An important nonlinear algebraic equation is the elliptic equation-

\[ y^2 = x^3 + ax + b \]

where \( a \) and \( b \) are specified real constants. The equation arises in a variety of areas including the factorization of large semi-primes and in the proof of Fermat’s last Theorem. We want in this note to discuss some of its more important properties.

First of all one notes that the symmetry about the x axis so that a given x will yield \( +y \) and \( -y \). Also there are real solutions only as long as the right hand side of the equation is positive. The transition points are given by the real roots of the reduced cubic-

\[ x^3 + ax + b = 0 \]

The derivative of the elliptic equation is-

\[ \frac{dy}{dx} = y' = \frac{3x^2 + a}{2y} \]

and so is independent of \( b \) and is infinite at \([x,y]=[-2,0]\).

Typically some of the solutions to the elliptic equation will be integer pairs \([x,y]\). We will denote these points as \( p_0=[x_0,y_0] \), \( p_1=[x_1,y_1] \), \( p_1=[x_1,-y_1] \) etc. An interesting point about elliptic equations is that a straight line passing through two integer pairs will often pass through a third integer pair as will be shown below.

Let us look at some specific forms beginning with-

\[ y^2 = x^3 - 2x + 4 \]

The graph of this equation looks as follows-
We can find the integer pairs using the search program

```
for n from -4 to 10 do {n,sqrt(n^3-2*n+4 )} od;
```

The lowest ones are \([x,\pm y]=\{-2,0\},[0,2],[3,5]\). I have marked them as blue circles in the graph. You will note the straight lines passing through \(p_0\) and either \(p_1\) or \(-p_1\). These intersect the third pair \(\pm p_2=[1,\pm 2]\). In a like manner a straight line through \(p_1\) and \(p_2\) may produce the pair \(p_3\). The line through \([0,2]\) and \([3,5]\) is \(y=x+2\). So performing the operation-

```
solve({y=x+1,y^2=x^3-2*x+4});
```

this produces the already stated three values of \(p_0, p_1,\) and \(p_2\) but nothing beyond these. To confirm this point we extended our search program to \(n=600\) and in agreement found no other integer pairs \([x, y]\).

We next looked at the equation-

\[
y^2 = x^3 - 6x + 9
\]

Its graph looks as follows-
Now to test if there are any extra integers possible beyond \( p_3 = [4,7] \), we draw a straight line between \(-p_1\) and \( p_2 \). Its equation is \( y = 5x - 3 \). To see if it intersects the elliptic curve we carry out-

\[
solve({y=5*x-3,y^2=x^3-6*x+9});
\]

It indeed yields a new pair \( p_4 = [24,117] \). To see if \( p_5 \) also exists we connect \(-p_2\) with \( p_3 \) and then solve-

\[
solve({y=3*x-5,y^2=x^3-6*x+9});
\]

This time the solution produces no new pair, so that no pairs exist greater than \([24,117]\). We also confirmed this by carrying out the search to \( n = 300 \) yielding no new integer pair.

Another elliptic equation reads-

\[
y^3 = x^3 - 5x - 8
\]

Four obvious integer solutions are \([3,\pm 2]\) and \([4,\pm 6]\). A straight line between \([3,-2]\) and \([4,6]\) reads \( y = 4x - 10 \). Its intersection with the elliptic equation occurs at-

\[
Solve({y=4x-10,y^2=x^3-5x-8})
\]

That is \([x,y] = [9,26]\) so that we get the extra two points \([9,\pm 26]\). Repeating the operation for the next possible integer pair, does not produce a pair but rather the non-integer value \([27.960,147.344]\). We can confirm this observation by carrying out-

\[
for\; x\; from\; 2\; to\; 50\; do\; \{x,\pm\sqrt{x^3-5x-8}\} od;
\]
This yields just \([3, \pm 2], [4, \pm 6], [9, \pm 26]\) and no other integer pair beyond these. Note that for this equation solutions can only exist for \(x \geq 2.80258\).

As a 4\(^{th}\) specific elliptic equation we consider-

\[y^2 = x^3 - 3x + 2\]

This is one of the most interesting elliptic forms possible. It resembles, but differs in detail, from both the classical Right Strophoid and the Tschirnhaus curves. Unlike other elliptic curves, it has an infinite number of integer pairs. The first few of these are as shown-

<table>
<thead>
<tr>
<th>N</th>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
</tr>
</thead>
<tbody>
<tr>
<td>[x,y]</td>
<td>-2,0</td>
<td>-1,2</td>
<td>1,0</td>
<td>2,2</td>
<td>7,18</td>
<td>14,52</td>
<td>23,110</td>
<td>34,198</td>
</tr>
</tbody>
</table>

Starting with \(n=3\), we observe that –

\[p(n+1) = p(n) + [2n-1, 3n^2-3n-2]\]

Thus \(p(8)\) will equal \([47, 322]\). Also with a bit more effort one finds-

\[p(n) = [x, y] = [n^2-2n-1, n^3-3n^2+2]\]

Thus \(p(10)\) has \([x, y] = [79, 702]\) and \(p(100)\) has \([x, y] = [9799, 970002]\). These integer pairs check exactly with the governing elliptic equation. Also we note the slope \(dy/dx\) is given by-

\[
\frac{dy}{dx} = \frac{3n(n-2)}{2(n-1)} \quad \text{when} \quad n \geq 3
\]

The solution has one zero at \(x=-2\) and a double root at \(x=1\). A graph of \(y^2=x^3-3x+2\) looks like this-
Real values for \( y \) exist only when \( x \geq -2 \) and the only infinite slope occurs at \( x = -2 \). This time a straight line between \([2,2]\) and a higher pair does not pass through a third pair. This equation may be of interest to those factoring large semi-primes using the Lenstra approach.

Related to this last equation one encounters the even simpler elliptic form:

\[
y^2 = x^3 - 1
\]

Its graph looks as follows:
There are just the five indicated integer pairs which are possible as shown by a search up to \(x=500\). The solution can exist only as long as \(x \geq -1\). It has zero slope at \(x=0\) and also an inflection point there.

U.H.Kurzweg  
October 19, 2019  
Gainesville, Florida