ is the point of $\mathcal{K}$ which lies at infinity. To compute $Q * Q$ we draw the tangent to the curve at Q, and locate the point S where the tangent cuts the curve again; then $S = Q * Q$. Trivially, $*$ is a commutative operation.

However, the pair $(\mathcal{K}, *)$ lacks a neutral point; that is, there does not exist any point N on $\mathcal{K}$ such that $P * N = P$ for every P on $\mathcal{K}$. For, if $P * N = P$ for every P, then $P * P = N$ for every P, which means that all the tangents to the curve pass through N; this is absurd.

Nor is $*$ associative. For example, if $P * Q = R$, then $P * (Q * R) = P * P$, whereas $(P * Q) * R = R * R$, which in general is different from $P * P$.

So, $(\mathcal{K}, *)$ falls short of being a group by a rather wide margin.

But a small modification of the operation changes the scenario completely. Let N be any fixed point on $\mathcal{K}$. We define $P \oplus Q$ as follows:

$$P \oplus Q \;=\; N * (P * Q). \qquad (2)$$

In words: *First locate the third intersection* R *of* $\overleftrightarrow{PQ}$ *with* $\mathcal{K}$*, then locate the third intersection* S *of* $\overleftrightarrow{NR}$ *with* $\mathcal{K}$*, and define* <u>*this*</u> *point to be* $P \oplus Q$. The construction is illustrated in *Figure* 6.

It is easy to see that the operation $\oplus$ is commutative, and that N is the neutral element for $\oplus$. For, the operation $*$ has the property that if $P * Q = R$, then P, Q, R are collinear, and so both of the relations

$$P * R = Q, \quad Q * R = P$$

are true. In particular, this means that $N * (P * N) = P$, i.e., $P \oplus N = P$. As this relation is true for every P, the claim follows. Note also that $N * (N * N) = N$, implying that $N \oplus N = N$, as it should be.

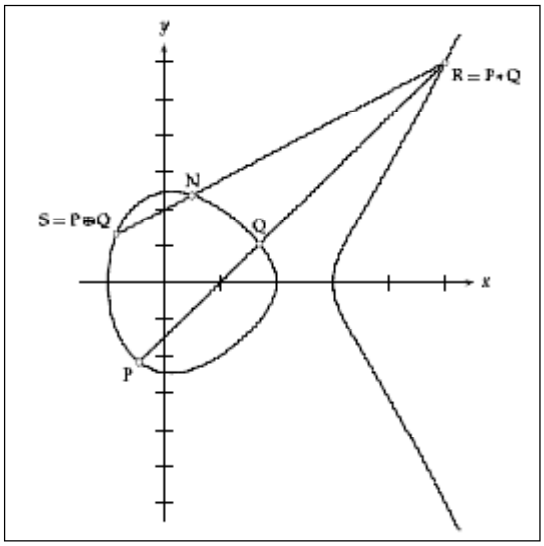


Figure 6. Addition of points on a cubic curve $\mathcal{K}$, with N as a fixed point.

Does an *inverse element* exist for every point on $\mathcal{K}$ with respect to $\oplus$? That is, given a point P on $\mathcal{K}$, can we necessarily find a point Q such that $P \oplus Q = N$? (Naturally, Q will depend on P.) We shall take up this question a bit later.

4. Associativity of the Operation

We now show a very significant property of $\oplus$; namely, that it is an *associative operation*. That is, we show that the identity

$$P \oplus (Q \oplus R) \;=\; (P \oplus Q) \oplus R \qquad (3)$$

holds for all triples of points P, Q, R on $\mathcal{K}$. A computational proof could be attempted – but only if one is prepared to rough it out! Instead, we shall use the "family of curves" principle and obtain a neat proof.

We shall prove associativity of addition using the "family of curves" principle.

Rather than draw the graph and insert all the points involved, we shall make a schematic sketch. Note the steps involved: (i) We compute $Q * R$ and $P * Q$. (ii) Next we compute $P \oplus Q = N * (P * Q)$ and $Q \oplus R = N * (Q * R)$. (iii) Then we compute $(P \oplus Q) * R$ and $P * (Q \oplus R)$. (iv) Finally we compute $(P \oplus Q) \oplus R = N * ((P \oplus Q) * R)$ and $P \oplus (Q \oplus R) = N * (P * (Q \oplus R))$. We may depict the points as shown in *Figure* 7.

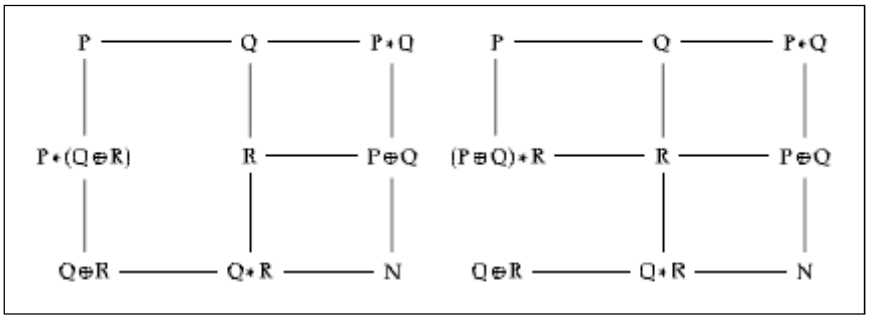


Figure 7. Schematic representation of addition of points on a cubic curve.

The diagram is read as follows: *If three points* X, Y, Z *are shown in a row or a column thus:* X–Y–Z*, then they represent collinear points.* So $\{P, Q, P * Q\}$ are collinear, as are $\{P * Q, P \oplus Q, N\}$, and so on. Observe that each grid has a blank; one 'line' is missing from each one. This tells us that we do not know at the outset whether $\{P \oplus Q, R, P * (Q \oplus R)\}$ are collinear or not; likewise for $\{P, (P \oplus Q) * R, Q \oplus R\}$. *Rather, this is what we have to prove.* For convenience we denote the various points as follows:

$$\begin{aligned} &X_1 = P, && X_2 = Q, && X_3 = P * Q, \\ &X_4 = P * (Q \oplus R), && X_5 = R, && X_6 = P \oplus Q, \\ &X_7 = Q \oplus R, && X_8 = Q * R, && X_9 = N, \end{aligned} \qquad (4)$$

and $X_{10} = (P \oplus Q) * R$. We must now show that $X_4 = X_{10}$.

Define cubics $\mathcal{K}_1, \mathcal{K}_2$ as follows (each is the union of three straight lines):

$$\begin{aligned} \mathcal{K}_1 &= \overleftrightarrow{X_1 X_4 X_7} \cup \overleftrightarrow{X_2 X_5 X_8} \cup \overleftrightarrow{X_3 X_6 X_9}, \\ \mathcal{K}_2 &= \overleftrightarrow{X_1 X_2 X_3} \cup \overleftrightarrow{X_{10} X_5 X_6} \cup \overleftrightarrow{X_7 X_8 X_9}. \end{aligned} \qquad (5)$$

Then $\mathcal{K}_1$ and $\mathcal{K}_2$ have 8 points in common (namely: X_1, X_2, X_3, X_5, X_6, X_7, X_8, X_9), while the given cubic curve $\mathcal{K}$ contains these 8 points as well as X_4, X_{10}.

Let the equations of $\mathcal{K}_1, \mathcal{K}_2, \mathcal{K}$ be $f_1 = 0$, $f_2 = 0$, $f = 0$, respectively. Then there exist real numbers r, s such that

$$f = r f_1 + s f_2. \qquad (6)$$

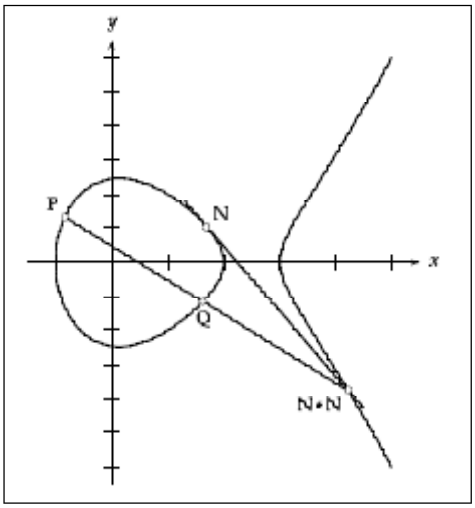


Figure 8. Construction of inverse of a point: if P * (N * N) = Q, then Q and P are a pair of inverse elements.

Since $f(X_4) = 0$ and $f_1(X_4) = 0$, it follows that $sf_2(X_4) = 0$. Similarly we find that $rf_1(X_{10}) = 0$. It cannot be that both r and s are 0. It follows that either $X_4 \in \mathcal{K}_2$, or $X_{10} \in \mathcal{K}_1$. In either case, since a straight line cannot intersect a cubic curve in more than three points, it must be that $X_4 = X_{10}$. Therefore, it must be that $P * (Q \oplus R) = (P \oplus Q) * R$, and associativity of $\oplus$ follows. □

Only one step remains before we can proclaim that $(\mathcal{K}, \oplus)$ is a group: we must show that each point P on $\mathcal{K}$ has a well-defined inverse, i.e., a point Q on $\mathcal{K}$ such that $P \oplus Q = N$.

By definition, if $P \oplus Q = N$, then $N * (P * Q) = N$. Now if $N * R = N$ for some point R on $\mathcal{K}$, it means that the tangent to $\mathcal{K}$ at N passes through R. That is, $R = N * N$. It follows that the inverse element Q is given by the neat relation

$$Q = P * (N * N). \qquad (7)$$

The construction is illustrated in *Figure* 8. It may be compactly described in words thus: *Each line through* $N * N$ *meets* $\mathcal{K}$ *in a pair of inverse points.*

It follows from the above that $(\mathcal{K}, \oplus)$ is an abelian group. □

Remark 1. It should now be clear why we insist that $\mathcal{K}$ must be irreducible and have no singular point. For, if $\mathcal{K}$ has a straight line component ℓ, then we are unable to compute inverses of points on ℓ; and if P is a singular point of $\mathcal{K}$, then the computation of $P \oplus P$ is problematic.

Remark 2. Suppose that the coefficients of the equation of the cubic curve $\mathcal{K}$ are all rational numbers. Consider the *rational points on* $\mathcal{K}$, i.e., the points on $\mathcal{K}$ whose coordinates are rational numbers. Denote the set of such points by $\mathcal{K}_{\mathbb{Q}}$. Choose the neutral point N from $\mathcal{K}_{\mathbb{Q}}$. Then, $(\mathcal{K}_{\mathbb{Q}}, \oplus)$ *is a subgroup of* $(\mathcal{K}, \oplus)$.

To see why, let A, B be points in $\mathcal{K}_{\mathbb{Q}}$. Since the coordinates of A and B are rational numbers, the equation of $\overleftrightarrow{AB}$ has rational coefficients. Eliminating y from this equation and that of $\mathcal{K}$, we get a cubic equation in x with rational coefficients. Since two solutions of this equation are rational numbers, so must be the third (invoke the 'sum of the roots' identity to see why). Hence, $A * B$ is a rational point. And since N is a rational point, so is $A \oplus B = N * (A * B)$. Therefore, $\mathcal{K}_{\mathbb{Q}}$ is closed under $\oplus$, and $(\mathcal{K}_{\mathbb{Q}}, \oplus)$ is a subgroup of $(\mathcal{K}, \oplus)$.

Remark 3. The study of irreducible, non-singular cubic curves leads to a fascinating topic: ***elliptic curves***. An enormous amount of work has been done on this topic in recent decades, resulting in applications in areas such as cryptography and integer factorization. Elliptic curves played a central role in the proof of Fermat's Last Theorem by Andrew Wiles. Readers may refer to [2], [3], and [4] for more on this topic.

5. Pascal's Theorem

In the first part of this article we gave an algebraic proof of Pascal's theorem: *The opposite sides of a hexagon inscribed in a conic intersect in three collinear points.* Now we give a second such proof, this time making use of cubic curves.

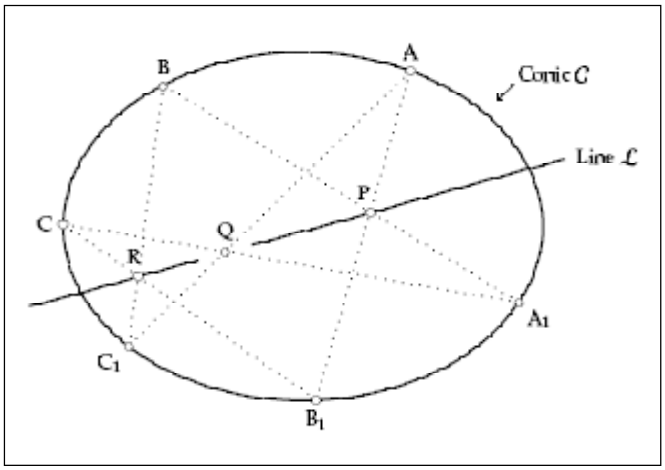


Figure 9.

In *Figure* 9 we see a conic $\mathcal{C}$ and an inscribed hexagon $AB_1CA_1BC_1$. The three pairs of opposite sides meet at P, Q, R. Let $\mathcal{L}$ be the line $\overleftrightarrow{PR}$. To show that P, Q, R are collinear, we must show that $Q \in \mathcal{L}$.

Consider the following three cubic curves,

$$\begin{aligned}\mathcal{K}_1 &= \overleftrightarrow{AB_1} \cup \overleftrightarrow{BC_1} \cup \overleftrightarrow{CA_1},\\ \mathcal{K}_2 &= \overleftrightarrow{A_1B} \cup \overleftrightarrow{B_1C} \cup \overleftrightarrow{C_1A},\\ \mathcal{K}_3 &= \mathcal{C} \cup \overleftrightarrow{PR};\end{aligned}$$

with equations $f_1 = 0$, $f_2 = 0$, $f_3 = 0$. Note that $A, B, C, A_1, B_1, C_1, P, R$ lie on all the three cubics, and Q lies on $\mathcal{K}_1$ and $\mathcal{K}_2$ as well. If we can show that $Q \in \mathcal{K}_3$, then our task will be done. Now the family of cubics passing through the eight points $A, B, C, A_1, B_1, C_1, P, R$ is a one-parameter family. This means that $f_3 = \alpha f_1 + \beta f_2$ for some real constants α, β, not both zero. Since $Q \in \mathcal{K}_1$ and $Q \in \mathcal{K}_2$, we have $f_1(Q) = 0 = f_2(Q)$, and hence $f_3(Q) = 0$ too. Therefore, $Q \in \mathcal{K}_3$. It cannot be that $Q \in \mathcal{C}$ (for this would mean that $\mathcal{C}$ and $\overleftrightarrow{AC_1}$ intersect in three distinct points); so it must be that $Q \in \mathcal{L}$. Hence, P, Q, R are collinear.

6. Taxicab Numbers

To conclude, we show how the above results help to find *taxicab numbers*. The significance of this term lies in a

well-known incident featuring Hardy and Ramanujan. Here it is, in Hardy's own words:

> I remember once going to see him when he was ill at Putney. I had ridden in taxi cab number 1729 and remarked that the number seemed to me rather a dull one, and that I hoped it was not an unfavorable omen. "No," he replied, "it is a very interesting number; it is the smallest number expressible as the sum of two cubes in two different ways."

The "two ways" are, of course, $1729 = 10^3 + 9^3$, $1729 = 12^3 + 1^3$. Numbers with such a property have come to be known as *taxicab numbers*. We shall show how to generate more such numbers analytically (as distinct from a computer-assisted search).

Suppose that an integer N may be written as $a^3 + b^3$, where a, b are integers. *Then* (a, b) *is a rational point on the cubic curve whose equation is* $x^3 + y^3 = N$. (This is an elliptic curve.) If we can find another rational point (c, d) on this curve, then we would have $a^3+b^3 = c^3+d^3$. By suitably scaling up all the quantities involved we would obtain an integer which is the sum of two cubes in two different ways. With some care we can ensure that all the quantities involved are positive and thus get an answer to our search.

To start with, let us take $a = 1$, $b = 2$; then $a^3 + b^3 = 9$. Shown in *Figure* 10 is the graph of the curve $x^3+y^3 = 9$, with the point $\mathrm{P}(1, 2)$ labeled.

A taxicab number is one which can be written as a sum of two positive cubes in more than one way.

A bit of computation reveals that the tangent t_{P} to the curve at P has the equation $x + 4y = 9$, and that it meets the curve again at the point $\mathrm{Q}\,(-\frac{17}{7}, \frac{20}{7})$. This means that we have the equality

$$1^2 + 2^3 \;=\; \left(-\frac{17}{7}\right)^3 + \left(\frac{20}{7}\right)^3,$$

which leads to $7^3+14^3+17^3 = 20^3$. Therefore the integer $7^3 + 14^3 = 3087$ is a sum of two cubes in two different

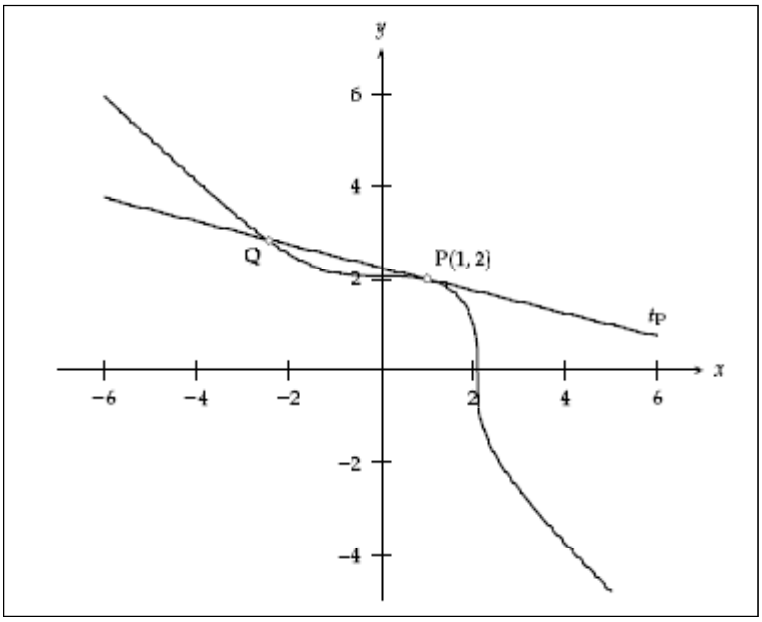


Figure 10.
Graph of $x^3 + y^3 = 9$.

ways, the other way being $(-17)^3 + 20^3$. Note that a negative integer has been used in one of the representations.

If we take $a = 1$, $b = 3$, then we get the curve $x^3 + y^3 = 28$. The tangent t_R to this curve at the point $R(1, 3)$ has the equation $x + 9y = 28$, and it meets the curve again at the point $S\left(-\frac{55}{26}, \frac{87}{26}\right)$. So we obtain more such equalities:

$$1^2 + 3^3 \;=\; \left(-\frac{55}{26}\right)^3 + \left(\frac{87}{26}\right)^3, \quad 26^3 + 78^3 + 55^3 \;=\; 87^3.$$

Once again we have used a negative integer in one of the representations. But if we take the trouble to find where the tangent to the curve at S intersects the curve again, we find that it is at the point

$$U \;=\; \left(\frac{63284705}{21446828}, \frac{28340511}{21446828}\right),$$

and now both the coordinates are positive. So we have:

$$1^3 + 3^3 \;=\; \left(\frac{63284705}{21446828}\right)^3 + \left(\frac{28340511}{21446828}\right)^3.$$

The existence of a Carmichael number shows in a strong way that the obvious converse of the Little Fermat Theorem is false.

Clearing the fractions we get the relation:

$$21446828^3 + 64340484^3 = 63284705^3 + 28340511^3, \quad (7)$$

each side being equal to 276214986237148421555456. We can generate many taxicab numbers in this way, though they tend to be extremely large.[1]

Further remarks.

1. In today's context we could simply do a 'brute force' computer search for taxicab numbers. We would find that the next few such numbers after 1729 are 4104, 20683, 39312, 40033, ... Thus, $4104 = 16^3 + 2^3 = 15^3 + 9^3$, and $20683 = 27^3 + 10^3 = 24^3 + 19^3$. (We have skipped the number $8 \times 1729 = 13832$ in the above list.)

2. It is curious that Hardy described 1729 as "rather dull", as it has many nice properties. One of these is that 1729 is a ***Carmichael number***; indeed, it is the third largest such number. (A number N is called a Carmichael number if it is composite and has the property that a is any integer coprime to N, then $a^{N-1} \equiv 1 \pmod{N}$. The existence of such a number shows in a strong way that the obvious converse of the Little Fermat Theorem is false. The first two Carmichael numbers are 561 and 1105. Curiously, 1105 is the smallest integer expressible in four different ways as a sum of two squares.)

[1] Who knows what Ramanujan might have said if Hardy had announced, "You know, I just traveled in a taxi whose number was 276214986237148421555456?"

Suggested Reading

[1] **Robert Bix, *Conics and Cubics: A Concrete Introduction to Algebraic Curves*, Springer-Verlag, 2006.**

[2] **Joseph H Silverman and John Torrence Tate, *Rational Points on Elliptic Curves*. Springer-Verlag, 1992.**

[3] **Ian Stewart and David Tall, *Algebraic Number Theory and Fermat's Last Theorem*, A K Peters, 2002.**

[4] **C S Yogananda, Fermat's Theorem, a Theorem at Last!, *Resonance*, Vol.1, No.1, pp.71–79, 1996.**

Address for Correspondence
Shailesh A Shirali
Rishi Valley School
Rishi Valley 517 352
Madanapalle, AP, India.
Email:
shailesh.shirali@gmail.com