Taxicabs and Sums of Two Cubes

Joseph H. Silverman*

Our story begins in 1913, when the distinguished British mathematician G. H. Hardy received a bulky envelope from India full of page after page of equations. Every famous mathematician periodically receives letters from cranks who claim to have proven the most wonderous results. Sometimes the proofs, incorrect or incoherent, are included. At other times the writer solicits a reward in return for revealing his discoveries. Now this letter to Hardy, which was from a poor clerk in Madras by the name of Ramanujan, was filled with equations, all given without any sort of proof. Some of the formulas were well-known, mere exercises; while many of the others looked preposterous to Hardy's trained eye.

Who would have blamed Hardy if he had returned this missive to the sender, unread? And in fact, Ramanujan had previously sent his results to two other British mathematicians, each of whom had done just that! But instead Hardy gave some thought to these "wild theorems. Theorems such as he had never seen before, nor imagined." And together, he and J. E. Littlewood, another eminent mathematician with whom Hardy often worked, succeeded in proving some of Ramanujan's amazing identities. At this point Hardy realized that this letter was from a true mathematical genius, and he became determined that Ramanujan should come to England to pursue his mathematical researches. Using travel money provided by Hardy's college, Ramanujan arrived in 1914. Over the next several years he continued to produce and publish highly original material, and he also collaborated with Hardy on a number of outstanding papers.

In 1918, at the age of 30, Ramanujan was elected a Fellow of the Royal Society and also of Trinity College, both signal honors which he richly deserved. Unfortunately, in the colder climate of England he contracted tuberculosis. He returned to his native Madras and died, in 1920, at the age of 33.

During all of Ramanujan's life, he considered numbers to be his personal friends. To illustrate, Hardy tells the story of how one day he visited Ramanujan in the hospital. At a loss for something to say, Hardy remarked that he had arrived at the hospital in taxicab number 1729. "It seemed to me," he continued, "a rather dull number." To which Ramanujan replied "No, Hardy! It is a very interesting number. It is the smallest number expressible as a sum of two cubes in two different ways:"²

$$1729 = 1^3 + 12^3 = 9^3 + 10^3.$$

^{*}This article is an expanded version of talks given at M.I.T. and Brown University

¹[10], page 32

²[10], page 37

Hardy then asked for the smallest number which is a sum of two *fourth* powers in two different ways, but Ramanujan did not happen to know.³

Rather than studying sums of higher powers, we will instead concern ourselves with another question that Hardy could just as easily have asked, namely for the smallest number which is a sum of two cubes in three (or more) distinct ways. In this case the answer is given in [3],

$$87,539,319 = 436^3 + 167^3 = 423^3 + 228^3 = 414^3 + 255^3$$

although if one is willing to allow both positive and negative integers there is the much smaller solution

$$4104 = 16^3 + 2^3 = 15^3 + 9^3 = (-12)^3 + 18^3$$
.

In this note we will be taking a leisurely number-theoretic stroll centered around the problem of writing numbers as sums of two cubes, specifically the search for integers with many such representations. It will be some time before we actually return to this specific question, but along the way we will view some beautiful mathematics which illustrates some of the interplay that can occur between geometry, algebra, and number theory.

We will thus be looking at solutions of the equation

$$X^3 + Y^3 = A.$$

What can be said about such solutions? First we have the elementary result that if A is a non-zero integer, then there are only finitely many solutions in integers X and Y. Of course, if X and Y are restricted to be positive integers, then this is obvious. But in any case we can use the factorization

$$A = X^3 + Y^3 = (X + Y)(X^2 - XY + Y^2)$$

to see that A must factor as A = BC in such a way that

$$B = X + Y$$
 and $C = X^2 - XY + Y^2$

Now there are only finitely many ways of factoring A as A = BC, and for each such factorization we substitute the first equation (i.e. Y = B - X) into the second to obtain

$$X^{2} - X(B - X) + (B - X)^{2} = C.$$

Thus each factorization of A yields at most two values for X, each of which gives one value for Y = B - X. Therefore there are only finitely many integer solutions (X, Y).

[Aside: This proof that the equation $X^3 + Y^3 = A$ has only finitely many solutions in integers depends heavily on the factorization of the polynomial $X^3 + Y^3$. It is similarly true, but quite difficult to prove, that an equation like $X^3 + 2Y^3 = A$ has only finitely many integer solutions. This was first proven by A. Thue in 1909 [11]. By way of contrast, note that the equation $X^2 - 2Y^2 = 1$ has infinitely many solutions.]

 $^{^{3}}$ The answer, $635,318,657 = 59^{4} + 158^{4} = 133^{4} + 134^{4}$, appears to have been discovered by Euler. And it does not seem to be known if there are any numbers which are a sum of two fifth powers in two different ways.

⁴Exercise: Show that any solution in integers satisfies $\max\{|X|, |Y|\} \le 2\sqrt{|A|/3}$.

As is generally the case in mathematics, when a person wants to work on a difficult mathematical problem, it is nearly always best to start with a related easier problem. Then, step by step, one approaches the original goal. In our case we are confronted with the equation

$$X^3 + Y^3 = A,$$

and a natural first question is to ask for the solutions in real numbers. In other words, what does the graph of this curve look like? Since $dY/dX = -(X/Y)^2$, the graph is always falling. Further, it is symmetric about the line Y = X and has the line Y = -X as an asymptote. With this information it is easy to sketch the graph, which is illustrated in Figure 1. We will denote the resulting curve by C.

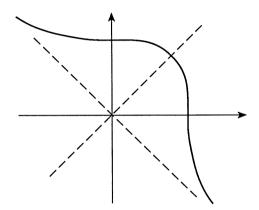


Figure 1. The curve $C: X^3 + Y^3 = A$

If (X, Y) is a point on this curve C, then so is the reflected point (Y, X). But there is another, less obvious, way to produce new points on the curve C which will be very important for the sequel. Thus suppose that $P = (X_1, Y_1)$ and $Q = (X_2, Y_2)$ are two (distinct) points on C, and let C be the line connecting C to C. Then C will (usually) intersect C at exactly one other point. To see this, suppose that C is given by the equation C gives the cubic equation

$$X^3 + (mX + b)^3 = A.$$

By assumption, this equation already has the solutions X_1 and X_2 , since P and Q lie on the intersection $C \cap L$, so the cubic equation has exactly one other solution X_3 . (We run into a problem if m = -1, but we'll deal with that later.) Then letting $Y_3 = mX_3 + b$, we have produced a new point $R = (X_3, Y_3)$ on C. Further, even if P = Q, the same procedure will work provided we take L to be the tangent line to C at P. Thus given any two points P and Q on C, we have produced a third point R. Finally we define an "addition law" on C by setting

$$P + Q =$$
(reflection of R about the line $Y = X$).

In other words, if $R = (X_3, Y_3)$, then $P + Q = (Y_3, X_3)$. (See Figure 2.) The reason we define P + Q with this reflection will soon become clear, but first we have to deal with the pesky problem that sometimes our procedure fails to yield a third point.

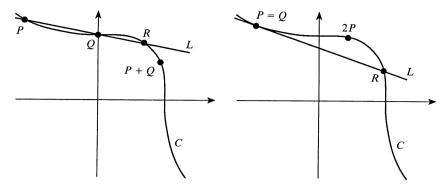


Figure 2. The addition law on the curve $C: X^3 + Y^3 = A$

This problem arises whenever the line connecting P and Q has slope -1, and thus is parallel to the asymptote Y = -X. We solve the problem in cavalier fashion; since there is no actual third intersection point we create one by fiat. To be precise, we take the XY-plane and add an extra point, which we will denote by \mathcal{O} . This point has the property that the lines going through \mathcal{O} are exactly the lines with slope -1. Further, if P is a point in the XY-plane, then the unique line through P and \mathcal{O} is the line through P having slope -1. Having done this, we are now in the happy position of being able to assert that given any two points P and Q on C, the above procedure will yield a unique third point R on C, so we are able to define P + Q for any P and Q. (By definition, we set $\mathcal{O} + \mathcal{O} = \mathcal{O}$.)

[Aside. Some readers will doubtless recognize that what we have done is start the construction of the real projective plane. The projective plane consists of the usual XY-plane together with one point for each direction. In our case, we only needed the direction with slope -1. The projective plane has the agreeable property that any two lines, even "parallel" ones, intersect at exactly one point. This is true because if two lines are parallel, then they intersect at the point corresponding to their common direction.]

The justification for our use of the symbol "+" is now this:

The addition law P + Q described above makes the points of C into an abelian group.

To be more precise, if P = (X, Y) is a point on C, we define its inverse to be its reflection, -P = (Y, X). Then for all points P, Q, R on C we have

$$P + \mathcal{O} = \mathcal{O} + P = P$$
 (identity)
 $P + (-P) = \mathcal{O}$ (inverse)
 $P + Q = Q + P$ (commutativity)
 $(P + Q) + R = P + (Q + R)$ (associativity).

All of these properties are quite easy to check except for the associativity, which we will return to in a moment.

Note that the addition procedure outlined above is entirely mechanical. We can write down explicit formulas for the sum of two points, although there are a number of special cases. For example, if P = (X, Y), then

$$P + P = 2P = \left(\frac{Y(X^3 + A)}{Y^3 - X^3}, \frac{X(Y^3 + A)}{X^3 - Y^3}\right).$$

The formula for the sum of two distinct points $P_1 = (X_1, Y_1)$ and $P_2 = (X_2, Y_2)$ is somewhat more complicated:

$$P_1 + P_2$$

$$=\left(\frac{A(Y_1-Y_2)-X_1X_2(Y_1X_2-Y_2X_1)}{X_1X_2(X_1-X_2)+Y_1Y_2(Y_1-Y_2)},\frac{A(X_1-X_2)-Y_1Y_2(X_1Y_2-X_2Y_1)}{X_1X_2(X_1-X_2)+Y_1Y_2(Y_1-Y_2)}\right).$$

And now that we are in possession of these formulas, verification of the associative law is a tedious, but straightforward, task.

Let us now look at an example, and what better choice than Ramanujan's equation

$$X^3 + Y^3 = 1729.$$

We already know two interesting points on this curve, namely

$$P = (1, 12)$$
 and $Q = (9, 10)$.

Using the addition law, we can easily compute some more points, such as

$$P + Q = \left(\frac{46}{3}, \frac{-37}{3}\right), \qquad P - Q = \left(\frac{453}{56}, \frac{-397}{56}\right), \qquad 2P = \left(\frac{20760}{1727}, \frac{-3457}{1727}\right),$$

$$2Q = \left(\frac{24580}{271}, \frac{-24561}{271}\right), \qquad 3P = \left(\frac{-5150812031}{107557668}, \frac{5177701439}{107557668}\right).$$

As the discerning reader will notice, the numbers produced seem to grow with frightening rapidity. But of far more importance is the fact that although we have not produced any new integer solutions, all of the new solutions are at least in rational numbers.

This is a consequence of the fact that the addition law on C is given by rational functions. That is, the coordinates of P+Q are given by quotients of polynomials in the coordinates of P and Q. Thus if the coordinates of P and Q are rational numbers, then so are the coordinates of P+Q. (If this is not clear, look for example at the formula for P given above. If P are all rational numbers, then the formula shows that the coordinates of P are also rational.) Let us define

$$C(\mathbb{Q}) = \{(X,Y): X \text{ and } Y \text{ are rational numbers and } X^3 + Y^3 = A\} \cup \{\mathscr{O}\}.$$

Here \mathbb{Q} is the usual symbol for the field of rational numbers. Then the remarks given above provide a proof of the following fact, first noted by Poincaré around 1900 [6]:

The set $C(\mathbb{Q})$ is a subgroup of C. In other words, $C(\mathbb{Q})$ supplied with the addition law from C becomes a group in its own right.

The sum of two cubes "Hall of Fame"

The following material gives the smallest integer I know with the indicated property. It has been collected from various sources, including [3] and [12]. Note that we are counting $X^3 + Y^3$ and $Y^3 + X^3$ as being the same representation.

Positive integers, 2 representations, cube-free

$$1729 = 1^3 + 12^3 = 9^3 + 10^3 = 7 \cdot 13 \cdot 19$$

Any integers, 3 representations, not cube-free

$$4104 = 16^3 + 2^3 = 15^3 + 9^3 = (-12)^3 + 18^3 = 2^3 \cdot 3^3 \cdot 19$$

Any integers, 3 representations, cube-free

$$3,242,197 = 141^3 + 76^3 = 138^3 + 85^3 = (-171)^3 + 202^3 = 7 \cdot 31 \cdot 67 \cdot 223$$

Positive integers, 3 representations, not cube-free

$$87,539,319 = 436^3 + 167^3 = 423^3 + 228^3 = 414^3 + 255^3$$

= $3^3 \cdot 7 \cdot 31 \cdot 67 \cdot 223$

Positive integers, 3 representations, cube-free

$$15,170,835,645 = 517^3 + 2468^3 = 709^3 + 2456^3 = 1733^3 + 2152^3$$
$$= 3^2 \cdot 5 \cdot 7 \cdot 31 \cdot 37 \cdot 199 \cdot 211$$

Any integers, 4 representations, not cube-free

$$42,549,416 = 348^{3} + 74^{3} = 282^{3} + 272^{3}$$

$$= (-2662)^{3} + 2664^{3} = (-475)^{3} + 531^{3}$$

$$= 2^{3} \cdot 7 \cdot 13 \cdot 211 \cdot 277$$

Positive integers, 4 representations, not cube-free

$$26,059,452,841,000 = 29620^{3} + 4170^{3} = 28810^{3} + 12900^{3}$$
$$= 28423^{3} + 14577^{3} = 24940^{3} + 21930^{3}$$
$$= 2^{3} \cdot 5^{3} \cdot 31 \cdot 43^{3} \cdot 97 \cdot 109$$

Any integers, 4 representations, cube-free

Unknown

Any integers, 5 representations, not cube-free

$$1,148,834,232 = 1044^{3} + 222^{3} = 920^{3} + 718^{3}$$

$$= 846^{3} + 816^{3} = (-7986)^{3} + 7992^{3} = (-1425)^{3} + 1593^{3}$$

$$= 2^{3} \cdot 3^{3} \cdot 7 \cdot 13 \cdot 211 \cdot 277$$

We have come a long way in our study of the solutions of the equation $X^3 + Y^3 = A$. What we have found is that the set of solutions in rational numbers becomes, in a very natural way, an abelian group. So if we can say something significant about this group, then we might feel that at last we have some understanding about this set of rational solutions. An answer to this problem is provided by one of the most celebrated theorems of the twentieth century. Aside from its intrinsic interest, this result has been the starting point for much of the study of Diophantine equations over the past 70 years. The theorem, as we state it, was first proven by L. J. Mordell in 1922 [5]. It was subsequently vastly generalized

by A. Weil in his 1928 thesis, and so is usually called the Mordell-Weil Theorem:

There exists a finite set of points P_1, \ldots, P_r in $C(\mathbb{Q})$ so that every point in $C(\mathbb{Q})$ can be obtained from P_1, \ldots, P_r by addition and subtraction. In fancier language, the group $C(\mathbb{Q})$ is finitely generated. The points P_1, \ldots, P_r are called generators for $C(\mathbb{Q})$.

This seems fairly satisfactory. Even though our equation may have infinitely many rational solutions, they can all be obtained by starting with some finite subset and applying a completely mechanical procedure. For example, on the curve

$$X^3 + Y^3 = 7.$$

every rational point is a multiple of the single generating point (2, -1). Similarly, it is probably true that every rational point on Ramanujan's curve has the form nP + mQ, where P = (1, 12), Q = (9, 10), and n and m are allowed to range over all integers, although I am not aware that anyone has verified this probable fact.

It may come as a surprise, then, to learn that the Mordell-Weil Theorem is far less satisfactory than it appears. This is due to the fact that it is not *effective*. What this means is that currently we do not have an algorithm which will determine, for every value of A, a set of generators P_1, \ldots, P_r for $C(\mathbb{Q})$. In fact, there is not even a procedure for determining exactly how many generators are needed, although it is possible to give a rather coarse upper bound. This problem of making the Mordell-Weil Theorem effective is one of the major outstanding problems in the subject.

Another open problem concerns the number of generators needed. As mentioned above, the curve $X^3 + Y^3 = 7$ requires only one generator, while Ramanujan's curve $X^3 + Y^3 = 1729$ needs at least two. The question is whether there are curves which require a large number of generators. More precisely, is it true that for every integer r there is some value of A so that the rational points on the curve $X^3 + Y^3 = A$ require at least r generators?

We now return to our original problem, namely the study of *integer* solutions to the equation $X^3 + Y^3 = A$. Specifically, we seek values of A for which this equation has many solutions. We have observed that the equation

$$X^3 + Y^3 = 7$$

has the solution P = (2, -1), and by taking multiples of P we can produce a sequence of points

$$P = (2, -1), \quad 2P = \left(\frac{5}{3}, \frac{4}{3}\right), \quad 3P = \left(\frac{-17}{38}, \frac{73}{38}\right), \quad 4P = \left(\frac{-1256}{183}, \frac{1265}{183}\right), \dots$$

Further, it is true (but moderately difficult to prove) that this sequence of points $P, 2P, 3P, \ldots$ never repeats. Each point in the sequence has rational coordinates, so we can write nP in the form

$$nP = \overbrace{P + P + \cdots + P}^{n\text{-terms}} = \left(\frac{a_n}{d_n}, \frac{b_n}{d_n}\right),$$

where a_n , b_n , and d_n are integers. We are going to take the first N of these rational solutions and multiply our original equation by a large integer so as to clear the denominators of all of them. Thus let

$$B = d_1 d_2 \cdots d_N$$

Then the equation

$$X^3 + Y^3 = 7B^3$$

has at least N solutions in integers, namely

$$\left(\frac{a_n B}{d_n}, \frac{b_n B}{d_n}\right), \quad 1 \le n \le N.$$

(Actually 2N solutions, since we can always switch X and Y, but for simplicity we will generally count pairs of solutions (X, Y) and (Y, X).) We have thus found the following answer to our original problem:

Given any integer N, there exists a positive integer A for which the equation $X^3 + Y^3 = A$ has at least N solutions in integers.

Of course, Ramanujan and Hardy were probably talking about solutions in positive integers; but with a bit more work one can show that infinitely many of the points $P, 2P, 3P, \ldots$ have positive coordinates, so we even get positive solutions.

Naturally, it is of some interest to make this result quantitative, that is, to describe how large A must be for a given value of N. The following estimate is essentially due to K. Mahler [4], with the improved exponent appearing in [8]:

There is a constant c > 0 such that for infinitely many positive integers A, the number of positive integer solutions to the equation $X^3 + Y^3 = A$ exceeds $c\sqrt[3]{\log A}$.

In some sense we have now answered our original question. There are indeed integers which are expressible as a sum of two cubes in many different ways. But a nagging disquiet remains. We have not really produced a large number of intrinsically integral solutions. Rather, we have cleared the denominators from a lot of rational solutions. In the solutions produced above, the X and Y coordinates will generally have a large common factor whose cube will divide A. What happens if we rule out this situation? The simplest way to do so is to restrict attention to integers A that are *cube-free*; that is, A should not be divisible by the cube of any integer greater than 1. This is a reasonable restriction since if D^3 divides A, then an integer solution (X,Y) to $X^3 + Y^3 = A$ really arises from the rational solution (X/D,Y/D) to the "smaller" equation $X^3 + Y^3 = A/D^3$.

Notice Ramanujan's example

$$1729 = 1^3 + 12^3 = 9^3 + 10^3 = 7 \cdot 13 \cdot 19$$

is cube-free. But the example with three representations given earlier,

$$87.539.319 = 436^3 + 167^3 = 423^3 + 228^3 = 414^3 + 255^3 = 3^3 \cdot 7 \cdot 31 \cdot 67 \cdot 223$$

is not cube-free. As far as I have been able to determine, the smallest cube-free integer which can be expressed as a sum of two positive cubes in three distinct ways was unearthed by P. Vojta in 1983 [12]:

$$15,170,835,645 = 517^3 + 2468^3 = 709^3 + 2456^3 = 1733^3 + 2152^3$$
$$= 3^2 \cdot 5 \cdot 7 \cdot 31 \cdot 37 \cdot 199 \cdot 211.$$

And now our problem has become so difficult that Vojta's number holds the current record! There is no cube-free number known today which can be written as a sum of two positive cubes in four or more distinct ways.

We are going to conclude by describing a relationship between the two problems that we have been studying. The first problem was that of expressing a number as a sum of two *rational cubes*, and in that case we saw that all solutions arise from a finite generating set and speculated as to how large this generating set might be. The second problem was that of writing a cube-free number as a sum of two *integral cubes*, and here we saw that there are only finitely many solutions and we wondered how many solutions there could be. It is not a priori clear that these two problems are related, beyond the obvious fact that an integral solution is also a rational solution. In 1974 V. A. Dem'janenko stated that if there are a large number of integer solutions, then any generating set for the group of rational points must also be large, but his proof was incomplete. (See [2, page 140] for Lang's commentary on and generalization of Dem'janenko's conjecture.) The following more precise version of the conjecture was proven in 1982 [8]:

For each integer A, let N(A) be the number of solutions in integers to the equation $X^3 + Y^3 = A$, and let r(A) be the minimal number of rational points on this curve needed to generate the complete group of rational points (as in the Mordell-Weil Theorem). There is a constant c > 1 such that for every cube-free integer A,

$$N(A) \le c^{r(A)}.$$

Note that the requirement that A be cube-free is essential. For as we saw above, we can make $N(7B^3)$ as large as we want by choosing an appropriate value of B. On the other hand, $r(7B^3) = r(7)$ for every value of B, so an inequality of the form $N(A) \le c^{r(A)}$ cannot be true if we allow arbitrary values of A. (To see that $r(7B^3) = r(7)$, note that the groups of rational points on the curves $X^3 + Y^3 = 7$ and $X^3 + Y^3 = 7B^3$ are the same via the map $(X, Y) \to (BX, BY)$.)

Final Remark. The cubic curve $X^3 + Y^3 = A$ is an example of what is called an elliptic curve. Those readers interested in learning more about the geometry, algebra, and number theory of elliptic curves might begin with [9] and continue with the references listed there. Elliptic curves and the related theory of elliptic functions appear frequently in areas as diverse as number theory, physics, computer science, and cryptography.

ACKNOWLEDGMENTS. I would like to thank Jeff Achter and Greg Call for their helpful suggestions.

REFERENCES

- 1. Dem'janenko, V. A.: On Tate height and the representation of a number by binary forms, *Math. USSR Isv.* 8, 463-476 (1974).
- 2. Lang, S.: Elliptic Curves: Diophantine Analysis. Berlin: Springer-Verlag, 1978
- 3. Leech, J.: Some solutions of Diophantine equations. Proc. Camb. Philos. Soc. 53, 778-780 (1957).
- 4. Mahler, K.: On the lattice points on curves of genus 1. Proc. London Math. Soc. 39, 431-466 (1935).
- 5. Mordell, L. J.: On the rational solutions of the indeterminate equation of the third and fourth degree. *Proc. Camb. Math. Soc.* 21, 431-466 (1922).
- Poincaré, H.: Sur les propriétés arithmétiques des courbes algébriques. J. de Liouville 7, 161–233 (1901).
- Silverman, J. H.: Integer points and the rank of Thue elliptic curves. *Invent. Math.* 66, 395–404 (1982).
- 8. Silverman, J. H.: Integer points on curves of genus 1. J. London Math. Soc. 28, 1-7 (1983).

- 9. Silverman, J. H., Tate, J.: Rational Points on Elliptic Curves. New York: Springer-Verlag, 1992.
- 10. Snow, C. P., Foreword to: *A Mathematician's Apology*. by G. H. Hardy (1940), Cambridge: Cambridge University Press, 1967.
- 11. Thue, A.: Über Annäherungswerte algebraischer Zahlen. J. reine ang. Math. 135, 284-305 (1909).
- 12. Voita, P.: private communication, 1983.

Added in proof: Richard Guy has pointed out to the author that Rosenstiel, Dardis and Rosenstiel have recently found the non-cube-free example

$$6963472309248 = 2421^3 + 19083^3 = 5436^3 + 18948^3 + 10200^3 + 18072^3$$
$$= 13322^3 + 16630^3$$

which is smaller than the example in the above table, and which is in fact the smallest such example. See *Bull. Inst. Math. Appl.* 27(1991), 155–157.

Mathematics Department Brown University Providence, RI 02912 USA jhs@gauss.math.brown.edu

Five Borromean Square Frames

William W. Chernoff

In [R. Brown and J. Robinson, Borromean circles, *Amer. Math. Monthly*, 99 (1992), 376–377], R. Brown and J. Robinson gave a Borromean arrangement of three square frames in \mathbb{R}^3 . In figure 1, we give a Borromean arrangement consisting of five square frames. In addition, we have constructed models consisting of seven hexagonal frames and of nine octagonal frames. A paper discussing Borromean arrangements in \mathbb{R}^3 of 2n+1 frames each with 2n sides is to appear.

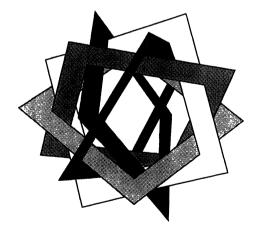


Fig. 1

Department of Mathematics and Statistics University of New Brunswick Frederiction, N.B. Canada E3B 5A3