# *Magic Squares, Finite Planes, and Points of Inflection on Elliptic Curves*

*Ezra Brown*

**Ezra (Bud) Brown** (brown@math.vt.edu) has degrees from Rice and Louisiana State, and has been at Virginia Tech since the first Nixon Administration. His research interests include graph theory, the combinatorics of finite sets, and number theory—especially elliptic curves. In 1999, he received the MAA MD-DC-VA Section Award for Outstanding Teaching, and he loves to talk about mathematics and its history to anyone, especially students.

## Many Threads

While leafing through a book [**5**] on elliptic curves—one of my favorite subjects—I came across a little gem of a result that ties many mathematical threads together, threads that originate in several different areas of mathematics. The result is that every elliptic curve has nine points of inflection which can be arranged, in a very natural way, to form a $3 \times 3$ magic square.

We are going to follow these threads. We'll learn a little about magic squares and finite planes, what elliptic curves are and how to add points on them, what points of inflection are, and finally how all of these threads tie together.

## Magic Squares and Finite Planes

To the ancient Greeks, arithmetic and geometry were as separate as, say, astronomy and music. In fact, to the Pythagoreans, these four were the subjects of study—or **mathemata**, whence the name of our fair discipline—on which their pupils were to concentrate [**2**, p. 88]. In the *Republic*, Plato described them as essential to the education of a citizen of the Republic [**3**, pp. 64–70]. This four–fold division became known in the Middle Ages as the quadrivium, and even in our own times, arithmetic and geometry may appear to be separate subjects. Sooner or later, however, mathematicians discover that they are not separate, and that there is some truly beautiful mathematics where they meet.

My first encounter at the place where arithmetic meets geometry was undoubtedly the $3 \times 3$ *magic square*, an arrangement of the numbers 1 through 9 in a $3 \times 3$ square grid so that the numbers in each line of three—that is, each row, each column and the two main diagonals—add up to 15, as

| | | |
|---|---|---|
| 8 | 1 | 6 |
| 3 | 5 | 7 |
| 4 | 9 | 2 |

This magic square is full of surprises, including the fact (see [**1**]) that

$$816^2 + 357^2 + 492^2 = 618^2 + 753^2 + 294^2.$$

(See [**4**] for many more magic square musings.)

 

However, what interests us here is that the $3 \times 3$ magic square is an example of a *nine–point plane*. For, by viewing rows, columns and diagonals as sets of points, and by allowing diagonals to "wrap" when they reach the edge of the grid, we find, not just eight lines of three numbers each, but twelve—namely:

| | |
|---|---|
| three rows: | $\{1, 6, 8\}, \{2, 4, 9\}, \{3, 5, 7\}$ |
| three columns: | $\{1, 5, 9\}, \{2, 6, 7\}, \{3, 4, 8\}$ |
| three main diagonals: | $\{1, 4, 7\}, \{2, 5, 8\}, \{3, 6, 9\}$ |
| three off diagonals: | $\{1, 2, 3\}, \{4, 5, 6\}, \{7, 8, 9\}$ |

By a *line*, we mean a set of points—not necessarily connected, straight, or infinite. For example, $\{1, 6, 8\}$ is a line. This nine–point plane follows some fairly simple rules:

**(1)** Each pair of points lies on a unique line.

**(2)** Each pair of lines intersects in at most one point.

**(3)** Each point lies on the same number $r$ of lines—in this case, $r = 4$.

**(4)** Each line contains the same number $k$ of points—in this case, $k = 3$.

**(5)** There exist four points with no three on a line.

The first two rules are reminiscent of Euclidean plane geometry. Rules **(3)** and **(4)** guarantee a certain regularity: that is, all points and lines have equal status. Rule **(5)** states that the object at hand is nontrivial. Arrangements that satisfy **(1–5)** are called *finite planes*—whence the name "nine–point plane."

Now, in order to understand how the $3 \times 3$ magic square (the nine–point plane) relates to elliptic curves, we need to talk about how to add points on an elliptic curve. You may not know what an elliptic curve is, so let's find out about them.

## Adding Points on Elliptic Curves

For our purposes, an **elliptic curve** is the set of all solutions to the equation

$$y^2 = x^3 + px + q,$$

where $x$ and $y$ are complex numbers and the cubic polynomial $x^3 + px + q$ has no repeated roots. Thus, $y^2 = x^3 + 2$ and $y^2 = x^3 - 2x$ are elliptic curves, since $x^3 + 2$ has one real and two complex conjugate roots, and the roots of $x^3 - 2x$ are 0 and $\pm\sqrt{2}$. On the other hand, $y^2 = x^3 + x^2$ and $y^2 = x^3$ are not, since 0 is a double root of $x^3 + x^2$ and a triple root of $x^3$.

Partly due to their connection with Fermat's Last Theorem (see [**7**]), elliptic curves have recently become popular objects of study. Many mathematicians had a hand in showing that the construction (called the **chord–and–tangent method**) can be used to add points on an elliptic curve, and that this addition turns the set of points on such a curve into a group.

Here's how it works. Suppose $P$ and $Q$ are points on the elliptic curve $E$. Join $P$ and $Q$ by the line $l$. Now $l$ meets $E$ in a third point we'll call $P * Q$. The sum $P + Q$ is defined to be the reflection of $P * Q$ in the $x$-axis, not $P * Q$ itself.

Let's look at this algebraically. If $P = (x_1, y_1)$ and $Q = (x_2, y_2)$, then the line $l$ has an equation of the form $y = mx + b$; solving the simultaneous equations $y = mx + b$

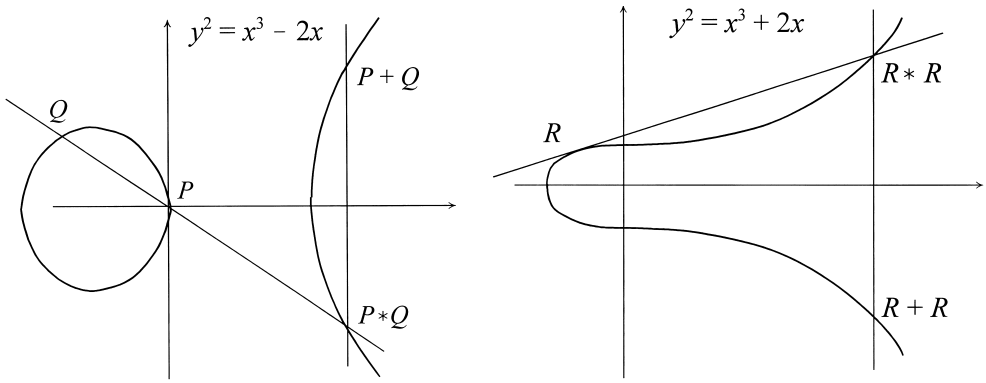


**Figure 1.** Chord and Tangent Addition

and $y^2 = x^3 + px + q$ leads to the one–variable equation

$$x^3 - m^2x^2 + (p - 2mb)x + q - b^2 = 0. \tag{1}$$

This cubic polynomial has three roots, namely $x_1$, $x_2$, and the $x$-coordinate $x_3$ of $P * Q = (x_3, y_3)$. Reflecting $P * Q$ in the $x$-axis gives us $P + Q = (x_3, -y_3)$.

For example, let $E_1$ be the curve $y^2 = x^3 - 2x$ (on the left in Figure 1), $P = (0, 0)$ and $Q = (-1, 1)$. Then $l$ is the line $y = -x$ and (1) becomes $x^3 - x^2 - 2x = 0$, whose roots are 0, $-1$ and 2. Then $P * Q = (2, -2)$ and so $P + Q = (2, 2)$.

Let $E_2$ be the curve $y^2 = x^3 + 2$ (on the right in Figure 1); let us add $R = (-1, 1)$ to itself. Then $l$ is the line $y = (3x + 5)/2$ tangent to $E_2$ at $R$ and (1) becomes $(x + 1)^2(x - (17/4)) = 0$, whose roots are $-1$ (a double root) and $17/4$. Then $R * R = (17/4, 71/8)$, and so $R + R = (17/4, -71/8)$.

If $P$ and $Q$ have rational coordinates, so do $P + Q$ and $P * Q$, because

$$x^3 - m^2x^2 + (p - 2mb)x + q - b^2 = (x - x_1)(x - x_2)(x - x_3). \tag{2}$$

Since $m^2 = x_1 + x_2 + x_3$ and since $m$, $x_1$ and $x_2$ are rational, so is $x_3$. Finally, $b = y_1 - mx_1$ is rational and so $y_3 = mx_3 + b$ is also rational. This always works because each line in the plane meets an elliptic curve in three points, **provided you count correctly**. "Counting correctly" means three things:

- We allow complex coordinates. Thus, you can verify that $y = 2$ meets $E_1$ in the three points $(2, 2)$, $(-1 + i, 2)$ and $(-1 - i, 2)$. Note that in Figure 1, what you see are just the points on the curves with both coordinates real—if we include complex points, then we would have a four–dimensional graph!
- We count multiplicities correctly. Thus, $y = (3x + 5)/2$ meets $E_2$ doubly at $R = (-1, 1)$—since $-1$ is a double root of $(x + 1)^2(x - (17/4))$—and singly at $(17/4, 71/8)$.

As for the line $x = 2$, there *is* a third point. Look at it this way: the line through $P + Q = (2, 2)$ and $S = (1.999, -1.9975\ldots)$ has equation $y = 3997.5x - 7993$, which is almost vertical. It turns out that

$$(P + Q) * S = (15980002.25\ldots, 63880049500.313\ldots).$$

 

This third point is very far from $P + Q$ and $S$, but it is on the curve. Moving $S$ closer to $(2, -2)$ moves $(P + Q) * S$ farther away; passing to the limit, if $S = (2, -2) = P * Q$, then $(P + Q) * S$ is "infinitely far away." This last point does not have finite coordinates. We call it the **point at infinity**, label it **O**, and include it as a point on every elliptic curve. The third rule for counting correctly is:

- We count the point at infinity, if necessary. Thus, $x = 2$ meets $E_1$ in $(2, 2)$, $(2, -2)$ and **O**; $x = 0$ meets $E_1$ doubly at $(0, 0)$ and singly at **O**; and $x = 1$ meets $E_1$ at $(1, i)$, $(1, -i)$ and **O**.

Note that if $P$ is a point, then the line through $P$ and the reflection of $P$ in the $x$-axis passes through **O**. Using this, we may now tell how to add points on an elliptic curve so as to include the counting rules and the point at infinity. Suppose $P$ and $Q$ are points on the elliptic curve $E$. To find $P + Q$, draw the line $l$ through $P$ and $Q$; if $P = Q$, then $l$ is the tangent line to $E$ at $P$. Locate $P * Q$, the third point at which $l$ meets $E$—counting correctly. Draw $l'$, the line through **O** and $P * Q$; $P + Q$ is the third point at which $l'$ meets $E$.

As with addition of numbers, we write $2P$ for $P + P$, $3P$ for $P + P + P$, etc.

We can do this algebraically, too. If $E : y^2 = x^3 + px + q$ is an elliptic curve, then we can express the sum $P_1 + P_2$ of points $P_1$ and $P_2$ on $E$ by means of the following formulas. Let $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2)$ and $P_1 + P_2 = (x_3, y_3)$.

If $x_1 = x_2$ and either $y_1 \neq y_2$ or $y_1 = y_2 = 0$, then $P_1 + P_2 = \mathbf{O}$, and we say that $P_2 = -P_1$.

Otherwise, the slope $m$ of the line $l$ through $P_1$ and $P_2$ is given by

$$m = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1}, & \text{if } x_1 \neq x_2; \\ \dfrac{3x_1^2 + p}{2y_1}, & \text{if } x_1 = x_2. \end{cases} \tag{3}$$

Finally, it follows from the discussion following (2), the fact that $P_1 * P_2 = (x_3, -y_3)$, and a little algebra, that

$$\begin{aligned} x_3 &= m^2 - x_1 - x_2, \\ y_3 &= -(y_1 + m(x_3 - x_1)). \end{aligned} \tag{4}$$

For example, if $E$ has equation $y^2 = x^3 - x + 4$, $P_1 = (0, 2)$ and $P_2 = (-1, -2)$, then you can check that $(0, 2) + (-1, -2) = (17, -70)$. Sure enough, $(-70)^2 = 4900 = 17^3 - 17 + 4$, so $(17, -70)$ is on $E$. To test these formulas, note that the point $(15, 58)$ is also on this curve. Find $(17, -70) + (15, 58)$ for yourself; surprised?

We will use these formulas from here on out. And now, on to points of inflection.

## Tangent Lines and Points Of Inflection

How many points of inflection does an elliptic curve have?

In order to answer this, let's first agree on what we mean by a tangent line and a point of inflection (PI). In calculus, when you meet the derivative, you also meet the notions of tangent line, local extrema, concavity, and points of inflection. You learn that the line tangent to a differentiable function $f$ at $P = (x_0, f(x_0))$ is the line through $P$ with slope $y' = f'(x_0)$. One calculus book [**6**, pp. 210–211] states that the graph of

a differentiable function $y = f(x)$ is concave up (respectively, down) on an interval where $y'$ is increasing (respectively, decreasing). A point of inflection is a point at which the graph of $y = f(x)$ has a tangent line and where the concavity changes. So, if $f$ is twice–differentiable, then $f$ has a PI where $y''$ changes sign.

A point of inflection on an elliptic curve is, similarly, a point $(x, y)$ on the curve where $y''$ is defined and changes sign. If we try to understand this in terms of "change in "concavity" (as we do in calculus) then we might think that each of the elliptic curves in Figure 1 has two PI's. But looks can be deceptive.

Let's find out by calculating $y''$, where $y^2 = x^3 + px + q$. We write $g(x) = x^3 + px + q$ and differentiate both sides of the equality $y^2 = g(x)$ twice; a bit of algebra shows that

$$y'' = \frac{2g(x)g''(x) - (g'(x))^2}{8yg(x)} = \frac{3x^4 + 6px^2 + 12qx - p^2}{8yg(x)}.$$

whose numerator is equal to $3x^4 + 6px^2 + 12qx - p^2$. Hence, if $P(x_0, y_0)$ is a PI of the elliptic curve $y^2 = x^3 + px + q$, then $x_0$ is a zero of the fourth–degree polynomial $I(x) = 3x^4 + 6px^2 + 12qx - p^2$.

Now, we're counting complex points when invoking the rule that a line and an elliptic curve meet in three points, so we want to include them when looking for points of inflection. A fourth–degree polynomial has four complex zeros, $x_i$ for $1 \le i \le 4$, and to each there corresponds two points on the curve, $(x_i, \sqrt{g(x_i)})$ and $(x_i, -\sqrt{g(x_i)})$. Hence, it follows that the curve has, not just two points of inflection, but at least eight!

The graphs in Figure 1 reveal only two PIs, but don't panic: for the other six PIs, at least one of the coordinates is nonreal, so you don't see all eight.

Well, nine, actually. Remember, we claimed that an elliptic curve has nine PIs. So, in order to show this, first we must show that the four zeros of $I(x)$ are distinct. Then, we have to show that for none of the zeros $x_i$ is $g(x_i) = 0$. Finally, we somehow have to produce another PI.

Fortunately, we can do this. Let's begin with the key lemma.

**Key Lemma.** If $E : y^2 = g(x) = x^3 + px + q$, and $I(x) = 3x^4 + 6px^2 + 12qx - p^2$, then $I(x)$ has four distinct zeros, none of which are zeros of $g(x)$.

*Proof.* Now $I(x)$ is a polynomial with real coefficients. Hence, $I(x)$ has distinct zeros if and only if it has no nonconstant factors in common with its derivative $I'(x)$. We have already found that $I(x) = 2g(x)g''(x) - (g'(x))^2$, and so

$$I'(x) = 2g(x)g'''(x) + 2g'(x)g''(x) - 2g'(x)g''(x) = 2g(x)g'''(x) = 12g(x),$$

since $g'''(x) = 6$.

Next, it is clear that any nonconstant divisor of $I'(x)$ is a nonconstant divisor of $g(x)$, so that any such divisor of $I(x)$ also divides the difference $I(x) - 2g(x)g''(x) = (g'(x))^2$. So, any such divisor is a nonconstant common factor of both $g(x)$ and $g'(x)$. But we're in luck: since $y^2 = g(x)$ is an elliptic curve, $g(x)$ is guaranteed to have distinct zeros, and so it has no nonconstant factors in common with $g'(x)$.

We conclude that $I(x)$ and $I'(x)$ have no common factors, and so the fourth–degree polynomial $I(x)$ has four distinct zeros.

This shows that $g(x)$ and $I(x)$ have no nonconstant common factors—hence, no common zeros. Thus, no zero of $I(x)$ is a zero of $g(x)$, and so we have indeed found

 

eight PIs of the curve $y^2 = g(x)$: namely, $(x_i, \pm\sqrt{g(x_i)})$, where $x_i$ is one of the four zeros of $I(x)$.

For our curve $E_2 : y^2 = x^3 + 2$, it happens that $I(x) = 3x^4 + 24x = 3x(x^3 + 8)$ has the four zeros 0, $-2$, $-2\omega$ and $-2\omega^2$, where $\omega = \frac{-1+i\sqrt{3}}{2}$. We do a little algebra and find that the eight known points of inflection are

$$(0, \pm\sqrt{2}), \quad (-2, \pm i\sqrt{6}), \quad (-2\omega, \pm i\sqrt{6}), \quad (-2\omega^2, \pm i\sqrt{6}).$$

Well, where's the ninth PI?

It's **O**, the point at infinity! But in order to show this, we're going to have to look at tangents and PIs slightly differently. What works is to notice that if the line $y = mx + b$ is tangent to the curve $y = f(x)$ at $(u, v)$, then the equation $mx + b = f(x)$ has a double root at $x = u$. For example, the tangent line to $y = x^3 - 2x + 5$ at $(2, 9)$ has equation $y = 10x - 11$, and we see that

$$x^3 - 2x + 5 - (10x - 11) = x^3 - 12x + 16 = (x - 2)(x - 2)(x + 4).$$

Thus, $x = 2$ is a double root of $f(x) - (mx + b) = 0$, since $(x - 2)^2$ is a factor of $f(x) - (mx + b)$.

What about PIs? Just this: if $(u, v)$ is a PI of the curve $y = f(x)$, then the equation $mx + b - f(x) = 0$ has a triple root at $x = u$. Continuing our example, $P = (0, 5)$ is a PI for $y = x^3 - 2x + 5$, since the tangent line at $P$ has equation $y = -2x + 5$, $f(x) - (mx + b) = x^3$, and so $f(x) - (mx + b) = 0$ has a triple root at $x = 0$.

For elliptic curves, we adopt this broader view of tangents and PIs. Let $l$ be a line that meets the curve **C** at a point $P$. We'll say that $l$ is a tangent line to **C** at $P$ if $l$ and **C** intersect doubly at $P$. That is, if $l$ has equation $y = mx + b$ and **C** has equation $F(x, y) = 0$, then $l$ is a tangent line at $P = (x_0, y_0)$ provided the equation $F(x, mx + b) = 0$ has a double root at $x_0$. Similarly, we'll say that $P$ is a point of inflection of the curve **C** if $l$ and **C** intersect triply at $P$—that is, if the equation $F(x, mx + b) = 0$ has a triple root at $P$.

Under this definition, we can now show that **O** is the ninth PI on an elliptic curve.

## The Magic Square Theorem

First, we need another lemma.

**Lemma on Points of Inflection.** Let $P = (x, y)$ be a finite point on the elliptic curve $y^2 = g(x)$—that is, $P \neq \mathbf{O}$. Then $P$ is a point of inflection if and only if $3P = \mathbf{O}$.

*Proof.* As we saw in the previous section, $(x, y)$ is a PI of $y^2 = g(x)$ precisely when $(g'(x))^2 = 2g(x)g''(x)$. Now it just so happens that the doubling formulas from (3) and (4) also involve $(g'(x))^2$. For, if we let $x_1 = x_2 = x$, $y_1 = y$, and $2P = (x_3, y_3)$, then from (3) we have that

$$m = \frac{3x^2 + p}{2y} = \frac{g'(x)}{2y},$$

and from (4) we have that

$$x_3 = m^2 - 2x = \left(\frac{g'(x)}{2y}\right)^2 - 2x = \frac{(g'(x))^2 - 8xy^2}{4y^2} = \frac{(g'(x))^2 - 8xg(x)}{4g(x)}.$$

Hence, $x_3 = x$ if and only if $x \cdot 4g(x) = (g'(x))^2 - 8xg(x)$, i.e., just when $(g'(x))^2 = 12xg(x)$. But $g''(x) = 6x$, so the $x$-coordinates of $P$ and $2P$ are the same just when $(g'(x))^2 = 2g(x)g''(x)$. This is the exact same condition for $P$ to be a point of inflection.

We'll be done when we know about the $y$-coordinate. But if $P$ and $2P$ have the same $x$-coordinate, then the only possibilities for the $y$-coordinate of $2P$ are $y$ and $-y$. That is, either $2P = P$ or $2P = -P$. If $2P = P$, then $P = \mathbf{O}$ (just add $-P$ to both sides). But that can't happen since $P$ is a finite point. Hence, $2P = -P$. But adding $P$ to both sides shows that $3P = \mathbf{O}$. Hence, we have shown that if $P$ is a finite point, then $P$ is a PI if and only if $3P = \mathbf{O}$. We are done.

As a corollary, we can show that $\mathbf{O}$ is also a point of inflection.

We merely count points. Suppose $l$ is a tangent line to the elliptic curve $E$ at $\mathbf{O}$. By point–counting, there must be another point where $l$ meets $E$: call it $R$. Could $R$ be a finite point? No, for if $R$ and $\mathbf{O}$ are on the line $l$, we have seen that $-R$ is also on that line. So, $l$ contains $R$ and $-R$—that makes two, even if $R = -R$—and also $\mathbf{O}$ doubly, which makes four in all. Too many points! Hence, $R$ cannot be a finite point, which means that $R = \mathbf{O}$. We conclude that a line tangent to $E$ at $\mathbf{O}$ intersects the curve $E$ triply. Hence, $\mathbf{O}$ is a point of inflection of $E$, and we are done.

Since $3\mathbf{O} = \mathbf{O}$, we now can say that the PIs of an elliptic curve are precisely those points $P$ for which $3P = \mathbf{O}$.

We are now ready for our main result, namely, that the nine PIs of an elliptic curve can be arranged to form a nine–point plane.

**The Magic Square Theorem.** Every elliptic curve has nine points of inflection, and these points form an affine plane of order 3. That is, each point of inflection lies on exactly four lines, each of which contains two other points of inflection—making 12 lines in all—and each pair of points of inflection determines a unique line.

*Proof.* Let us first show that a line through two PIs meets the curve in a third PI. The reason for this is that if $P$, $Q$ and $R$ are points of $E$ which lie on a line, then $R = P * Q = -(P + Q)$. Then, since $3P = 3Q = \mathbf{O}$, we see that

$$\mathbf{O} = \mathbf{O} + \mathbf{O} = 3P + 3Q = 3(P + Q) = 3(-R) = -3R.$$

Hence, $3R = -\mathbf{O} = \mathbf{O}$, and we conclude that $R$ is also a PI.

Next, by point–counting, no more than three distinct PIs of $E$ can lie on a line. Since each pair of PIs on $E$ lies on a unique line, each line containing two PIs contains exactly one other, and that line accounts for three pairs of PIs. Now there are a total of 36 pairs of PIs, 36 being the number of 2-element subsets of a 9-element set. Thus, there are twelve lines in all, each containing three PIs.

Finally, a given PI $Q$ must pair up with each of the other eight PIs. Since there are three PIs on a line, that puts exactly four lines through $Q$, each containing two other PIs. We are done!

For an example, let us look at $E_2 : y^2 = x^3 + 2$, the curve on the right in Figure 1. As we saw in the last Section, $y'' = \frac{3x^4+24x}{2y^3}$, so that $(x, y)$ is a finite PI if and only if $3x^4 + 24x = 0$. From this and a little algebra, we find that the nine PIs are

$$\pm A = (0, \pm\sqrt{2}), \quad \pm B = (-2, \pm i\sqrt{6}), \quad \pm C = (-2\omega, \pm i\sqrt{6}),$$
$$\pm D = (-2\omega^2, \pm i\sqrt{6}), \quad \text{and } \mathbf{O},$$

where $\omega = (-1 + i\sqrt{3})/2$.

 

How do these nine line up? Since three points on a line must sum to zero, it's clear that four of the lines are $\{\mathbf{O}, A, -A\}$, $\{\mathbf{O}, B, -B\}$, $\{\mathbf{O}, C, -C\}$, and $\{\mathbf{O}, D, -D\}$. To find the other eight lines, just use the slope formula from analytic geometry, and don't worry if your slopes are nonreal! (For example, the line through $A$, $-B$ and $D$ has slope $-\omega^2\sqrt{2}$.) When you are done, you will be able to arrange the points into this $3 \times 3$ magic square, which resembles the one in the book [**5**] I was reading on elliptic curves:

| | | |
|---|---|---|
| $B$ | $-A$ | $-D$ |
| $C$ | $\mathbf{O}$ | $-C$ |
| $D$ | $A$ | $-B$ |

This result ties together threads from finite geometry, recreational mathematics, combinatorics, calculus, algebra, and number theory. Quite a feat!

## References


1. Arthur Benjamin and Kan Yasuda, Magic "Squares" Indeed!, *Amer. Math. Monthly* **106** (1999), 152–156.
2. David M. Burton, *The History of Mathematics* (3rd ed), McGraw–Hill, 1997.
3. Ronald Calinger (ed.), *Classics of Mathematics*, Prentice–Hall, 1995.
4. Martin Gardner, *Penrose Tiles To Trapdoor Codes . . . And The Return Of Dr. Matrix*, W. H. Freeman, 1989.
5. Viktor Prasolov and Yuri Solvyev, *Elliptic Functions and Elliptic Integrals*, American Mathematical Society, 1997.
6. George B. Thomas and Ross L. Finney, *Calculus and Analytic Geometry* (9th edition), Addison–Wesley, 1996.
7. Andrew Wiles, Modular elliptic curves and Fermat's Last Theorem, *Annals of Mathematics* **142** (1995), 443–551.


### Digits

Paul Kaschube (kaschube@tri.sbc.com) was inspired by the twin primes in the March 2001 issue, $665551035 \cdot 2^{80025} \pm 1$, to calculate all 24099 digits of both. They start with 560 and end with 121 and 119, respectively. He will supply them all to anyone who is interested. Who knows that secrets they contain? Do they have 314159265358979 in them? Or perhaps, as 665551035, rather more 5s than could be expected? They could be worth a look.