Solving a Number Theory Problem With Vieta Jumping

Candidate Code: hzh277

1 Introduction

Vieta's formulas relate the coefficients of a polynomial with sums and products of its roots. For a polynomial $P(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$ with roots $r_1, r_2, \ldots, r_n$, Vieta's formulas state that

$$\begin{aligned} r_1 + r_2 + \cdots + r_n &= -\frac{a_{n-1}}{a_n} \\ r_1 r_2 \ldots r_n &= \frac{(-1)^n a_0}{a_n}. \end{aligned}$$

Vieta's formulas can be derived by rewriting the polynomial in its factored form, $P(x) = a_n (x - r_1)(x - r_2) \cdots (x - r_n)$, expanding this expression, and matching coefficients. Matching the constant term and the coefficient of x^{n-1} yields the two above equations.

These formulas can be applied to solve number theory problems through a technique called Vieta jumping, where we "jump" from a known root of a (typically quadratic) polynomial to another using Vieta's formulas. In this exploration, I aimed to solve a challenging number theory problem using Vieta jumping. The following problem was the fifth problem in the 2009 USA Team Selection Test.

> **Problem.** Find all ordered pairs of positive integers (m, n) such that $mn - 1$ divides $\left(n^2 - n + 1\right)^2$.

1.1 Vieta jumping and infinite descent

As mentioned above, I will attempt to use Vieta jumping to tackle this problem. In number theory and algebra, a Diophantine equation is an equation in which the variables represent integers, such as in the problem given above. The process of Vieta jumping entails rewriting a Diophantine equation in the form of a quadratic, and then using a known root of the quadratic, "jumping" to the other root of the quadratic using Vieta's formulas, from which useful information can be gleaned.

Vieta jumping is almost always used as a step in a proof by infinite descent, a number theory proof technique which utilizes the extremal principle to arrive at a contradiction. To generate a contradiction with infinite descent, we typically assume a solution is the smallest solution to a statement (by some definition of what makes a solution "small"), then proceed to show there must exist a smaller solution. This gives rise to the name "infinite descent", as we will always be able to "descend" to a smaller solution. To demonstrate this technique, below is a proof that $\sqrt{3}$ is irrational, using infinite descent.

1. As infinite descent is a proof by contradiction, we first assume that $\sqrt{3}$ is rational, and can be expressed as a fraction.

2. Let $\frac{a}{b}$ be the fraction equal to $\sqrt{3}$ *with the smallest numerator* (where a and b are integers).

3. Squaring $\sqrt{3}$ and $\frac{a}{b}$, we get $3 = \frac{a^2}{b^2}$.

4. Rearranging yields $3b^2 = a^2$, and thus a must be a multiple of 3. Let $a = 3c$ for some integer c. Substituting into the previous equation, we get $3b^2 = (3c)^2 = 9c^2$. Dividing by 3 yields $b^2 = 3c^2$.

5. This implies that b must also be a multiple of 3, so let $b = 3d$ for an integer d.

6. But this means $\sqrt{3} = \frac{a}{b} = \frac{3c}{3d} = \frac{c}{d}$ where $c < a$, contradicting the minimality of the numerator a. Thus, $\sqrt{3}$ must be irrational.

Vieta jumping can be used in a proof by infinite descent to generate a solution that is smaller than the assumed minimal solution (steps 4 and 5 above).

2 Introductory Vieta Jumping Problem

Before attempting the main problem I wanted to solve in this exploration, I started by solving an easier problem to get comfortable with Vieta jumping. This problem also demonstrates Vieta jumping in a context which is easier to understand.

Problem. Let (a, b) be an ordered pair of distinct positive integers. Prove that

$$\frac{a^2 + b^2}{ab}$$

is not an integer.

For the sake of contradiction, assume there exists some pair (a, b) such that $\frac{a^2+b^2}{ab}$ equals an integer k. We can write

$$\frac{a^2 + b^2}{ab} = k. \tag{1}$$

More specifically, let (a, b) be the solution to this equation, for a certain value of k, with the minimum sum, $a + b$. We can use Vieta jumping to show there must exist another solution to the equation for the same value of k whose sum is less than $a + b$, thus contradicting the minimality of (a, b). Since a and b are distinct and the two variables are symmetric (we can replace every occurrence of a with b, and vice versa, and still get the same equation), without loss of generality we can assume a is the larger number, or $a > b$. In this step, we could have equivalently assumed b is the larger number, or $a < b$. We can later note which inequality seems useful, then backtrack and use either inequality[1].

To proceed with Vieta jumping, the first step is to rewrite (1) as a quadratic. Rearranging

[1] Another way of thinking of this is as follows. If (a, b) is a solution, so is (b, a) by symmetry. Without loss of generality, let $a > b$. At a later step, we can choose to use either ordered pair (a, b) or (b, a), which is equivalent to using one solution (a, b) and later choosing which inequality to use.

(1) yields

$$\begin{aligned} a^2 + b^2 &= kab \\ a^2 - kab + b^2 &= 0. \end{aligned} \tag{2}$$

We can look at this Diophantine equation as a quadratic in a – replacing a with the variable x, we can define

$$f(x) = x^2 - kb(x) + b^2.$$

We know a is a root of this quadratic, since equation (2) tells us that $f(a) = 0$. Next, we can "jump" to the other root of $f(x)$ using Vieta's formulas, and gain useful information from this other root.

Let A be the other root of $f(x)$. Then, Vieta's formulas tell us that

$$\begin{aligned} a + A &= kb \\ aA &= b^2. \end{aligned} \tag{3}$$

From the first equation, we can deduce that A is an integer, since a and kb are both integers. The second equation (3) also tells us that A is positive. This means that (A, b) is also a valid solution to the Diophantine equation (1) for the same value of k. But we assumed that (a, b) was the minimal solution to this Diophantine equation for this value of k, so A must be greater than or equal to a.

From (3), it follows that

$$a^2 < aA = b^2,$$

and subsequently

$$a < b$$

since a and b are positive. Recall that, without loss of generality, we could have chosen to assume $a > b$ or $a < b$ at the start. We can choose to have assumed the inequality $a > b$, which contradicts the above inequality[2]. Hence, there are no minimal ordered pairs of distinct integers, (a, b), which satisfy $\frac{a^2+b^2}{ab} = k$ for any k. If there did exist 1 or more solutions such that $\frac{a^2+b^2}{ab}$ is an integer, then there would have to exist a minimal solution for that quotient. Since there are no minimal solutions, this implies that there must be no solutions entirely, proving the claim in the problem.

I also attempted several other problems which used Vieta jumping to gain experience using the technique to solve difficult problems.

3 Solving the Main Problem

Next, I began working on the advanced problem introduced at the start of the paper. To reiterate, the problem asks for all ordered pairs of positive integers (m, n) such that $mn - 1$ divides $\left(n^2 - n + 1\right)^2$. Note, I knew the solution to this problem utilized Vieta jumping in some way before I attempted it, which motivated some of the steps I took.

The first step I took was to set up a Diophantine equation, as before. Let (m, n) be a solution to the problem. Then, we can write

$$\frac{\left(n^2 - n + 1\right)^2}{mn - 1} = k$$

for some integer k. Multiplying both sides by $(mn - 1)$, we get

$$\left(n^2 - n + 1\right)^2 = k(mn - 1). \tag{4}$$

[2] Another way of thinking of this is that, if we chose to write the quadratic in terms of b, by symmetry we would arrive at the inequality $b > a$. Since we cannot have both $a > b$ and $a < b$, this is a contradiction.

3.1 Initial exploration

I first explored the problem by testing possible values of m and n. I wrote out the value of $\left(n^2-n+1\right)^2$ for $n=1,2,\ldots,20$:

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
$\left(n^2-n+1\right)^2$	1^2	3^2	7^2	13^2	21^2	31^2	43^2	57^2	73^2	91^2	111^2	133^2	157^2	183^2	211^2	241^2	273^2	307^2	343^2	381^2

I deliberately left the numbers in the bottom row in the form of a number squared, to better see if a certain factor divides the value. To satisfy the problem statement, there must exist a positive integer m such that $mn-1$ divides the corresponding number in the bottom row of the table. After extensive checking, the only possible ordered pairs for values of n from 1 to 20 were $(2,1)$, $(1,2)$, $(2,2)$, $(5,2)$, $(2,5)$, $(10,5)$, $(5,10)$, $(17,10)$ and $(10,17)$. For example, $(2,5)$ solves the problem condition because $mn-1=9$ and $\left(n^2-n+1\right)^2=(25-5+1)^2=21^2=441$, and 9 divides 441.

We can notice that, for any solution (m,n), the pair (n,m) is also a solution, which suggests there is some symmetry between m and n. Only taking the solutions where $m<n$, we have the 4 pairs $(1,2)$, $(2,5)$, $(5,10)$, and $(10,17)$. Notice that the value of n in one pair is the value of m in the next, suggesting that there might be a way to "jump" from one solution to the next, perhaps using Vieta jumping. This also suggests that there is an infinite family of solutions stemming from the minimal solution $(2,1)$. Knowing this turned out to be helpful, as I gained an idea of what to look for.

3.2 Blunt application of Vieta jumping

My first idea was to proceed similar to the introductory problem, bluntly applying Vieta jumping to this Diophantine equation. Notice the left hand side of (4), the expression $\left(n^2-n+1\right)^2$, is a degree 4 polynomial, as its expansion contains an n^4 term. From my experience with other Vieta jumping problems, I knew that it was nearly impossible to use Vieta jumping for a non-quadratic polynomial. This is because it is extremely difficult to show the other roots of the polynomial are positive integers as we did with the introductory problem. For the sake of completion, I made a brief attempt to use Vieta jumping on this degree 4 polynomial.

Rearranging and expanding, then writing the polynomial in terms of n yields

$$\begin{aligned}\left(n^2-n+1\right)^2-k(mn-1)&=n^4+n^2+1-2n^3-2n+2n^2-kmn-k\\&=n^4-2n^3+3n^2-(2+km)n+1-k\\&=0.\end{aligned}$$

As before, let

$$f(x)=x^4-2x^3+3x^2-(2+km)x+1-k,$$

and let the other three roots of this polynomial be n_1, n_2, and n_3. Using Vieta's formulas for the sum and products of the roots, we can write

$$\begin{aligned}n+n_1+n_2+n_3&=2\\nn_1n_2n_3&=1-k\end{aligned}$$

Although there are more complicated Vieta equations we could write, relating symmetrical polynomials of the roots with the coefficients of x^2 and x, the two equations above are enough to show that it would be extremely difficult to proceed with this approach. Both equations tell us that it is impossible for all 4 roots to be positive integers, which makes it very difficult to make any definitive and useful claims about the other three roots. Thus, I abandoned this approach relatively quickly.

3.3 Creating better opportunities for Vieta jumping

From my experience with other problems, I knew that Vieta jumping works best when dealing with a symmetrical Diophantine equation, with no powers greater than 2. A symmetrical equation means that two of the variables in the equation appear in the exact same way, such as equation (2) in the introductory problem. Having a symmetrical equation allows us to assume one variable is larger than or equal to the other, which is often very helpful as it was in the introductory problem. I had reason to believe that I could find a symmetric equation because of the symmetry in the solutions I found in my initial exploration. Also, having no powers greater than 2 would allow me to interpret the equation as a quadratic. Since equation (4) is not symmetric and contains higher powers, I looked to manipulate the problem condition to create an equation better suited for Vieta jumping.

The condition given in the problem is that $mn-1$ divides $\left(n^2-n+1\right)^2$. I looked to transform this condition into an equivalent condition which is better for Vieta jumping. For example, adding $mn-1$ to the dividend $\left(n^2-n+1\right)^2$ yields an equivalent condition: if $mn-1$ does not divide $\left(n^2-n+1\right)^2$, then $mn-1$ will also not divide $\left(n^2-n+1\right)^2+mn-1$; similarly, if $mn-1$ does divide $\left(n^2-n+1\right)^2$, then $mn-1$ will also divide $\left(n^2-n+1\right)^2+mn-1$. Note, this works with any multiple of $mn-1$ as well.

One property that stands out about the number $mn-1$ is that it is relatively prime to both m and n – in other words, it does not share any factors with m and n (other than 1). This is true because $mn-1$ is one away from mn, meaning there are no factors greater than 1 that $mn-1$ and mn could share. It follows that $mn-1$ also does not share any factors with m and n (if $mn-1$ did share a factor with m or n, that factor would also be shared with mn). This implies that multiplying the dividend $\left(n^2-n+1\right)$ by m or n is another action which yields an equivalent condition. If $mn-1$ does not divide $\left(n^2-n+1\right)$, then multiplying the dividend by a number which shares no factors with $mn-1$ will still result in a number not divisible by $mn-1$. Additionally, if $mn-1$ does divide $\left(n^2-n+1\right)^2$, then multiplying the dividend by any number, including m and n, will still yield a multiple of $mn-1$. Also note that this action is reversible – if the dividend is a multiple of m or n, we can divide the dividend by m or n to arrive at an equivalent condition.

Using these two actions, I was able to create a condition equivalent to the original condition, but which is better for Vieta jumping. The first step is to add $mn-1$ to the expression inside the parentheses, so the dividend becomes $\left(n^2-n+1+(mn-1)\right)^2 = \left(n^2-n+mn\right)^2$. Adding $mn-1$ inside the parentheses works because we are essentially just adding multiples of $(mn-1)$ to the dividend $\left(n^2-n+1\right)^2$, as we can see by expanding $\left(n^2-n+1+(mn-1)\right)^2$:

$$\left(\left(n^2-n+1\right)+(mn-1)\right)^2 = \left(n^2-n+1\right)^2 + 2\left(n^2-n+1\right)(mn-1)+(mn-1)^2.$$

Next, we might notice that each term inside the parentheses in the new dividend $\left(n^2-n+mn\right)^2$ is divisible by n. We can divide the dividend by n^2 (since the expression in the parentheses is squared) to get $(n-1+m)^2$, or $(m+n-1)^2$. Thus, our new equivalent condition is that $mn-1$ divides $(m+n-1)^2$. If an ordered pair (m,n) satisfies this condition, then it will also satisfy the original condition, and conversely if (m,n) does not satisfy this condition, then it will also not satisfy the original condition. This new dividend is much better for Vieta jumping, as it is a symmetrical expression and does not contain any powers greater than 2.

3.4 Vieta Jumping to solve the new condition

As before, assuming (m,n) satisfies this condition, we can write the Diophantine equation

$$\frac{(m+n-1)^2}{mn-1} = k \tag{5}$$

for some integer k. Note, the symmetry of m and n in the above equation implies that if (m,n) is a solution, then so is (n,m) – confirming our observation in the initial exploration. It would be useful to be able to assume, without loss of generality, one of the inequalities $m > n$ or $m < n$. However, we cannot do this yet as m could be equal to n. Thus, we will handle this case separately.

3.4.1 Solutions with $m = n$

If $m = n$, we need to find a positive integer m such that $m^2 - 1$ divides $(2m-1)^2 = 4m^2 - 4m + 1$. As before, we can manipulate this condition by subtracting the divisor, $m^2 - 1$, four times from the dividend, $4m^2 - 4m + 1$, to eliminate the m^2 term. This yields

$$4m^2 - 4m + 1 - 4(m^2 - 1) = 5 - 4m.$$

Thus, the new equivalent condition is that $m^2 - 1$ divides $5 - 4m$.

Next, unless $m = 1$, the expression $5 - 4m$ will be negative. If $m = 1$, we get $m^2 - 1 = 0$, which clearly cannot divide the dividend. Thus, m must be at least 2. Then, $5 - 4m$ is negative, so we can use the positive difference $4m - 5$ instead.

If m is a solution to this condition, the quotient

$$\frac{4m - 5}{m^2 - 1}$$

must be at least 1, since it is the integer quotient of two positive values. We can write

$$\begin{aligned} \frac{4m-5}{m^2-1} &< \frac{4m-4}{m^2-1} \\ &= \frac{4(m-1)}{(m+1)(m-1)} \\ &= \frac{4}{m+1}. \end{aligned}$$

Thus, $\frac{4}{m+1}$ must be strictly greater than 1. We have

$$\begin{aligned} \frac{4}{m+1} &> 1 \\ 4 &> m + 1 \\ m &< 3, \end{aligned}$$

which means m has to be 2 (we already checked $m = 1$). When $m = 2$, we have $\frac{4m-5}{m^2-1} = \frac{8-5}{4-1} = \frac{3}{3}$, which is clearly an integer. This means that, when $m = n$, the only pair which satisfies the condition given in the problem is $\boxed{(2, 2)}$.

3.4.2 Minimal solutions with $m \neq n$ (using Vieta jumping)

Next, we can consider solutions with $m \neq n$. I will first find all possible minimal solutions, then use the minimal solution(s) to generate all possible solutions in the next section. We can now assume, without loss of generality, that one of m and n is larger than the other, since the condition we wish to satisfy – that $mn - 1$ divides $(m + n - 1)^2$ – is symmetrical. As in the introductory problem, we can keep this fact in mind and later choose to use $m > n$ or $m < n$, depending on which inequality will be more useful.

We can rearrange equation (5) as

$$(m + n - 1)^2 = k(mn - 1).$$

Let (m, n) be a solution of this equation for some k. Furthermore, let (m, n) have the minimum sum $m+n$ for solutions with this value of k. Expanding and moving terms to the left hand side, we get

$$m^2 + n^2 + 1 + 2mn - 2m - 2n - kmn + k = 0.$$

As before, we can now employ Vieta jumping, by treating this equation as a quadratic in m:

$$m^2 + (2n - 2 - kn)m + n^2 - 2n + 1 + k = 0,$$

which can be written as

$$m^2 + (2n - 2 - kn)m + (n - 1)^2 + k = 0. \tag{6}$$

Let

$$f(x) = x^2 + (2n - kn - 2)x + (n-1)^2 + k. \tag{7}$$

We already know that m is a root of $f(x)$. Let the other root of $f(x)$ be M. Then, from Vieta's formulas, we know that

$$\begin{aligned} m + M &= kn + 2 - 2n \qquad (8) \\ mM &= (n-1)^2 + k. \end{aligned}$$

Similar to the introductory problem, the first equation tells us that M is an integer, and the second equation tells us that M is positive. Therefore, if (m, n) is a solution to the problem for a certain value of k, then (M, n) is also a solution for the same value of k. Similar to the introductory problem, we know that $M \geq m$ because we assumed (m, n) is the minimal solution for this value of k.

In the introductory problem, we were able to glean useful information from Vieta's formula for the product of the roots (equation (3)) because it related three variables – the variables of the minimal solution, a and b, and the other root of the quadratic, A. However, the two Vieta equations above both contain a fourth variable k. Therefore, I looked to eliminate k by multiplying the second equation by n, and subtracting the two equations.

$$\begin{aligned} mMn &= n(n-1)^2 + kn \\ mMn - (m + M) &= n(n-1)^2 + kn - (kn + 2 - 2n) \\ mMn - m - M &= n(n-1)^2 + 2n - 2 \\ &= n(n-1)^2 + 2(n-1) \\ &= (n-1)(n(n-1) + 2) \\ &= (n-1)\left(n^2 - n + 2\right). \qquad (9) \end{aligned}$$

This is an equation relating the desired three variables, but it is relatively complicated, which makes it difficult to extract useful information. Again looking at the equation (3) from introductory problem, we might notice that it is easy to use this equation because both the left and right hand sides are in the form of a product. Returning to equation (9), I realized that it was not just the complexity, but the sum of various terms on the left hand side which truly made it difficult to use an inequality with this equation as I was able to do with the introductory problem. Thus, I looked to somehow transform equation (9) such that both sides are a product.

The right hand side is already factored, so I first focused on the left hand side, $mMn - m - M$. My first thought about this expression was that it was reminiscent of the expansion of $(m-1)(M-1)$, which is

$$mM - m - M + 1.$$

This led me to try a technique commonly called Simon's Favorite Factoring Trick (SFFT), sometimes referred to as completing the rectangle, which is useful when an expression almost matches a certain factorable expression. When using SFFT to factor an expression, we typically try to add a constant to both sides of an equation to make one side factorable.

We cannot simply add 1 to both sides to match the expansion of $(m-1)(M-1)$ – the left hand side of (9) would become $mMn - m - M + 1$, not $mM - m - M + 1$. More advanced versions of SFFT also include multiplying both sides by the same constant, or raising both sides to the same power. After some experimentation, I figured out multiplying both sides of (9) by n gives an expression that is much closer to being factorable:

$$mMn^2 - mn - Mn = n(n-1)\left(n^2 - n + 2\right). \tag{10}$$

The left hand side is very close to the expansion of $(mn-1)(Mn-1)$, which is

$$mMn^2 - mn - Mn + 1.$$

We can now use standard SFFT, adding 1 to both sides of (10) to get

$$\begin{aligned} mMn^2 - mn - Mn + 1 &= n(n-1)\left(n^2 - n + 2\right) + 1 \\ (mn-1)(Mn-1) &= n(n-1)\left(n^2 - n + 2\right) + 1. \end{aligned} \tag{11}$$

Next, I worked on factoring the right hand side of (11). I noticed that if I expanded the first $n(n-1)$, I would get the product of two very similar expressions.

$$n(n-1)\left(n^2 - n + 2\right) + 1 = \left(n^2 - n\right)\left(n^2 - n + 2\right) + 1.$$

The first product contains two terms which have a difference of 2. As a general multiplication trick, I already knew that the product of two numbers, each 1 above and below a central number, is equal to 1 less than the middle number squared (e.g. $4 \cdot 6 = 24$ is 1 less than $5^2 = 25$). Therefore, I knew the first product should be 1 less than $\left(n^2 - n + 1\right)^2$, which when added to 1 will become just $\left(n^2 - n + 1\right)^2$, which interestingly is the original expression given in the problem! This can be proven by expanding the product as a difference of squares:

$$\begin{aligned} \left(n^2 - n\right)\left(n^2 - n + 2\right) + 1 &= \left(\left(n^2 - n + 1\right) - 1\right)\left(\left(n^2 - n + 1\right) + 1\right) + 1 \\ &= \left(n^2 - n + 1\right)^2 - 1^2 + 1 \\ &= \left(n^2 - n + 1\right)^2. \end{aligned}$$

Equation (9) can thus be rewritten as

$$(mn-1)(Mn-1) = \left(n^2 - n + 1\right)^2, \tag{12}$$

an equation which is much easier to extract useful information from.

Now, finally we can use either the inequality $m > n$ or $m < n$ to solve this Diophantine equation. Since we know that $M \geq m$, it logically follows to use the inequality $m > n$, as it allows us to relate all three variables with the inequality $M \geq m > n$.

This means that the left hand side of (12) has a lower bound

$$(mn-1)(Mn-1) > (n^2-1)(n^2-1) = (n^2-1)^2,$$

and subsequently

$$(n^2-1)^2 < \left(n^2-n+1\right)^2. \tag{13}$$

From here, it is tempting to simply remove the squares on both sides and write

$$n^2-1 < n^2-n+1,$$

but this is only correct if n^2-1 and n^2-n+1 are both positive. We can complete the square on the expression n^2-n+1, which yields

$$\left(n-\frac{1}{2}\right)^2+\frac{3}{4},$$

which is clearly positive for any n. However, the expression n^2-1 can be 0 when $n=1$ (this is the only possibility since n must be a positive integer). Thus, we must treat this case separately.

Case 1: $n=1$. Returning to our original condition, expressed in equation (5), we can rewrite the left hand side as

$$\frac{(m+1-1)^2}{m(1)-1} = \frac{m^2}{m-1}.$$

Recall that this fraction must be an integer to solve the original problem. Since $m-1$ and m are relatively prime, so are $m-1$ and m^2. Thus, for $m-1$ to evenly divide m^2, we must have $m-1=1$ and thus $m=2$. This gives the solution $\boxed{(2,1)}$. This was indeed the minimal solution predicted by my initial exploration, which is further evidence that this is correct.

Case 2: $n \neq 1$. We must have $n \geq 2$ (since n is a positive integer), and thus both $n^2 - 1$ and $n^2 - n + 1$ are positive. Hence, we can simply remove the squares from both sides of (13):

$$n^2 - 1 < n^2 - n + 1.$$

We can subtract n^2 from both sides:

$$-1 < -n + 1,$$

and equivalently

$$n < 2.$$

Clearly, this inequality is impossible for $n \geq 2$. Therefore, there exist no minimal solutions when $n \neq 1$, for any value of k.

From these two cases, we can deduce that the only minimal solution with $m \neq n$ and $m > n$ is $(2, 1)$, for $k = \frac{(m+n-1)^2}{mn-1} = \frac{4}{1} = 4$. Note that $(1, 2)$ is also a valid minimal solution, since we assumed $m > n$ without loss of generality. This implies that 4 is the only possible value of k for all solutions with $m \neq n$ (no other value of k has a minimal solution, so solutions with other values of k must not exist).

3.4.3 Vieta jumping to find all solutions of the new condition

In my initial exploration, I discovered that there likely exists an infinite family of solutions with $m > n$, with some kind of connection between each pair of consecutive solutions. Using the process of Vieta jumping described above, for any solution (m, n), we can generate another solution (M, n). Vieta's formula for the sum of the roots, equation (8), tells us that

$$m + M = kn + 2 - 2n = 2n + 2$$

since k must be 4, and thus

$$M = 2n + 2 - m. \tag{14}$$

This allows us to generate a new solution (M, n) from (m, n). For example, starting from the solution $(10, 5)$, we can generate the solution $(2(5) + 2 - 10, 5) = (2, 5)$, which is another valid solution. However, since m and M are roots of the quadratic given in equation (7), there are no other values x for which (x, n) is a solution of the problem. We can generate further solutions by flipping the newly generated solution (M, n) to get another solution (n, M), and then repeating the Vieta jumping process. This allows us to chain together Vieta jumping steps to generate many solutions from a single one. To summarize, this algorithm to generate solutions is as follows.

1. Find an existing solution (m, n).
2. Use Vieta jumping to generate a new solution (M, n), where $M = 2n + 2 - m$.
3. Switch the order of (M, n), to get the ordered pair (n, M). This is also a solution because the condition given in the problem was shown to be equivalent to a symmetrical condition.
4. Repeat, using (n, M) as the initial solution.

For example, we can start from the solution $(17, 10)$ and use this algorithm to generate the following solutions, terminating when we reach the minimal solution. We have

$$(17, 10) \mapsto (5, 10) \mapsto (10, 5) \mapsto (2, 5) \mapsto (5, 2) \mapsto (1, 2).$$

We can also reverse this process, starting from the minimal solution $(1, 2)$. For simplicity, I skipped the steps which just switched the order of the pair.

$$(1, 2) \mapsto (2, 5) \mapsto (5, 10) \mapsto (10, 17) \mapsto (17, 26) \mapsto (26, 37) \mapsto \cdots \tag{15}$$

Since we proved by infinite descent that $(2, 1)$ and $(1, 2)$ are the only minimal solutions for $m \neq n$, the solutions generated by this algorithm, using $(1, 2)$ as the first solution, account for every possible solution when $m \neq n$.

3.5 Final answer

Finally, I tried to write an algebraic expression for the kth term in the sequence given in (15). I first looked at just the numbers present in the sequence (15):

$$1, 2, 5, 10, 17, 26, 37, \ldots.$$

We might notice that this is a quadratic sequence, because the difference between consecutive terms forms an arithmetic sequence $1, 3, 5, 7, 9, 11, \ldots$. Knowing this, I was able to spot that each number is 1 greater than the kth perfect square. Thus, the kth term in the sequence is $k^2 + 1$, where the first number is actually the 0th term. Therefore, we can conjecture that the kth solution in the sequence (15) is

$$S_k = \left(k^2 + 1, (k + 1)^2 + 1\right) \tag{16}$$

I proceeded to prove this was true using induction.

We can verify that, for $k = 0$, this holds true, as (16) becomes $(0^2+1, (1)^2+1) = (1, 2)$, which is the 0th term of the sequence (15). Next, I will show that if performing our algorithm once on S_k results in S_{k+1}. The first step is to apply Vieta jumping to the solution S_k. The new value M is equal to $2\left((k + 1)^2 + 1\right)+2-\left(k^2 + 1\right) = 2k^2+4k+2+2+2-k^2-1 = k^2+4k+5 = (k+2)^2+1$. This means the solution generated by Vieta jumping is $\left((k + 2)^2 + 1, (k + 1)^2 + 1\right)$. The next step of the algorithm is to swap the two values in the ordered pair. This yields the ordered pair $\left((k + 1)^2 + 1, (k + 2)^2 + 1\right)$, which is indeed S_{k+1}. Therefore, if S_k is equal to the kth term in the sequence (15), the next term S_{k+1} will also match the $(k + 1)$th term of (15), since both are equal to the value produced by performing our algorithm on S_k. Thus, (16) accurately describes the sequence (15).

This means that all solutions with $m \neq n$ are of the form

$$\boxed{\left(k^2+1,(k+1)^2+1\right)}$$

or

$$\boxed{\left((k+1)^2+1,k^2+1\right)}$$

for $k = 0, 1, 2, \ldots$. Recall that we also had a single solution, $\boxed{(2,2)}$, when $m = n$. These encompass all the possible ordered pairs (m, n) such that $mn - 1$ divides $\left(n^2 - n + 1\right)^2$.

I was able to verify this result using a computer for $m, n \leq 10^4$. I first found all solutions for $m, n \leq 10^4$, then checked if each solution was of the form $\left(k^2+1,(k+1)^2+1\right)$ or $\left((k+1)^2+1,k^2+1\right)$, or if the solution was $(2, 2)$. The computer found that indeed all the solutions fit into one of these 3 categories. I then verified that $(2, 2)$ was a solution, and that $\left(k^2+1,(k+1)^2+1\right)$ and $\left((k+1)^2+1,k^2+1\right)$ were actually solutions for every value of $k \leq 10^4$. The computer again confirmed that these ordered pairs all satisfied the problem condition. The full code can be found in Appendix A.

4 Conclusion

Vieta jumping is a technique which cleverly utilizes Vieta's formulas for the sum and product of the roots of a polynomial to solve Diophantine equations in number theory. I solved some introductory problems, managing to gain some more experience with the technique. Then, I attempted to solve a very challenging problem from the 2009 USA Team Selection Test. In the introductory problem, I showed how Vieta jumping can be used as a part of a proof by infinite descent, by assuming an existing solution is minimal, and generating a new solution which contradicts the minimality of the existing solution. In the more challenging problem, we first needed to transform the problem condition such that we could use Vieta jumping. Then, we used Vieta jumping and infinite descent to find a significant constraint on any minimal solutions (recall there was a possible minimal solution for each value of the quotient k) – indeed, we found that there was only 1 possible minimal solution, when the quotient k was equal to 4. This allowed us to show that all solutions must have the same quotient of 4, and then we again used Vieta jumping to generate an infinite family of solutions stemming from the single minimal solution.

In this way, Vieta's formulas, which typically describe a relation between continuous variables, can be cleverly applied to solve Diophantine equations and various number theory problems. Traditionally, analyzing the roots and coefficients of a continuous function such as a polynomial is very separate from discrete mathematics and number theory. Much of modern math research is similarly concerned with connecting entirely separate fields of math. The most well-known example of this is the Langlands Program, which seeks to relate traditionally isolated areas of math such as number theory and geometry, and possibly find some underlying structures connecting different mathematical fields of study. Wiles' famous proof of Fermat's Last Theorem, which states that there are no solutions to the Diophantine equation $x^p + y^p = z^p$ for $p \geq 3$, is a great example of connecting a discrete number theory problem with tools usually associated with continuous variables. The key steps boil down to showing that rational elliptical curves and modular forms are identical mathematical objects (the Taniyama-Shimura-Weil conjecture), and that an integer solution of $x^p + y^p = z^p$ with $p \geq 3$ would imply the existence of an elliptical curve which was not modular (Ribet's theorem) – a contradiction. Modular forms belong to the field of complex analysis, the analysis of functions with complex inputs and outputs, but Wiles' proof exemplifies how they can be used to prove conjectures in number theory. The use of an algebraic tool such as Vieta's formulas to solve challenging number theory problems is somewhat reminiscent of this kind of modern math research.

Appendices

A Computer Code

I wrote my code in Python. Imports and function definitions:

```python
import math


def is_solution(m: int, n: int) -> bool:
    divisor = m * n - 1
    dividend = (n ** 2 - n + 1) ** 2
    try:
        return not bool(dividend % divisor)
    except ZeroDivisionError:
        return False
```

Checking that all solutions (m,n) with $m,n \leq 10^4$ are of the form $\big(k^2+1,(k+1)^2+1\big)$ or $\big(k^2+1,(k+1)^2+1\big)$, other than $(2,2)$:

```python
for m in range(1, 10 ** 4 + 1):
    for n in range(1, 10 ** 4 + 1):
        if is_solution(m, n):
            if m == n == 2:
                continue

            small = min(m, n)
            big = max(m, n)
            k = math.isqrt(small - 1)  # Same as int(math.sqrt(small - 1))
            if small == k ** 2 + 1 and big == (k + 1) ** 2 + 1:
                continue

            print(f"Solution ({m}, {n}) is not of one of the three predicted forms.")

print("Done")
```

Output:

```
Done
```

Checking that $(2, 2)$ is a solution, and that $\big(k^2 + 1, (k + 1)^2 + 1\big)$ and $\big(k^2 + 1, (k + 1)^2 + 1\big)$ are solutions for all values of k up to 10^4:

```
if not is_solution(2, 2):
    print(f"(2, 2) is not a solution")

for k in range(10 ** 4):
    small, big = k ** 2 + 1, (k + 1) ** 2 + 1
    if not is_solution(small, big):
        print(f"Predicted solution ({small}, {big}) with k = {k} is not a
                                        solution.")
        continue
    elif not is_solution(big, small):
        print(f"Predicted solution ({big}, {small}) with k = {k} is not a
                                        solution.")
        continue

print("Done")
```

Output:

```
Done
```

Both programs verified my final answer was correct, for $m, n, k \leq 10^4$.