E29: On the solution of Diophantine problems in whole numbers
Euler, Sarah Fujimori

When we encounter an equation of the form $ax^2 + bx + c = y^2$, we often find that there are no solutions. For example, since squares are always 0 or 1 mod 3, the equation $3x^2 + 2 = y^2$ has no solution. However, if we can come up with one solution to this equation, then Euler shows that there are infinitely many other solutions that follow from that one.

In this paper, Euler excludes cases where a is equal to a square, since it is more difficult to make $ax^2 + bx + c$ equal to a square when it is already very close to one.

1. FINDING ANOTHER SOLUTION

Let the ordered pair (n, m) satisfy the equation $ax^2 + bx + c = y^2$. We set the next solution equal to $(\alpha n + \beta + \gamma m, \delta n + \epsilon + \zeta m)$. We plug these values into the $ax^2 + bx + c = y^2$ and obtain the following expression on the left side, organized by powers of n and m:

$$\begin{gathered} a\alpha^2 n^2 + \alpha^2\gamma^2 n^2 \\ +2a\alpha\beta n + ab\gamma^2 n + b\alpha n \\ +a\beta^2 + ac\gamma^2 + b\beta + c \\ +2a\alpha\gamma nm \\ +2a\beta\gamma m + b\gamma m \end{gathered}$$

On the right side, we have:

$$\begin{gathered} \delta^2 n^2 + a\zeta^2 n^2 \\ +2\delta\epsilon n + b\zeta^2 n \\ +\epsilon^2 + c\zeta^2 \\ +2\delta\zeta nm \\ +2\epsilon\zeta m \end{gathered}$$

When we set these two expressions equal to each other, we can compare coefficients and obtain the following system of equations:

$$\begin{gathered} a\alpha^2 + \alpha^2\gamma^2 = \delta^2 + a\zeta^2 \\ 2a\alpha\beta + ab\gamma^2 + b\alpha = 2\delta\epsilon + b\zeta^2 \\ a\beta^2 + ac\gamma^2 + b\beta + c = \epsilon^2 + c\zeta^2 \\ 2a\alpha\gamma = 2\delta\zeta \\ 2a\beta\gamma + b\gamma = 2\epsilon\zeta \end{gathered}$$

We start at the fourth equation, since it is the most simple. Dividing both sides by 2ζ gives us $\delta = \frac{a\alpha\gamma}{\zeta}$. Next, in the last equation, we divide both sides by 2ζ, giving us $\epsilon = \frac{2a\beta\gamma + b\gamma}{2\zeta}$.

We now use our expression for δ to simplify the first equation:

$$\begin{gathered} a\alpha^2 + \alpha^2\gamma^2 = \delta^2 + a\zeta^2 \\ a\alpha^2 + \alpha^2\gamma^2 = \frac{a^2\alpha^2\gamma^2}{\zeta^2} + a\zeta^2 \end{gathered}$$

We multiply by ζ^2 to get rid of the fraction, and then rearrange and group terms to factor:

$$a\alpha^2\zeta^2 + a^2\gamma^2\zeta^2 = a^2\alpha^2\gamma^2 + a\zeta^4$$
$$a\alpha^2\zeta^2 + a^2\gamma^2\zeta^2 - a^2\alpha^2\gamma^2 - a\zeta^4 = 0$$
$$a\alpha^2\zeta^2 - a\zeta^4 - a^2\alpha^2\gamma^2 + a^2\gamma^2\zeta^2 = 0$$
$$a\zeta^2(\alpha^2 - \zeta^2) - a^2\gamma^2(\alpha^2 - \zeta^2) = 0$$
$$(a\zeta^2 - a^2\gamma^2)(\alpha^2 - \zeta^2) = 0$$

From this equation we see that one of these two quantities must be 0. Specifically, $\alpha^2 = \zeta^2$ or $\zeta^2 = a\gamma^2$. However, we mentioned earlier that we exclude cases where a is a perfect square; therefore, it is impossible for $a\gamma^2$ to be equal to a square. Thus, we take $\alpha^2 = \zeta^2$ to be true, and if we square root both sides, we have $\alpha = \zeta$.

If we substitute this value into our expression for δ, then we get $\delta = a\gamma$.

We now substitute all of these values into the second equation:

$$2a\alpha\beta + ab\gamma^2 + b\alpha = 2(a\gamma)(\tfrac{2a\beta\gamma + b\gamma}{2\alpha}) + b\alpha^2$$

To clear denominators, we multiply by α, and then rearrange and group terms like before:

$$2a\alpha^2\beta + a\alpha b\gamma^2 + b\alpha^2 = (a\gamma)(2a\beta\gamma + b\gamma) + b\alpha^3$$
$$2a\alpha^2\beta + a\alpha b\gamma^2 + b\alpha^2 = 2a^2\beta\gamma^2 + ab\gamma^2 + b\alpha^3$$
$$b\alpha^3 - 2a\alpha^2\beta - b\alpha^2 = a\alpha b\gamma^2 - 2a^2\beta\gamma^2 - ab\gamma^2$$
$$\alpha^2(b\alpha - 2a\beta - b) = a\gamma^2(b\alpha - 2a\beta - b)$$
$$(\alpha^2 - a\gamma^2)(b\alpha - 2a\beta - b) = 0$$

From this equation, we again obtain two possibilities: either $\alpha^2 = a\gamma^2$ or $b\alpha - 2a\beta - b = 0$. As before, we have excluded cases where a is a square, so $a\gamma^2$ cannot be a perfect square. Solving the second equation for β gives $\beta = \frac{b(\alpha-1)}{2a}$.

We now simplify our expression for ϵ: $\frac{\frac{2a\gamma b(\alpha-1)}{2a} + b\gamma}{2\zeta} = \frac{\alpha\gamma b - \gamma b + b\gamma}{2\alpha} = \frac{b\gamma}{2}$.

Now, we work with the third equation. We start by separating the terms with c from the terms without it:

$$a\beta^2 + ac\gamma^2 + b\beta + c = \epsilon^2 + c\zeta^2$$
$$\epsilon^2 - a\beta^2 - b\beta = c\alpha^2 - ac\gamma^2 - c$$

We now substitute all of our values into this equation:

$$(\tfrac{b\gamma}{2})^2 - \tfrac{ab^2(\alpha-1)^2}{4a^2} - \tfrac{b^2(\alpha-1)}{2a} = c(\alpha^2 - a\gamma^2 - 1)$$

We add the fractions using the common denominator $4a$:

$$\tfrac{b^2\gamma^2}{4} - \tfrac{\alpha^2b^2 - 2\alpha b^2 + b^2}{4a} - \tfrac{b^2\alpha - b^2}{2a} = c(\alpha^2 - a\gamma^2 - 1)$$
$$\tfrac{ab^2\gamma^2 - \alpha^2b^2 + 2\alpha b^2 - b^2 - 2b^2\alpha + 2b^2}{4a} = c(\alpha^2 - a\gamma^2 - 1)$$
$$\tfrac{ab^2\gamma^2 - \alpha^2b^2 + b^2}{4a} = c(\alpha^2 - a\gamma^2 - 1)$$
$$\tfrac{b^2}{4a}(-\alpha^2 + a\gamma^2 + 1) = c(\alpha^2 - a\gamma^2 - 1)$$
$$(c - \tfrac{b^2}{4a})(\alpha^2 - a\gamma^2 - 1) = 0$$

We are solving for values of α, β, γ, etc., not a, b, c, so we conclude that $\alpha^2 - a\gamma^2 - 1 = 0$. If we solve for α, we get that $\alpha = \sqrt{a\gamma^2 + 1}$.

We now make new variables p and q such that $q = sqrtap^2 + 1$. Then, $\alpha = q, \beta = \frac{b(q-1)}{2a}, \gamma = p, \delta = ap, \epsilon = \frac{bp}{2}$, and $\zeta = q$. Substituting these values into our original ordered pair, we obtain the following theorem:

Theorem 1 *If the solution (n, m) satisfies the equation $ax^2 + bx + c = y^2$, then the solution $(qn + \frac{bq-b}{2a} + pm, apn + \frac{bp}{2} + qm)$ does too.*

2. GENERATING A SEQUENCE OF SOLUTIONS

Using Theorem 1, we can generate an infinitely long sequence of solutions. To do this, we treat $qn + \frac{bq-b}{2a} + pm$ as the new value of n, and $apn + \frac{bp}{2} + qm$ as the new value of m.

Therefore, our next value of n would be $q(qn + \frac{bq-b}{2a} + pm) + \frac{bq-b}{2a} + p(apn + \frac{bp}{2} + qm)$. Simplifying,

$$\begin{gathered} q^2n + \tfrac{bq^2-bq}{2a} + pqm + \tfrac{bq-b}{2a} + ap^2n + \tfrac{bp^2}{2} + pqm \\ = q^2n + ap^2n + 2pqm + \tfrac{bq^2-b}{2a} + \tfrac{bap^2}{2a} \\ = q^2n + ap^2n + 2pqm + \tfrac{bq^2-b+bap^2}{2a} \end{gathered}$$

To make this expression look a little nicer, we can use the fact that $q^2 = ap^2 + 1$:

$$\begin{gathered} 2ap^2n + n + 2pqm + \tfrac{bap^2+b-b+bap^2}{2a} \\ = 2q^2n - n + 2pqm + bp^2 \end{gathered}$$

We do the same for m:

$$\begin{gathered} m = ap(qn + \tfrac{bq-b}{2a} + pm) + \tfrac{bp}{2} + q(apn + \tfrac{bp}{2} + qm) \\ = apqn + \tfrac{bpq-bp}{2} + ap^m + \tfrac{bp}{2} + apqn + \tfrac{bpq}{2} + q^m \\ = 2apqn + bpq + ap^m + q^m \\ = 2apqn + bpq + 2q^m - m \end{gathered}$$

If we want, we can extend these sequences to be as long as we want. Below, we list the first few solutions that are generated using this method:

$$\begin{gathered} 1.(n, m) \\ 2.(qn + pm + \tfrac{b(q-1)}{2a}, apn + qm + \tfrac{bp}{2}) \\ 3.(2q^2n + 2pqm + \tfrac{b(q^2-1)}{a} - n, 2apqn + 2q^2m + bpq - m) \\ 4.(4q^3n + 4pq^2m + \tfrac{b(4q^3-3q-1)}{2a} - 3qn - pm, 4apq^2n + 4q^3m + 2bpq^2 - apn - 3qm - \tfrac{bp}{2}) \\ 5.(8q^4 + 8pq^3m + \tfrac{4bq^2(q^2-1)}{a} - 8qn^2 - 4pqm + n, 8apq^3n + 8q^4m + 4bpq^3 - \\ 4apqn - 8q^2m - 2bpq + m) \end{gathered}$$

Let the kth x value be x_k, and let the kth y value by y_k. We notice by looking at these terms that $x_3 = 2qx_2 - x_1 + \frac{b(q-1)}{a}$. We can generalize to $x_{k+2} = 2qx_{k+1} - x_k + \frac{b(q-1)}{a}$ because the theorem we developed is also a recursion, and we can treat any term as n and use our method to generate the next one.

Similarly, for y values, $y_{k+2} = 2qy_{k+1} - y_k$.

We see from looking at these x and y values that not all of these solutions are whole number solutions. In the values of y, the term $\frac{bp}{2}$ shows up every other value, which means that at least every other y value is a whole number.

Looking at x values, the term $\frac{b(q-1)}{2a}$ or some multiple of it shows up in every other value, and in the values it does not appear in, there is a multiple of $\frac{b(q^2-1)}{a}$. We know that the former is not always an integer, and will be an integer when $2a$ divides $bq - b$. On the other hand, the latter is always an integer, because if we make the substitution $q^2 = ap^2 + 1$, it becomes equal to bp^2. Therefore, at least every other x term is an integer.

Additionally, the x terms that are guaranteed to be integers and the y terms that are guaranteed to be integers correspond, so we are guaranteed that at least every other ordered pair will be a whole number solution.

3. FINDING POSITIVE p, q

It remains now to find values of p and q such that $q^2 = ap^2 + 1$. We can see that one solution would be $p = 0, q = 1$. However, if we substitute these values into the sequences x_k and y_k, then both of the sequences contain only n's and m's, i.e. there are no new values. Consequently, we wish to find values of p and q that are positive integers.

Euler cites a special method for finding these values, which was created by Pell and Fermat and explained by Wallis. Therefore, he does not explain or prove it in the paper, but shows an example of how to use it, since it is useful in generating this sequence of solutions.

As an example, let $q^2 = 5p^2 + 1$. Then $q = \sqrt{5p^2 + 1}$. Since $sqrt4p^2 < \sqrt{5p^2 + 1}$, we know that $q > 2p$, so we set it equal to $2p + a$.

Now, we solve for p by equating the different expressions for q:

$$q = 2p + a = \sqrt{5p^2 + 1}$$

We square both sides and then move all terms to one side:

$$4p^2 + 4ap + a^2 = 5p^2 + 1$$
$$p^2 - 4ap + 1 - a^2 = 0$$

Now, we employ the quadratic formula to express p in terms of a:

$$p = \frac{4a \pm \sqrt{16a^2 + 4a^2 - 4}}{2} = \frac{4a \pm \sqrt{20a^2 - 4}}{2} = 2a \pm \sqrt{5a^2 - 1}$$

Note that there are two solutions to this equation. We take the one with plus, since we want positive integer solutions.

Next, we repeat the process. We know $2a + \sqrt{5a^2 - 1} > 2a + \sqrt{4a^2} = 4a$, so $p > 4a$, so then we set p equal to $4a + b$.

Again, we set the two known expressions of p equal to each other and solve for b:

$$p = 4a + b = 2a + \sqrt{5a^2 - 1}$$
$$2a + b = \sqrt{5a^2 - 1}$$
$$4a^2 + 4ab + b^2 = 5a^2 - 1$$
$$a^2 - 4ab - 1 - b^2 = 0$$
$$a = \frac{4b \pm \sqrt{16b^2 + 4b^2 + 4}}{2} = \frac{4b \pm \sqrt{20b^2 + 4}}{2} = 2b \pm \sqrt{5b^2 + 1}$$

Again, we take the greater solution only because we seek positive integer solutions. Therefore, $a = 2b + \sqrt{5b^2 + 1}$.

This is what we have been looking for, because now we can set b equal to 0, making a a positive integer. This gives $a = 1$, $p = 4$, and $q = 9$. Indeed, $9 = \sqrt{5 * 4^2 + 1} = \sqrt{81}$.

we can use this method for any value of a, and in fact, this method will give us the smallest positive integer solution for p and q (If we use our method of generating a sequence of solutions, then we can obtain higher values).

4. APPROXIMATING SQUARE ROOTS

If we manipulate the equation $q^2 = ap^2 + 1$ a bit to obtain the value of a, we will get that $a = \frac{q^2-1}{p^2}$. Then, if we square root both sides, $\sqrt{a} = \frac{\sqrt{q^2-1}}{p}$.

Given a value of a, we can find an infinite number of (p, q) that satisfy this condition. As p and q approach infinity, $\frac{\sqrt{q^2-1}}{p}$ will approach $\frac{q}{p}$, so a will be approximately $\frac{q}{p}$. This means that we can use both the method mentioned earlier and our sequence of solutions to $ax^2 + bx + c$ to approximate $\sqrt{a}$.

Let us first work with our previous example where $a = 5$. Based on the main theorem of our paper, $p_k = 2q(p_{k-1}) - p_{k-2}$, and $q_k = 2q(q_{k-1}) - q_{k-2}$. (Here, q is the value that we found using Pell and Fermat's method, namely 9). So, $p_k = 18(p_{k-1}) - p_{k-2}$, and $q_k = 18(q_{k-1}) - q_{k-2}$

We list out the different values of p and q. We know that $p = 0, q = 1$ is a solution, as well as $p = 4, q = 9$. Therefore, we can generate an infinitely long sequence of values for p and q using our method. The values we get for p are:

$$0, 4, 72, 1292, 23184, 416020 \cdots$$

And the values we get for q are:

$$1, 9, 161, 2889, 51841, 930249 \cdots.$$

If we divide the values of q by the corresponding values of p, $\frac{q}{p}$ gets closer to $\sqrt{a}$. Taking the last p and q values that we found, 416020 and 930249, then we get $\frac{q}{p} \approx 2.23606797750$. In comparison, $\sqrt{5} = 2.236067977749$, which shows that we have accuracy up to 10 digits! Not bad.

5. APPLICATION TO TRIANGULAR NUMBERS

Next, Euler applies this formula to find the triangular numbers that are squares. The xth triangular number is given as $\frac{x^2+x}{2}$, or $\frac{2x^2+2x}{4}$ if we multiply the top and bottom by 2. We see that if $\frac{2x^2+2x}{4}$ is a perfect square, then $2x^2 + 2x$ must

also be a square. We then solve for values of x that will make this expression a perfect square, and exclude the odd solutions so that the resulting triangular number will actually be an integer.

By comparing the expression with the generalized form $ax^2 + bx + c$, we see that $a = 2, b = 2$, and $c = 0$. Since $c = 0$, we know $x = 0$ is a solution, so we set $n = 0$.

We now find the values of p and q: if $q = \sqrt{2p^2 + 1}$, then $q > p$, so we let $q = p + a$ and solve for p in terms of a:

$$p + a = \sqrt{2p^2 + 1}$$

We square both sides and then move all terms to one side:

$$p^2 + 2ap + a^2 = 2p^2 + 1$$
$$p^2 - 2ap + 1 - a^2 = 0$$

Now, we use the quadratic formula to find p:

$$p = \frac{2a \pm \sqrt{4a^2 + 4a^2 - 4}}{2} = \frac{2a \pm \sqrt{8a^2 - 4}}{2} = a \pm \sqrt{2a^2 - 1}$$

As before, we take the larger solution with $+$ instead of $-$, because we are looking for positive integer solutions. Since the expression for p does not contain some form of $\sqrt{2k^2 + 1}$, we repeat the process:

Since $p > 2a$, we set it equal to $2a + b$. We now solve for b:

$$2a + b = a + \sqrt{2a^2 - 1}$$
$$a + b = \sqrt{2a^2 - 1}$$
$$a^2 + 2ab + b^2 = 2a^2 - 1$$
$$a^2 - 2ab - 1 - b^2 = 0$$
$$a = \frac{2b + \sqrt{4b^2 + 4b^2 + 4}}{2} = \frac{2b + \sqrt{8b^2 + 4}}{2} = b + \sqrt{2b^2 + 1}$$

Now, we can set $b = 0$, which gives $a = 1$, $p = 2$, and $q = 3$. Using these values, our recursions for x and y values are $x_k = 6x_{k-1} - x_{k-2} + 2$ and $y_k = 6y_{k-1} - y_{k-2}$. Additionally, by substituting numbers into the formula, we get that the next solution is $(1, 2)$.

If we continue generating solutions, the values of x will be:

$$0, 1, 8, 49, 288, 1681, 9800, \cdots$$

The values of y will be:

$$0, 1, 6, 35, 204, 1189, 6930, \cdots$$

Finally, we exclude the odd values of x, since $\frac{2x^2 + 2x}{4}$ wouldn't be a whole number.

6. POLYGONAL NUMBERS IN GENERAL

After applying his method to triangular numbers, Euler generalizes to polygonal numbers. The xth polygonal number of side s is given by the expression $\frac{(s-2)x^2-(s-4)x}{2}$. Like before, we conclude that if this is a square, then $2(s-2)x^2 - 2(s-4)x$ is also a square. We see that $(0,0)$ is a solution, and by comparing this to the general form ax^2+bx+c, we let $a = 2(s-2)$, $b = -2(s-4)$, and $c = 0$.

By substituting our values into the formula, the next values of x are:

$$0, \frac{-(s-4)}{2(s-2)}(q-1), \frac{-(s-4)}{s-2}(q^2-1), \cdots$$

where our usual definition of p and q applies, i.e. $2(s-2)p^2 + 1 = q^2$.

Unfortunately, if $s > 4$, then all of these terms are negative except for 0. However, we can replace q with $-q$ here because $2(s-2)p^2 + 1 = q^2$ will still hold. Then, every other term would become positive.

This gives us the following y values:

$$0, (s-4)p, 2(s-4)pq, \cdots$$

We can then solve for the values of p and q given s and substitute them into these sequences.

In the case where $2(s-2)$ is a perfect square, Euler claims that the polygonal numbers of side s are either all squares, or only a few of them are squares. For example, if $s = 4$, the square numbers are simply x^2, so all of them are squares. If $s = 10$ and $2(s-2) = 16$, then only the values 0 and 1 work for x.