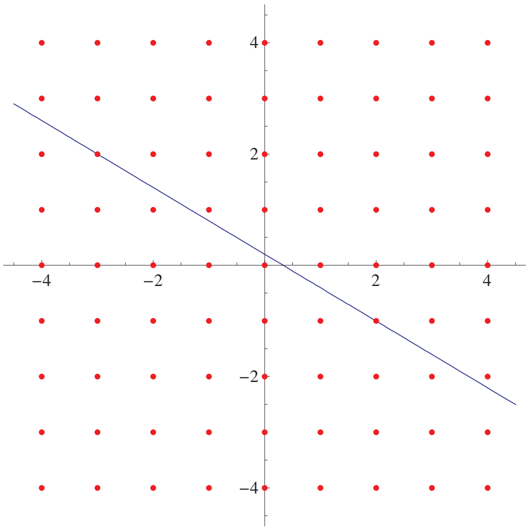
Diophantine equations

So far, we have considered solutions to equations over the real and complex numbers. This chapter instead focuses on solutions over the integers, natural and rational numbers. There is no algorithm for solving a generic Diophantine equation, which is why they can be very difficult to solve. In fact, many open problems such as the Riemann hypothesis can be embedded in questions about Turing machines, which can in turn be converted to hideously complicated Diophantine equations. Even proving the non-existence of positive integer solutions to the innocuous-looking equation $x^n + y^n = z^n$ $(n \geq 3)$ (Fermat's last theorem) occupied mathematicians for three centuries before finally being settled by Andrew Wiles.

We will adopt a geometric approach to the problem, locating points in $\mathbb{Z}^n$, $\mathbb{N}^n$ and $\mathbb{Q}^n$ lying on some particular curve. The simplest curve is a straight line (or plane, or hyperplane), corresponding to a *linear Diophantine equation*. Linear Diophantine equations are easy. Let's consider the example $3\,x + 5\,y = 1$.

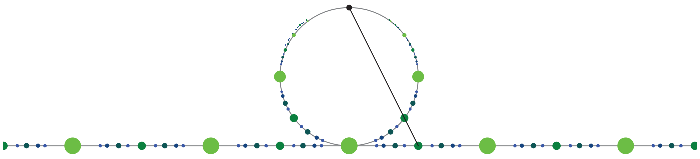


We can see that this has integer solutions, such as $(x,\ y) = (2,\ -1)$. In general, any linear Diophantine equation with coprime coefficients has infinitely many solutions in the integers, which can be found using the Chinese remainder theorem. If the coefficients are not coprime, such as $6\,x - 4\,y = 5$, there may be (as in this case) no solutions. If there are no solutions, a simple proof exists using modular arithmetic.

- A point $(x,\ y)$ is *rational* if and only if both x and y are rational.

1. Let Γ be a conic with rational coefficients, and let A be a rational point on Γ. If B is another point on Γ, show that B is rational if and only if $A\,B$ has rational gradient.

This theorem enables us to find all integer solutions to $a^2 + b^2 = c^2$, known as *Pythagorean triples* as they correspond to right-angled triangles with integer side lengths such as the famous (3, 4, 5) triangle used as a set square by the Ancient Egyptians. We can apply the geometrical concept of stereographic projection.



2. Show that all rational points on the unit circle can be obtained by inverting the rational line, as shown above.

3. Find all rational solutions to $x^2 + y^2 + z^2 = 1$.

4. Hence find all integer solutions to $a^2 + b^2 = c^2$, where $\gcd(a, b, c) = 1$. **[Elementary Pythagorean triples]**

5. Show that there exists an infinite set S of points, no three of which are collinear, such that the distance between any two points is rational.

Vieta jumping

Suppose we are attempting to determine whether or not a certain quadratic equation in two variables has integer solutions. This can be visualised as a conic section, which is either an ellipse, parabola or hyperbola. As an ellipse is finite, we need only check a few pairs of values for integer solutions. To deal with the parabola, we can change the coordinate system by applying an affine transformation to convert it into a simpler equation. For the hyperbola, however, it is necessary to adopt a more sophisticated technique such as *Vieta jumping*.

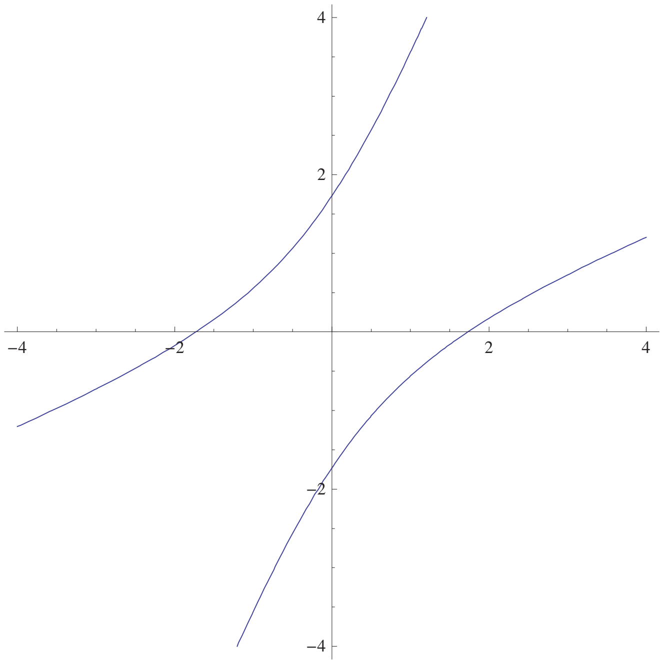
For example, consider the equation $a^2 + b^2 = k(a\,b + 1)$, where k is a fixed positive integer.

6. Find all integer solutions to the equation $a^2 + b^2 = k(a\,b + 1)$ for the cases where $k = 1$ and $k = 2$.

We will now consider the cases where $k \geq 3$.

7. Show that there are no integer solutions to $a^2 + b^2 = k(a\,b + 1)$ where $k \geq 3$ and one of a, b is negative and the other is positive.

8. Sketch the curve Γ described by the equation $x^2 + y^2 = k(x\,y + 1)$, for $k \geq 3$.



9. Suppose that $P = (a, b)$ is a positive integer solution, and draw a vertical line through P. Show that it meets Γ again at another non-negative integer point, $Q = (a, c)$. Also, if $b > a$, then show that $c < b$.

This is the principle behind Vieta jumping. We start with some (hypothetical) solution, then use it as the basis to construct a smaller solution until we reach a contradiction. Fermat employed this process of infinite descent to prove that there are no solutions in the positive integers to $x^4 + y^4 = z^4$. Euler later refined the approach to apply to the equation $x^3 + y^3 = z^3$.

10. If $a^2 + b^2 = k(a\,b + 1)$ (for some $k \geq 3$) has a solution in the integers, then show that there is a solution where $b = 0$.

11. Let a and b be positive integers. Prove that if $\frac{a^2+b^2}{a\,b+1}$ is a positive integer, then it is a perfect square. **[IMO 1988, Question 6]**

12. Let a and b be positive integers. Prove that if $\frac{a^2+b^2+1}{a\,b}$ is a positive integer, then it equals 3.

Pell equations

Vieta jumping is primarily useful for proving the non-existence of solutions to hyperbolic equations. What if, instead, we want to find an infinite family of solutions? The idea is to create new solutions from old by some form of recurrence relation. Firstly, consider equations of the form $x^2 = n\,y^2 + 1$, where n is not a perfect square. These are known as *Pell equations*, even though Pell had absolutely nothing to do with them. Basically, someone wanted to solve these equations, so told Euler that Pell was working on them. Consequently, Euler solved the equations, but attributed them to Pell.

13. Consider the complex numbers $z = a + b\sqrt{-n}$ and $w = c + d\sqrt{-n}$. Prove that $\left(a^2 + n\,b^2\right)\left(c^2 + n\,d^2\right) = (a\,c - b\,d\,n)^2 + n(a\,d + b\,c)^2$. **[Brahmagupta's identity]**

Brahmagupta's identity can also be verified algebraically, so is true even when n is negative. This gives us the related identity $\left(a^2 - n\,b^2\right)\left(c^2 - n\,d^2\right) = (a\,c + b\,d\,n)^2 - n(a\,d + b\,c)^2$.

14. Show that we can generate infinitely many solutions (in positive integers) to $x^2 = n\,y^2 + 1$ (where $\sqrt{n} \notin \mathbb{N}$) from one known solution.

15. Hence prove that there are infinitely many square triangular numbers.

As x and y can be very large, we obtain very good rational approximations $\frac{x}{y} \simeq \sqrt{n}$ in this manner. These rational approximations can also be generated by analysing the *continued fraction* expansion of $\sqrt{n}$, i.e. the unique expression of $\sqrt{n}$ of the following form:

$$x = \cfrac{1}{\cfrac{1}{\cfrac{1}{a_4+\ldots} + a_3} + a_2} + a_1$$

We write this as $[a_1; a_2, a_3, a_4, \ldots]$. The sequences of all quadratic irrationals (solutions to quadratic equations in integer coefficients) are eventually periodic, and the converse also holds. For example, the sequence $[1; 1, 1, 1, 1, \ldots]$ corresponds to $\phi = \frac{1+\sqrt{5}}{2}$, and truncating the sequence produces the approximations $\frac{F_{n+1}}{F_n}$, where F_n is the nth Fibonacci number. Every Pell equation has infinitely many solutions. This is not true in general of the *negative Pell equation*, $x^2 = n\,y^2 - 1$ (where $\sqrt{n} \notin \mathbb{N}$); the negative Pell equation has solutions if the continued fraction has an odd period length.

The continued fraction for π is somewhat chaotic: $[3; 7, 15, 1, 292, \ldots]$. Truncating before the 292 yields the approximation $[3; 7, 15, 1] = [3; 7, 16] = \frac{355}{113}$, which agrees with the actual value of π to six decimal places. e has a very regular continued fraction expansion of $[2; 1, 2, 1, 1, 4, 1, 1, 6, 1, 1, 8, 1, \ldots]$.

Sums of squares

Brahmagupta's identity, in the case where $n = 1$, provides the identity $\left(a^2 + b^2\right)\left(c^2 + d^2\right) = (a\,c - b\,d)^2 + (a\,d + b\,c)^2$ as a special case. In other words, if S is the set of numbers that can be expressed as the sum of two squares (of integers, or, more generally, of rationals), then S is closed under multiplication. Using Hamiltonian quaternions, we can produce an analogous formula for four squares:

- $(a^2 + b^2 + c^2 + d^2)(e^2 + f^2 + g^2 + h^2) =$
  $(a\,e - b\,f - c\,g - d\,h)^2 + (a\,f + b\,e + c\,h - d\,g)^2 + (a\,g - b\,h + c\,e + d\,f)^2 + (a\,h + b\,g - c\,f + d\,e)^2$
  [Euler's four-square identity]

Using even more bizarre eight-dimensional numbers called octonions, there is a similar identity for eight squares. However, there are no identities beyond this, as doubling the number of dimensions causes the numbers to lose their useful properties. Quaternions are non-commutative, i.e. $x\,y \neq y\,x$ in general. Octonions are even worse, since they also lose associativity: $x(y\,z) \neq (x\,y)\,z$. Beyond this, the numbers have no useful properties remaining, and the 2^n-square identity breaks down.

It is interesting to see when an integer can be expressed as the sum of n squares of integers. Clearly, if N can be expressed as the sum of squares of n integers, then it can also be expressed as the sum of squares of $n + 1$ integers, as we can set one of those equal to zero. This gives a nested hierarchy:

- A positive integer N can be expressed as the sum of **one** square if and only if it is a perfect square, i.e. $N = a^2$ for some $a \in \mathbb{N}$. **[Trivial one-square theorem]**

- A positive integer N can be expressed as the sum of **two** squares if and only if it can be expressed as $N = a^2\,2^k\,(p_1\,p_2\,\ldots\,p_n)$, where each p_i is a prime congruent to 1 (modulo 4) and a and k are non-negative integers. **[Fermat's Christmas theorem]**

- A positive integer N can be expressed as the sum of **three** squares if and only if it is **not** of the form $4^k\,(8\,m + 7)$. **[Legendre's three-square theorem]**

- Any positive integer can be expressed as the sum of **four** squares. **[Lagrange's four-square theorem]**

16. Generalise each of the above theorems to determine when a rational number is expressible as the sum of one, two, three or four squares of rationals.

Sam Cappleman-Lynes technique

Consider the Diophantine equation $x^3 + y^6 = z^7$. If we have a solution to the equation $a^3 + b^6 = c$ (which is trivial), then we can multiply all terms by c^6 to obtain $a^3\,c^6 + b^6\,c^6 = c^7$, which is a solution to the original equation. This enables us to create infinitely many distinct solutions in this manner. This idea, known as the *Sam Cappleman-Lynes technique*, is applicable in many problems.

17. Show that there are infinitely many solutions to $x^4 + y^6 = z^{10}$ in the positive integers.

More generally, if a, b, c are pairwise coprime, then $x^{a\,k} + y^{b\,k} = z^{c\,k}$ has infinitely many solutions in the positive integers when $k = 1$ or $k = 2$. A consequence of Fermat's last theorem is that there are no solutions for $k \geq 3$.

18. Let A be the set of all integers of the form $a^2 + 13\,b^2$, where a and b are integers and b is non-zero. Prove that there are infinitely many pairs of integers $x,\ y$ such that $x^{13} + y^{13} \in A$ but $x + y \notin A$. **[Mongolian TST]**

19. Determine whether there exists a set S of 2012 positive integers such that the sum of elements in each subset of S is a non-trivial power of an integer. **[IMO 1992 shortlist]**

A large proportion of the problems solved using the Sam Cappleman-Lynes technique reduce to this (very general) theorem, which is proved first by applying linear algebra to the simultaneous equations followed by a similar approach to the last question.

- Suppose we have a system of m equations in n variables $(x_1, x_2, \ldots, x_n)$ of the following form, where $m < n$:
  - $r_{(1,1)}\, x_1{}^{a_1} + r_{(1,2)}\, x_2{}^{a_2} + \ldots + r_{(1,n)}\, x_n{}^{a_n} = 0$;
  - $r_{(2,1)}\, x_1{}^{a_1} + r_{(2,2)}\, x_2{}^{a_2} + \ldots + r_{(2,n)}\, x_n{}^{a_n} = 0$;
  - …
  - $r_{(m,1)}\, x_1{}^{a_1} + r_{(m,2)}\, x_2{}^{a_2} + \ldots + r_{(m,n)}\, x_n{}^{a_n} = 0$.

  Suppose that the following conditions are also true:
  - All of the coefficients, $r_{(i,j)}$, are rational (not necessarily all non-zero);
  - All of the exponents, a_i, are positive integers;
  - $\det\begin{pmatrix} r_{(1,1)} & r_{(1,2)} & \cdots & r_{(1,m)} \\ r_{(2,1)} & r_{(2,2)} & \cdots & r_{(2,m)} \\ \vdots & \vdots & \ddots & \vdots \\ r_{(m,1)} & r_{(m,2)} & \cdots & r_{(m,m)} \end{pmatrix} \neq 0$;
  - For all $i \leq m$ and $i < j \leq n$, a_i is coprime with a_j;
  - There is at least one solution in the positive *real* numbers.

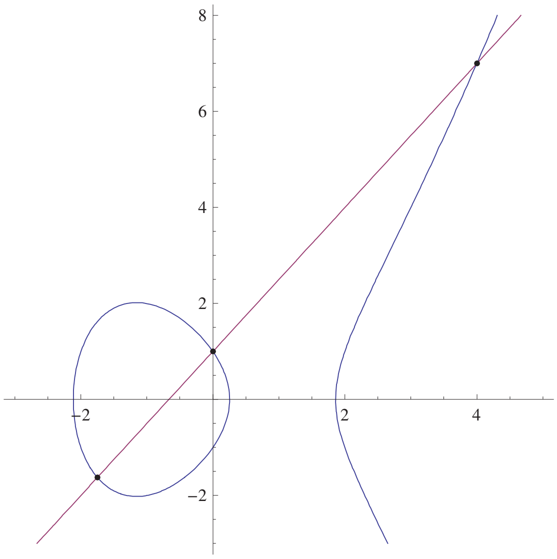
  In that case, there are infinitely many solutions in the positive integers. **[Generalised Sam Cappleman-Lynes theorem]**

The invertibility of the matrix enables us to apply elementary row operations to reduce it to a diagonal matrix in a process known as *Gauss-Jordan manipulation*. We then have m equations of the form $x_i{}^{a_i} = q_{(i,m+1)}\, x_{m+1}{}^{a_{m+1}} + q_{(i,m+2)}\, x_{m+2}{}^{a_{m+2}} + \ldots + q_{(i,n)}\, x_n{}^{a_n}$ (one equation for each $1 \leq i \leq m$), and a real solution to the equations. This is a linear equation in $x_i{}^{a_i}$ (for all $1 \leq i \leq n$), so can be represented by a $(n - m)$-dimensional hyperplane in n-dimensional space (which passes through the origin, like a projective $(n - m - 1)$-hyperplane). The single real solution means that this hyperplane intersects the positive quadrant, so we can set initial rational values for each of the *free variables* $\{x_{m+1}, x_{m+2}, \ldots, x_n\}$. This forces every $x_i{}^{a_i}$ to be positive and rational. We then apply the Sam Cappleman-Lynes technique to the equations, relying on the coprimality of various exponents. After all variables have been rationalised, we multiply out by a large power of the lowest common multiple of the denominators of the variables, turning them into integer solutions.

Elliptic curves

20. Let Γ be a non-singular cubic curve with integer coefficients. Suppose we have a line Λ which meets Γ at three points, A, B and C. Prove that if A and B are rational, then C is also rational.

For example, the curve $y^2 = x^3 - 4x + 1$ has rational points $(0, 1)$ and $(4, 7)$. We then draw the line through the two points, namely $y = \frac{3}{2}x + 1$. This intersects the curve at a third point, which is the solution of the cubic equation $\left(\frac{3}{2}x + 1\right)^2 = x^3 - 4x + 1$, which simplifies to $x^3 - \frac{9}{4}x^2 - 7x = 0$. We can factorise this, as we already know two of the roots, obtaining $x(x - 4)\left(x + \frac{7}{4}\right) = 0$. This gives us a third rational point on the elliptic curve, namely $\left(-\frac{7}{4}, -\frac{13}{8}\right)$.



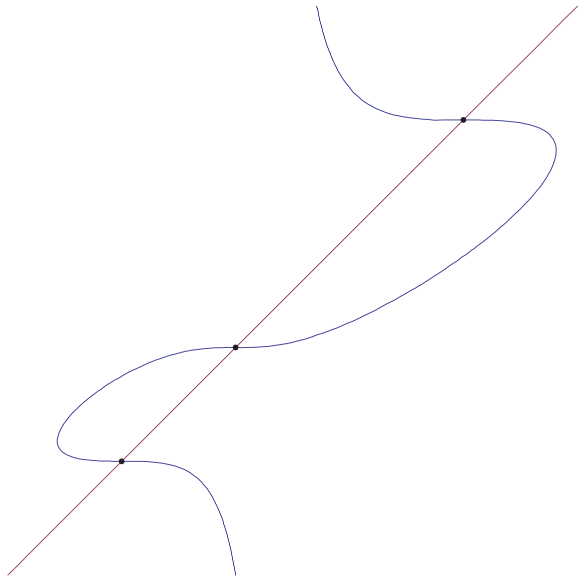
One of the great unsolved problems in mathematics, the Birch and Swinnerton-Dyer conjecture, is concerned with counting the number of integer points on an elliptic curve modulo p. Elliptic curves also featured prominently in Andrew Wiles' proof of the Tanayama-Shimura conjecture and Fermat's last theorem. Specifically, Wiles showed that every elliptic curve could be associated with a 'modular form', a complex function with the same hyperbolic symmetries as the Ford circles. Even the simplest, most elementary proof of Poncelet's porism involves elliptic curves.

We define a binary operation + on the points on the cubic curve, such that $A + B + C = 0$ for any three collinear points A, B, $C \in \Gamma$. In other words, $C = -(A + B)$. Let $O = 0$ be one of the points of inflection, so the line passing through C and O meets Γ again at $C' = A + B$. It is trivially obvious that this operation is commutative, but proving associativity is a little more difficult.

21. Let X, Y, Z be three non-collinear points on Γ. Show that $(X + Y) + Z = X + (Y + Z)$, where addition is defined as in the last paragraph. **[Associativity of elliptic curve operation]**

After proving associativity, parentheses can be omitted from expressions without ambiguity. For example, we can refer to the last expression simply as $X + Y + Z$. Addition of elements forms a group operation. We can then multiply by an integer n, by defining $n X = X + X + \ldots + X$. It is difficult to compute n from the points $n X$ and X, so can form the basis of a cryptosystem similar to RSA using the group $\{\Gamma, +\}$ instead of $\{\mathbb{Z}_{p q}, \times\}$. Elliptic curve cryptography is considered to be more secure than RSA. Again, it is susceptible to attacks from quantum computers.

22. Let A, B, C be three collinear points on Γ. If A and B are both points of inflection, then show that C is also a point of inflection.



In the above diagram, a line is drawn through the three real points of inflection of a cubic curve. A general cubic curve on the complex projective plane has nine points of inflection lying on twelve lines in what is known as the *Hesse configuration*. It is a remarkable fact that this cannot be embedded in the *real* projective plane due to the *Sylvester-Gallai theorem*: if there is a finite set S of points such that no line contains exactly two points, then all points are collinear. Hence, a cubic curve has at most three real points of inflection.

Solutions

1. Clearly, if $A\,B$ has irrational gradient, then A is the only rational point on Γ. If $A\,B$ has rational gradient, then we can express it as a linear equation in rational coefficients. By solving this simultaneously with the equation for Γ, we obtain a quadratic equation in rational coefficients for x (the abscissa). As one root of this (the coordinates of A) is rational, then the other root must also be. Repeating this process for y (the ordinate), it is evident that $B \in \mathbb{Q}^2$.

2. Inverting about a rational point A on the unit circle transforms the circle into a line by stereographic projection. All lines with rational slopes through A clearly correspond to the entire set of rational points on the real line.

3. This is the three-dimensional analogue of the problem. We want to transform a point $\overrightarrow{O\,A}$ on the horizontal plane into a vector $\overrightarrow{O\,B}$ on the unit sphere by inverting about a sphere with centre $C = (0,\ 0,\ 1)$ and radius $\sqrt{2}$. We have that $\overrightarrow{C\,A}$ and $\overrightarrow{C\,B}$ are parallel, and the product of their lengths is 2. Hence, this gives us the formula $\overrightarrow{C\,B} = \frac{2\,\overrightarrow{C\,A}}{|\overrightarrow{C\,A}|^2}$. If we let A have coordinates $\left(\frac{p}{q},\ \frac{r}{q},\ 0\right)$, where p, q and r are coprime, then we obtain $\overrightarrow{C\,B} = \frac{2\left(\frac{p}{q},\frac{r}{q},-1\right)}{\left(\frac{p}{q}\right)^2+\left(\frac{r}{q}\right)^2+1}$. This simplifies to $\overrightarrow{C\,B} = \frac{2\,(p\,q, r\,q, -q^2)}{p^2+q^2+r^2}$. Now, $\overrightarrow{O\,B} = \overrightarrow{O\,C} + \overrightarrow{B\,C} = \frac{(2\,p\,q, 2\,r\,q, p^2+r^2-q^2)}{p^2+q^2+r^2}$, giving us the complete set of solutions; $x = \frac{2\,p\,q}{p^2+q^2+r^2}$, $y = \frac{2\,r\,q}{p^2+q^2+r^2}$, $z = \frac{p^2-q^2+r^2}{p^2+q^2+r^2}$, where $p,\ q,\ r \in \mathbb{Z}$, $q > 0$ and $\gcd(p,\ q,\ r) = 1$.

4. a and b cannot both be odd; assume without loss of generality that a is even. Hence, b is odd as otherwise a, b and c would all be even. Using the previous question (and setting $r = 0$), the solutions to $\left(\frac{a}{b}\right)^2 + \left(\frac{a}{c}\right)^2 = 1$ are $\frac{a}{c} = \frac{2\,p\,q}{p^2+q^2}$ and $\frac{b}{c} = \frac{p^2-q^2}{p^2+q^2}$. If p and q are both odd then c is even, so one of p and q must be even. Hence, $p^2 - q^2$ and $p^2 + q^2$ are coprime (by applying Euclid's algorithm to obtain $2\,p^2$ and $2\,q^2$, which only share 2 as a common factor). This gives us the irreducible general solution; $(a,\ b,\ c) = \left(2\,p\,q,\ p^2 - q^2,\ p^2 + q^2\right)$, where p and q are coprime integers.

5. Let $A\,B$ be the base of a semicircle with unit radius. A point C on the curved edge of the semicircle belongs to S if and only if both $A\,C$ and $B\,C$ are rational. (The previous question guarantees infinitely many choices of C.) If we have two such points, C_1 and C_2, (such that A, C_1, C_2, B appear in that order) then $C_1\,C_2 \cdot A\,B = C_1\,B \cdot C_2\,A - C_1\,A \cdot C_2\,B$ (by Ptolemy's theorem), and thus $C_1\,C_2$ is rational.

6. For $k = 2$, the equation $a^2 + b^2 = 2\,a\,b + 2$ simplifies to the $(a - b)^2 = 2$, which clearly has no integer solutions. For $k = 1$, $a^2 + b^2 = 1 + a\,b$ is an ellipse. As $a^2 + b^2 \geq 2\,a\,b$, then $a\,b \leq 1$. Also, $a\,b \geq -1$, since otherwise $a^2 + b^2$ would be negative. It is a simple matter to check all combinations of $a,\ b \in \{-1,\ 0,\ 1\}$ and deduce that the solutions $(0,\ 1)$, $(1,\ 0)$, $(0,\ -1)$, $(-1,\ 0)$, $(1,\ 1)$ and $(-1,\ -1)$ are the only solutions.

7. If one of a, b is negative and the other is positive, then $a\,b < 0$. Hence, $a\,b \leq -1$ and thus $k(a\,b + 1) \leq 0$. However, $a^2 + b^2 = k(a\,b + 1)$ is strictly positive.

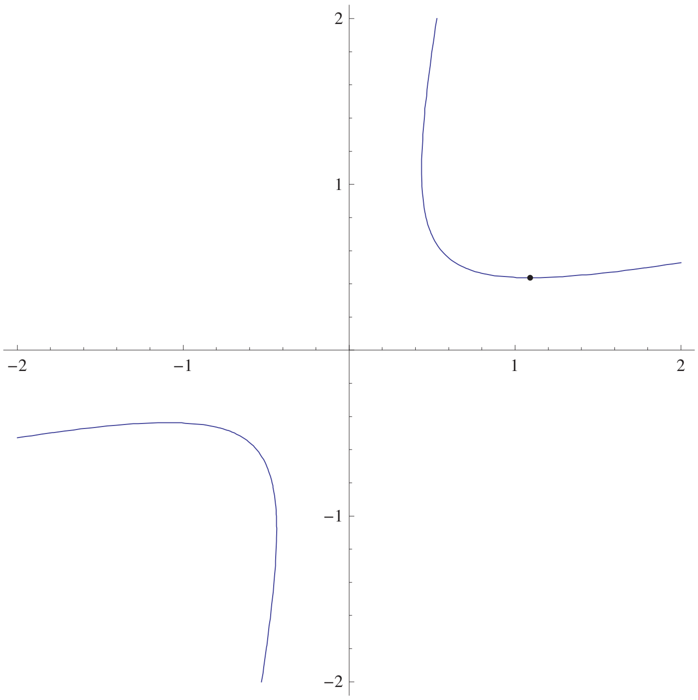
8. If we apply the substitution $z = x + y$, $w = x - y$ then we obtain a hyperbola in standard position. Hence, the original curve is a hyperbola with centre $(0,\ 0)$ and an axis of symmetry $y = x$, which does not intersect the hyperbola on the real plane.

9. As $a^2 + b^2 = k(a\,b + 1)$, b is a root of the quadratic $z^2 - k\,a\,z + \left(a^2 - 1\right) = 0$. By Vieta's formulas, we have $b + c = k\,a$, and thus $c = k\,a - b$. This is obviously an integer point. As $b > a$, P is on the upper branch of the hyperbola, so Q must be on the lower branch and therefore $c < b$.

10. Assume that $P = (a, b)$ is a positive integer solution and that $b > a$. We can generate a smaller solution in the non-negative integers by choosing the other intersection point $Q = (a, c)$ of the line $x = a$ and curve Γ. By reflecting in the line $y = x$, we obtain a solution $P' = (c, a)$, where $a > c$. This process will generate continually smaller solutions until one of the coordinates is zero.

11. Let $\frac{a^2+b^2}{a\,b+1} = k$. If $k = 2$, then there are trivially no solutions. Otherwise, if $k \geq 3$ and we have an integer solution (a, b), we can generate a solution where $b = 0$. So, there is a solution in the positive integers if and only if there is a value k such that $\frac{a^2}{1} = k$, which only occurs when k is a perfect square.

12. Consider the equation $a^2 + b^2 + 1 = a\,b\,k$. This can be algebraically manipulated to $(a - b)^2 + 1 = (k - 2)\,a\,b$; hence, it is obvious that $k \geq 3$. We now fix the value of k. As there are no solutions for $a = 0$ or $b = 0$, and every solution (a, b) yields alternative solutions $(-a, -b)$ and (b, a), the curve must be a hyperbola with centre $(0, 0)$ and diagonal lines of symmetry. Moreover, the hyperbola is contained entirely within the first and third quadrants. Using Vieta jumping, we can get from a solution (a, b) to $(b\,k - a, b)$. If (a, b) lies to the right of the stationary point of the hyperbola, then this will generate a smaller (in terms of $a + b$) solution. We can then reflect in the line $a = b$ and repeat the process until (a, b) lies to the left of this stationary point and below (or on) the line $a = b$. By considering the discriminant of $a^2 - b\,k\,a + b^2 + 1 = 0$, the stationary point can be located as $\left(\frac{k}{\sqrt{k^2-4}}, \frac{2}{\sqrt{k^2-4}}\right)$. The only integer point lying to the left of this such that $a \geq b$ is $(1, 1)$, which clearly is only a solution when $k = 3$. The graph below is the hyperbola for $k = 5$.



13. This is simply the equation $|z|^2\,|w|^2 = |z\,w|^2$.

14. If we have two solutions (not necessarily distinct), (a, b) and (c, d), then $a^2 - n\,b^2 = 1$ and $c^2 - n\,d^2 = 1$. We can multiply them together and use Euler's identity to obtain $(a\,c + b\,d\,n)^2 - n(a\,d + b\,c)^2 = 1$, which is a strictly larger solution to the equation. Repeating the process from some initial solution (b, a), we expand $\left(a^2 - n\,b^2\right)^k$ using Euler's identity recursively to obtain infinitely many solutions, one for each $k \in \mathbb{N}$.

15. For every triangular number T, $8\,T + 1$ is square and the converse also holds. Hence, we want to solve the Pell equation $x^2 = 8\,y^2 + 1$. A preliminary solution is that 36 is both square and triangular, or $17^2 = 8 \cdot 6^2 + 1$, from which we generate an infinitude.

16. Suppose we have a rational $\frac{a}{b}$, where a and b are coprime. Squaring it results in $\frac{a^2}{b^2}$, where a^2 and b^2 are still coprime. Hence, squares of rationals (or sums of one square) have both a square numerator and denominator when expressed in lowest terms. Suppose $\frac{a}{b} = \frac{c^2}{d^2} + \frac{e^2}{f^2} = \frac{c^2\,f^2 + e^2\,d^2}{d^2\,f^2}$ is expressible as the sum of two rational squares. Then, it is expressible as a square of a rational multiplied by the sum of squares of two integers, therefore of the form $N = t^2\,2^k\,(p_1\,p_2\,\ldots\,p_n)$, where each p_i is a prime congruent to 1 (modulo 4), k is an integer and t is a non-negative rational. For sums of three squares of rationals, we can express it as a square of a rational multiplied by the sum of squares of three integers. Hence, it is something that **cannot** be expressed as $\frac{4^k\,(8\,m+7)}{t^2}$, where t is an odd integer, k is an integer and m is a non-negative integer. Any rational can be expressed as the sum of four squares of rationals.

17. We begin with a solution to $a^2 + b^2 = c^2$, i.e. a Pythagorean triple. Multiplying by a^2 gives us $a^4 + b^2\,a^2 = c^2\,a^2$. Then multiply by $b^4\,a^4$, giving us $b^4\,a^8 + b^6\,a^6 = c^2\,b^4\,a^4$. Finally, multiply by $c^{48}\,b^{96}\,a^{96}$, resulting in $c^{48}\,b^{100}\,a^{104} + c^{48}\,b^{102}\,a^{102} = c^{50}\,b^{100}\,a^{100}$. This is clearly a solution to the equation $x^4 + y^6 = z^{10}$.

18. If $x \equiv 1 \pmod 4$ and $y \equiv 2 \pmod 4$, then clearly $x + y \notin A$. All numbers of the form $13\,b^2$ are in A, so if we can find infinitely many solutions satisfying $x^{13} + y^{13} = 13\,b^2$ and the modulo-4 congruences then we are done. Start with a solution to $w^{13} + z^{13} = 13\,u$, where $w \equiv 1$ and $z \equiv 2 \pmod 4$. We note that u must be congruent to 1 (mod 4), as $w^{13} \equiv 1$ and $z^{13} \equiv 0$. We multiply by u^{13} to give a solution $(u\,w)^{13} + (u\,z)^{13} = 13\left(u^7\right)^2$, without changing the congruence class of any of the variables. We can start with $w = 13 + 52\,k$ and $z = 26$, generating a solution for every $k \in \mathbb{N}$. As these solutions can become arbitrarily large, there must be infinitely many.

19. For each $1 \le j \le 2^{2012} - 1$, consider the Diophantine equation of the form $\sum a_i^2 = b_j^{p_j}$, where a_i $(1 \le i \le 2012)$ is included in the sum if and only if the ith binary digit of j is 1, and p_j is the jth odd prime. We then apply the Sam Cappleman-Lynes technique to all equations simultaneously starting from the $2^{2011} - 1$ equations of the form $\sum x_i^2 = y_j$. We initially set $x_i = i$, and then multiply all equations by an appropriate power of $y_j^{2\,p_1\,p_2\,\cdots\,p_{j-1}}$. This preserves the perfect-power property of all previous equations, and we can do this until the jth equation is also converted to the desired form. Repeating for all $2^{2012} - 1$ equations gives us a solution to the original Diophantine equations. Then just take $S = \left\{a_1^2,\, a_2^2,\, \ldots,\, a_{2^{2012}-1}^2\right\}$.

20. The line passes through two rational points, so must have rational gradient. Hence, we can express y as a linear function of x with rational coefficients. Let a, b, c be the abscissae of A, B, C, respectively. The intersection of the cubic curve and the line is a cubic equation with rational coefficients and roots a, b, c. Due to Vieta's formulas, $a + b + c$ is one of the rational coefficients. Hence, the rationality of a and b implies that of c.

21. Let Φ be the union of the lines $\{Y, -(X+Y), X\}$, $\{-(Y+Z), O, Y+Z\}$ and $\{Z, X+Y, -((X+Y)+Z)\}$. Similarly, let Ψ be the union of the lines $\{Y, -(Y+Z), Z\}$, $\{-(X+Y), O, X+Y\}$ and $\{X, Y+Z, -(X+(Y+Z))\}$. The three cubic curves Γ, Φ and Ψ intersect in eight points, namely $\{X, Y, Z, -(X+Y), -(Y+Z), X+Y, Y+Z, 0\}$, so must intersect in the ninth point by Cayley-Bacharach. Hence, $-((X+Y)+Z) = -(X+(Y+Z))$, and thus $(X+Y)+Z = X+(Y+Z)$.

22. The tangent lines passing through A and B do so with multiplicity 3, so we have $3\,A = 3\,B = 0$. We then have $3\,C = -3\,(A+B) = 0$, so C is also a point of inflection.