Chapter 4

Elliptic Curves and KdV Traveling Waves

As we saw in the previous chapter, the first mathematical step in the story of solitons was the discovery of the solitary wave solution to the KdV Equation. In this chapter, we will rediscover that solution by starting with the assumption that the solution is a fixed profile that simply translates in time and by making use of some algebraic geometry.

4.1 Algebraic Geometry

It was the observation of René Descartes that identifying an equation in the variables x and y with the set of points in the (x, y) whose coordinates satisfy the equation allows us to turn questions about some geometric figures into algebra problems. It is through this correspondence that every high school student immediately pictures the geometric form of a parabola upon seeing the equation $y = x^2$ and a circle of radius one when encountering $x^2 + y^2 = 1$. A slightly more interesting question is to consider the intersections of two such geometric objects, which algebraically would take the form of solving the two equations simultaneously.

More generally, algebraic geometry associates to a finite set of polynomials $\{p_1, \ldots, p_k\}$ in n variables the set of points in n-dimensional Euclidean space whose coordinates simultaneously satisfy all k equations $p_i = 0$. Pursuing Descartes' seemingly simple prescription in this way, one quickly is forced to deal with very abstract objects such as *projective spaces* (where there are no parallel lines) and *coordinate rings* (which are algebraic structures, such as those you might encounter in a course on abstract algebra).

We will only see hints of these more advanced concepts in this book, but it is important to realize that there is more to the algebraic geometry correspondence than simply the set of points satisfying an algebraic equation. As a prescient example, let us further consider the simple case of the circle $x^2 + y^2 = 1$ and the way in which it naturally has the algebraic structure of a *group*.

Example 4.1 Let p_1 and p_2 be points on the unit circle $x^2+y^2 = 1$. We can then find numbers θ_1 and θ_2 such that $p_i = (\cos(\theta_i), \sin(\theta_i))$. Using this, we can define an algebraic structure on the circle that allows us to add points to get other points. Define their "sum" as $p_3 = p_1 + p_2$ by

$$p_3 = (\cos(\theta_1 + \theta_2), \sin(\theta_1 + \theta_2)).$$

Show that this gives the circle the structure of a *group*, namely that this binary operation is well defined, has an identity element, and that every element has an inverse.

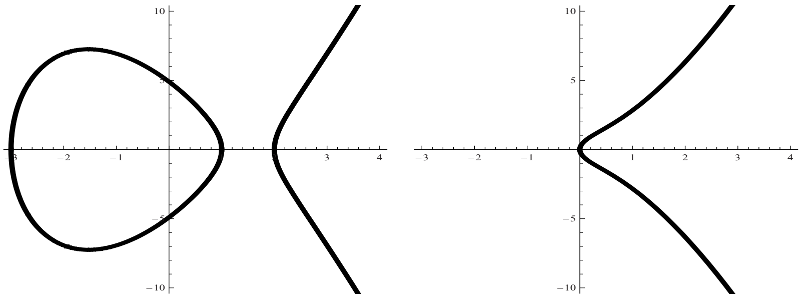
Solution This definition depends on the (elementary) fact that each point on the circle *can* be written in the form $(\cos(\theta), \sin(\theta))$ for some number θ. (For better comparison to the case of elliptic curves in the next section, it might be wise to think of this as $(f(\theta), -f'(\theta))$ where $f(x) = \cos(x)$.) Of course, there is not a unique value of θ corresponding to any given point on the circle as adding any integer multiple of 2π to the size of the angle leaves the point unchanged. However, this does not lead to any problems in the definition of this binary operation as changing θ_1 and θ_2 each by some integer multiple of 2π will not change the corresponding p_3 either.

Essentially, this group structure just takes two points on the circle and associates to them the angle that they make with the point $(1, 0)$ (up to addition by an arbitrary integer multiple of 2π). The sum adds together those two angles (again, modulo 2π). Thus, the point $(1, 0)$ is the identity element and the inverse of any point is its reflection through the x-axis.

4.2 Elliptic Curves and Weierstrass $\wp$-functions

Almost as famous as the circle is the curve with the equation

$$y^2 = 4x^3 - k_1x - k_2, \tag{4.1}$$



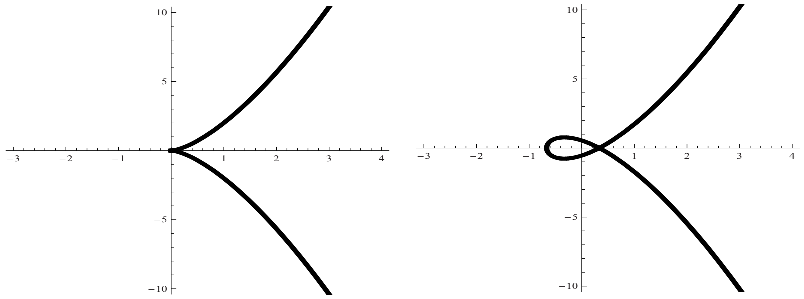
$y^2 = 4x^3 - 4x$ $y^2 = 4x^3 + 4x$

Figure 4.2-1: Two nonsingular elliptic curves.

known as an *elliptic curve*[1]. Depending on the values of k_1 and k_2, the elliptic curve will look basically like one of the diagrams in Figures 4.2-1 and 4.2-2. (Note that one could more generally consider any cubic polynomial on the right-hand side of equation (4.1), but it is always possible to put it into this form with a simple change of coordinates, so it is standard to describe them using only the two parameters k_1 and k_2.)

You can tell what the graph will look like by considering the number $27k_2^2 - k_1^3$. If this number is negative, then the graph has two components as in the illustration on the left in Figure 4.2-1. If it is positive, then it has one component like the graph on the right in Figure 4.2-1. If this quantity is *zero*, then the curve is not *technically* an elliptic curve but rather a *singular* elliptic curve, generally considered by algebraic geometers to be a different sort of "creature" all together. However, for the purposes of this book we will ignore this subtle distinction and consider these curves including a singular point to just be a special type of elliptic curve. Two singular elliptic curves are illustrated in Figure 4.2-2.

[1] Do not confuse elliptic curves with the familiar *ellipse*, which has the equation $ax^2 + by^2 = 1$. This is a completely different object. Historically, the study of elliptic curves grew out of the theory of integration of functions. Just as certain integrals can be worked out using sine and cosine through 'trig substitution' and are therefore related to circles, other integrals which would be impossible to evaluate otherwise naturally lead to elliptic functions and their corresponding curve. (The name "elliptic" refers to the fact that one application of the corresponding integrals is to evaluate arc lengths on ellipses.) This is not the approach that will be followed here, however. For a more classical introduction to elliptic curves, see *[58]*.



$y^2 = 4x^3$ $y^2 = 4x^3 - \frac{4}{3}x + \frac{8}{27}$

Figure 4.2-2: Two singular elliptic curves.

Example 4.2 What are the different ways in which the real roots of the polynomial $f(x) = 4x^3 - k_1x - k_2$ can be arranged and how are these reflected in Figures 4.2-1 and 4.2-2? Which case is not illustrated and what would the graph of the corresponding elliptic curve look like?

Solution The graph of $y = f(x)$ will have between one and three real roots, and it will take both positive and negative values. When $f(x)$ is negative, the equation $y^2 = f(x)$ will have no solution, and when it is positive it will have two solutions that differ only by a change in sign of the y-coordinate. Hence, the elliptic curve $y^2 = f(x)$ will look something like the portion of the graph of $y = f(x)$ that lies above the x-axis, reflected so that it is symmetric across that axis. (The shape will also be slightly different, because taking the square root will distort it slightly.)

Now, we can see that the first graph in Figure 4.2-1 illustrates the case in which $f(x)$ has three real roots. The graph takes positive values between the first two roots, and reflecting this little "hump" that sticks up over the line $y = 0$ produces the egg shaped component. It then takes negative values between the second and third roots, corresponding to the gap between the two components. Finally, where it comes up again after the third root we begin to see the graph as it heads off towards infinity.

In contrast, the second graph illustrates the case of a single real root of multiplicity one. (Here, $f(x) = 4x^3 + 4x$ so $f(0) = 0$ but $f'(0) = 4 \neq 0$.) The elliptic curve only has one real component since $f(x)$ is negative to the left of this root and positive to the right.

The two singular curves illustrate the case of a single real root of multiplicity three (which has a sharp "cusp" due to the fact that it has horizontal slope when intersecting the symmetry line at $y = 0$) and the case of a real root of multiplicity two appearing to the right of a real root of multiplicity one.

Not pictured here is the case in which a root of multiplicity two is to the left of a root of multiplicity one. The graph of $y = f(x)$ in that case would have a local maximum on the x-axis and would then cross the x-axis at the other root. Consequently, the graph of $y^2 = f(x)$ would look like the one component nonsingular graph in Figure 4.2-1 combined with an isolated point on the x-axis located at the other root.

Elliptic curves may not be quite as well known as circles, but they are really very famous and useful. There are methods of cryptography based on elliptic curves. The proof of Fermat's Last Theorem depends on elliptic curves. And, as we will see, they show up very naturally in the context of the KdV Equation.

4.2.1 Parametrization in Terms of the $\wp$-function There is a function called the "Weierstrass p-function" written $\wp(z; k_1, k_2)$ (or just $\wp(z)$ for short if k_1 and k_2 are understood) which has the property that for every z in its domain, $x = \wp(z)$ and $y = \wp'(z)$ satisfy the equation of the elliptic curve[2]. Although every point on the curve comes from some value[3] of z, there are z's for which these functions are undefined. ($\wp(0)$, for instance, is never defined.) However, even these values of z are thought of as corresponding to a point on the curve since mathematicians generally work with elliptic curves in a geometric setting called *projective space* where there is an additional "point at infinity" on the curve. One can imagine that this point resides far to the right at the ends of the two open arms of the graph, tying them together into another (infinitely large) loop. Consequently, it is common (and mathematically justifiable) to regard this point at infinity as being the point on the curve whose coordinates are given by substituting $z = 0$ into the parametrization.

[2] A brief discussion of how one might rigorously verify the claim that the $\wp$-function and its derivative satisfy the equation of the curve follows in Section 4.2.4.

[3] As we will see, we may have to consider *complex* values of z in order to obtain all of the points on the real curve.

You may at this point be interested in a formula or definition for $\wp(z)$. In fact, one can find the formula

$$\wp(z) = \frac{1}{z^2} + \sum_{w \in L\setminus\{0\}} \left(\frac{1}{(z-w)^2} - \frac{1}{w^2} \right) \tag{4.2}$$

in textbooks and on the Internet. Here L is a set of points in the complex plane of the form $L = \{aw_1 + bw_2 | a, b \in \mathbb{Z}\}$ where w_1 and w_2 are two particular (complex) constants determined by the property that

$$k_1 = 60 \sum_{w \in L\setminus\{0\}} w^{-4} \qquad \text{and} \qquad k_2 = 140 \sum_{w \in L\setminus\{0\}} w^{-6}. \tag{4.3}$$

There are many interesting questions about this formula that we will not be addressing. Questions of whether and how it converges, or how we know that equation (4.3) can be solved are beyond the scope of this book, but can be found in other fine sources such as *[58, 95]*.

You may initially find this lack of details regarding the function $\wp$ disappointing, but keep in mind that the functions $\sin(x)$ and $\cos(x)$ do not have simple formulas in terms of x and that you were able to work quite well with them even prior to learning their series expansions merely from knowing some of their basic properties and having a calculator/computer to estimate their values.

In the same way, here we will be able to get all we need to know about these functions from making use of their existing encoding in *Mathematica* where $\wp(z; k_1, k_2)$ and its derivative are denoted `WeierstrassP[z,{k1,k2}]` and `WeierstrassPPrime[z,{k1,k2}]`. *Mathematica* can manipulate them symbolically and can also compute approximate values of them from the infinite series definition. However, it does *not* know everything about them that we might want it to know, as the next example illustrates.

4.2.2 Double-Periodicity of $\wp$ The graph of $y = \wp(x; 28, -24)$ is shown in Figure 4.2-3. This was achieved by simply typing

```
Plot[WeierstrassP[x,{28,-24}],{x,-10,10}]
```

into *Mathematica*. Note that it has a vertical asymptote at $x = 0$ and is periodic so that this singularity repeats itself infinitely many times.

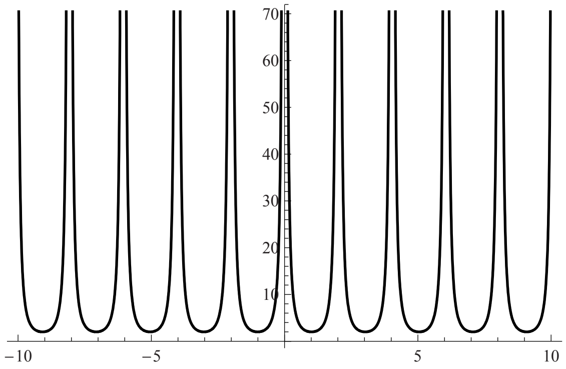


Figure 4.2-3: This is a plot of the curve $y = \wp(x; 28, -24)$. Note that it is periodic. Thus, if we considered a larger domain for z in the graph at the left it would just parametrize this same component over and over again.

One might at first think that the period is 2 with the vertical asymptote showing up again at $x = 2$ and $x = -2$, and it does look like this might be the case. However, looking more closely at the other integer-valued points on the x-axis reveals that the period actually seems to be a little bit larger than 2. In particular, one can see that the local minimum near $x = 5$ actually occurs just a bit to the right of the tick mark and that the tick mark for $x = 8$ is a bit to the left of the vertical asymptote.

Since the numbers k_1 and k_2 determine the ℘-function, it makes sense that *Mathematica* can tell us what the period of the function is given these two parameters. In fact, there is a command built into the program which does so, although for historical reasons it is designed to give *half* of the period rather than the period itself. The command `WeierstrassHalfPeriods[{k1,k2}]` evaluates in *Mathematica* to give two numbers γ_1 and γ_2 which have the property that

$$\wp(z + 2\gamma_i; k_1, k_2) = \wp(z; k_1, k_2).$$

Example 4.3 Use *Mathematica* to determine a very accurate numerical approximation of the period of the graph shown in Figure 4.2-3 and demonstrate that it is correct by graphing an appropriate horizontally shifted version of the ℘-function.

Solution Typing `WeierstrassHalfPeriods[{28,-24}]` into *Mathematica* is not particularly helpful. It simply gives us back something that looks exactly the same. However, if we enter instead

```
N[WeierstrassHalfPeriods[{28, -24}]]
```

we get `{-0.742206 i, 1.00945}` as an output. (If the *Mathematica* command `N[]` that provides numerical approximations to otherwise exact mathematical quantities is unfamiliar, consult Appendix A.)

The first of these is an imaginary number, and we will discuss that further below. The second one, however is a real number just slightly larger than one. Since twice this is supposed to be the period of the function, it makes sense that it might have looked to us as if the period was 2. In fact, a better approximation is

$$2 \times 1.00945 = 2.0189.$$

To further verify that this is the case, we plot both $\wp(x; 28, -24)$ and $\wp(x + 2.0189; 28, -24)$ on the same axes using the *Mathematica* command

```
Plot[{WeierstrassP[x + 2.0189, {28, -24}],
       WeierstrassP[x, {28, -24}]}, {x, -10, 10}]
```

The result is indistinguishable from Figure 4.2-3. We know that two functions are graphed there and that they differ only by a horizontal shift. The fact that it looks like the original graph confirms that (at least to the accuracy that we can see) the shift of 2.0189 units has not changed the graph at all.

To see this even more clearly, you can say

```
Plot[{WeierstrassP[x + 2.0189, {28, -24}],
  WeierstrassP[x, {28, -24}]}, {x, 0, 2.02},
  PlotStyle -> {{AbsoluteThickness[3],RGBColor[0,.2,.8]},
  {AbsoluteThickness[1], RGBColor[1, 1, .7]}}]
```

which graphs a thin, purplish line representing the unshifted $\wp$-function on top of a thicker, blue shifted version. This allows us to see the difference between shifting by 2 and shifting by 2.0189.

What about the *other* number which shows up in *Mathematica*'s output when prompted for the half periods? As we saw, at least in the case $k_1 = 28$ and $k_2 = -24$ that other number was an imaginary number. We do know that shifting the argument by an imaginary number can sometimes leave a real-valued function unchanged. For example, if $f(x) = e^x$, then the fact that $e^{\theta i} = \cos(\theta) + i\sin(\theta)$ (see Appendix B) implies that

$$f(x + 2\pi i) = e^{x+2\pi i} = e^x e^{2\pi i} = e^x.$$

In this sense, e^x is a periodic function with period $2\pi i$, even though this periodicity is not apparent from looking at its graph as a real function.

One of the defining characteristics of the Weierstrass function $\wp(z; k_1, k_2)$ is that it is *doubly periodic* (at least for nonsingular elliptic curves). In the case of the example we saw earlier, this means that shifting by *twice* $-.742206i$ should also leave the graph unchanged.

Example 4.4 Continue the previous example and demonstrate that the same idea works for a shift by twice the imaginary half-period, but that a more accurate approximation is required.

Solution What one might try at first does not seem to work. Just saying

```
Plot[{WeierstrassP[x + 2*-0.7422062 I, {28, -24}],
  WeierstrassP[x, {28, -24}]}, {x, 0, 2.02},
 PlotStyle -> {{AbsoluteThickness[3],
    RGBColor[0, .2, .8]}, {AbsoluteThickness[1],
    RGBColor[1, .2, .7]}}]
```

produces a graph only of the unshifted $\wp$-function. The other graph does not appear at all. This is because we are using a numerical approximation for the half-period and it was not quite accurate enough. (In the other case, this would have resulted in a very slight horizontal shift in the graph, but here the result is that the output of the function is a complex number rather than a real number and so cannot be graphed at all.)

We only need to get a *more accurate* approximation of the imaginary half-period for it to be close enough to produce the output we expect. An optional argument on the `N[]` command allows control of the number of decimal places of accuracy. So we say

```
N[WeierstrassHalfPeriods[{28, -24}], 20]
```

instead to get a better approximation and find that

```
Plot[{WeierstrassP[x+2*-0.74220623671119322645 I,{28,-24}],
  WeierstrassP[x, {28, -24}]}, {x, 0, 2.02},
  PlotStyle -> {{AbsoluteThickness[3],
    RGBColor[0, .2, .8]}, {AbsoluteThickness[1],
    RGBColor[1, .2, .7]}}]
```

does produce the same output as we got from the horizontal shift of the graph in the previous example.

In hindsight, we can now see the double periodicity of the $\wp$-function in its defining formula (4.2). Note that since adding either w_1 or w_2 to the set of points L leaves the set completely invariant, the series expansions for $\wp(z)$ and $\wp(z + w_i)$ contain the same terms, although they are reordered. As this suggests (though we would have to check some questions regarding convergence to be certain), the complex numbers w_1 and w_2 from equation (4.3) *are* the periods of the function. As we know how to write k_1 and k_2 in terms of these numbers, this means that one can also identify the curve by specifying the two half-periods, $w_1/2$ and $w_2/2$. Again, *Mathematica* has a built in command to help us with this. The *Mathematica* command

```
WeierstrassInvariants[{gamma1,gamma2}]
```

will give the values of k_1 and k_2 corresponding to an elliptic curve whose $\wp$-function has half-periods `gamma1` and `gamma2`, as illustrated in the following example.

Example 4.5 Use the `WeierstrassInvariants[]` command to find two different $\wp$-functions which have period 3. Plot them with *Mathematica* to confirm that it worked.

Solution Since the period should be three, we want the half-period to be 1.5. The other half-period can be any imaginary number. When we ask *Mathematica* for `WeierstrassInvariants[{I, 1.5}]`, it returns `{8.27476, -4.26937}`. In fact, plotting the corresponding $\wp$-function with the command

```
Plot[WeierstrassP[x,{8.27476,-4.26937}],{x,-9,9}]
```

we see a graph that does appear to have period 3. Similarly, although

```
WeierstrassInvariants[{2 I, 1.5}]
```

returns very different values for k_1 and k_2 ($k_1 \approx 1.69$ and $k_2 \approx .345$), a plot reveals that the period is the same.

4.2.3 Sweeping Out the Curves We can parametrically represent the elliptic curve $y^2 = 4x^3 - k_1x - k_2$ using the Weierstrass $\wp$-function $\wp(z; k_1, k_2)$ and its derivative. See, for example, Figure 4.2-4 where the case $k_1 = 28$, $k_2 = -24$ is illustrated. This was a achieved using the *Mathematica* commands:

```
w[z_] := WeierstrassP[z, {28, -24}]
  ParametricPlot[{w[z], w'[z]}, {z, .01, 1.99},
  AspectRatio -> 1, PlotRange -> {{-3, 4}, {-10, 10}}]
```

As promised, this graph does seem to coincide with the corresponding elliptic curve. However, this elliptic curve should have *two*

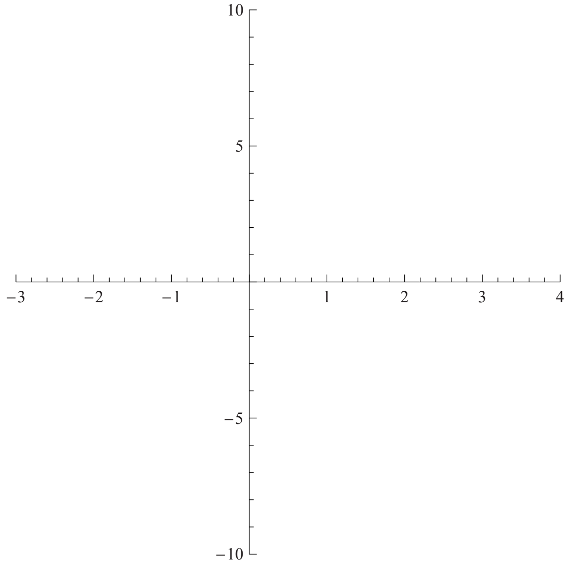


Figure 4.2-4: This is a plot of the curve parametrized as $z = \wp(z; 28, -24)$, $y = \wp'(z; 28, -24)$ for $.01 \leq z \leq 1.99$. Note that it coincides with (part of) the corresponding elliptic curve.

components and we only see one of them here. We will not get the other component by considering a larger interval of values for z. As shown in Figure 4.2-3, this $\wp$-function is periodic and will only give us this same component again if we were to consider it on another interval. Still, it is possible to get the "egg-shaped" component of this elliptic curve using this $\wp$-function using the *imaginary* half-period.

Sometimes, adding an imaginary number to the argument of a real function does not leave it unchanged (as it did for e^x with a shift of $2\pi i$) but actually turns it into a different real-valued function. For example, just as we know that $\sin(x+\pi) = -\sin(x)$, a similar formula applies to the related function $\sinh(x)$ (the hyperbolic sine). We get

$$\sinh(x + i\pi) = -\sinh(x).$$

(If you want to check this or understand better why it works, you can rewrite sinh in terms of exponential functions and use the famous formula $e^{\pi i} = -1$.) The reason this is relevant here is that in the case of the elliptic curves whose (real) graphs are made up of two separate components, when the $\wp$-function is shifted by the imaginary half-period, it becomes a real-valued function which "sweeps out" the egg-shaped component.

So, let us continue the previous example, this time parametrizing the other component by adding the imaginary half-period to the argument of the functions. Asking *Mathematica* to evaluate `WeierstrassHalfPeriods[{28,-24}]` is not particularly useful as the program simply spits the same thing back at us. However, if we ask it for a numerical approximation of this quantity (using the `N[]` command) we learn that the two half-periods are approximately $-.7422062367i$ and 1.00945. The latter of these two will not do us any good as adding it to the argument will just shift the graph horizontally by half of its period. Adding the imaginary value, however, will produce different output and interestingly it produces real values that we can plot. See Figures 4.2-5 and 4.2-6 where we have plotted the curve parametrized as $x = \wp(z - .7422062367i; 28, -24)$ and $y = \wp'(z - .7422062367i; 28, -24)$ for $0 \leq z \leq 2$ and also the graph of $\wp(z - .742206236i; 28, -24)$ to illustrate that it is still periodic but now *nonsingular*. In particular, we can see that this would "sweep out" the "egg-shaped" part of the elliptic curve over and over again, in much the same way that cosine and its derivative sweep out the unit circle.

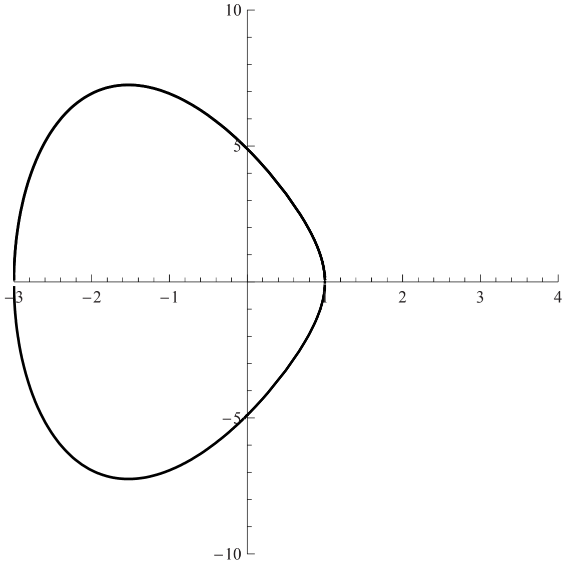


Figure 4.2-5: Adding an imaginary constant, one of the Weierstrass half-periods, to the real parameter z in the same functions used in Figure 4.2-4 sweeps out the "egg-shaped" part of the corresponding elliptic curve.

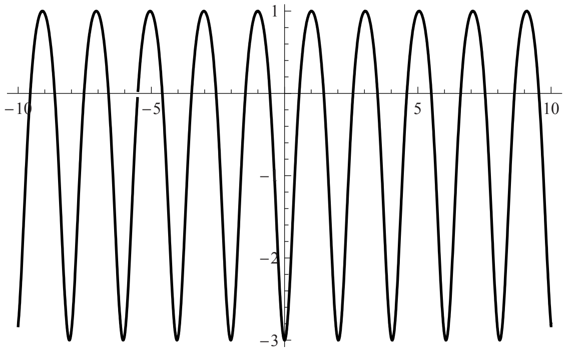


Figure 4.2-6: The graph of the ℘-function with this half-period added to the argument is a periodic function taking values between -3 and 1. Note that these are the x-coordinates of the portion of the elliptic curve shown on the left.

4.2.4 A Differential Equation Satisfied by $\wp$

Since $(\wp(z), \wp'(z))$ are always the coordinates of a point on the curve, the Weierstrass $\wp$-function always satisfies a differential equation which looks like the equation for the corresponding elliptic curve.

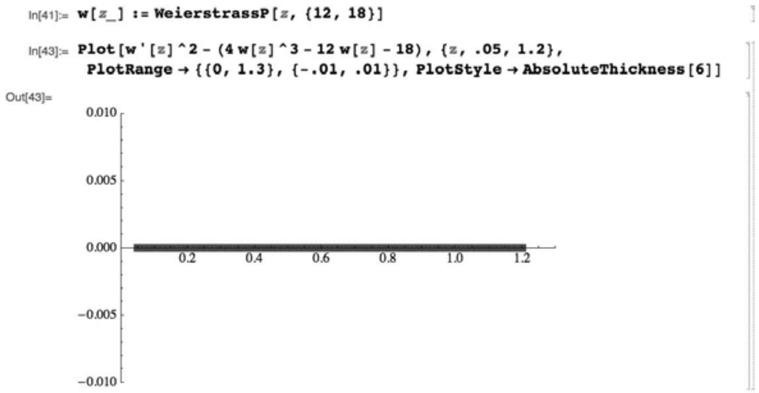
Example 4.6 Define `w[z_]:=WeierstrassP[z,{12,18}]` in *Mathematica* and verify that it satisfies

```
w'[z]^2-4w[z]^3-12w[z]-18=0.
```

Solution We seem to have a problem. *Mathematica* does not recognize that `Simplify[w'[z]^2 - (4 w[z]^3 - 12w[z] - 18)]` is equal to zero. Even though we asked it to `Simplify` that expression, it simply returns the same thing expanded out in terms of the definition.

If you are skeptical, you then might think that this expression is not in fact equal to zero and that this book is presenting false information. However, we can use the following non-rigorous procedure to convince ourselves that *Mathematica* is simply not "smart" enough to recognize this as zero. Plot a graph of the expression for $0.05 \leq z \leq 1.2$ as shown in Figure 4.2-7 and note that the values are all very close to zero.

This *numerical experiment* supports the claim that for any choice of k_1 and k_2, we know that $w(z) = \wp(z; k_1, k_2)$ solves the differential



```
In[41]:= w[z_] := WeierstrassP[z, {12, 18}]

In[43]:= Plot[w'[z]^2 - (4 w[z]^3 - 12 w[z] - 18), {z, .05, 1.2},
          PlotRange → {{0, 1.3}, {-.01, .01}}, PlotStyle → AbsoluteThickness[6]]

Out[43]=
```

Figure 4.2-7: A demonstration that $\wp(z; k_1, k_2)$ satisfies the ordinary differential equation (4.4).

equation

$$(w')^2 = 4w^3 - k_1 w - k_2. \tag{4.4}$$

(To prove this rigorously, one can begin with the expression for $\wp(z)$ given in (4.2), remove the poles of $\wp$ and $\wp'$ manually by subtracting an appropriate power of z, and compute Taylor expansions at $z = 0$. In attempting to create a combination which will cancel the initial terms, one soon derives an equation of the form (4.4). That the equation actually cancels *all* of the terms in the expansion requires a bit more of the theory of elliptic curves and complex analysis. See *[95]* for details.)

In fact, we can say not only that $\wp(z)$ is *a* solution, but because the equation is *autonomous* it follows that

$$w(z) = \wp(z + \gamma; k_1, k_2)$$

is a one-parameter family of solutions to (4.4) with γ playing the role of the single "constant of integration" we would expect for a first order equation.

The best way to think of this "constant" is as a *point on the curve.* Consider how convenient it is to simply state "there is a solution to this equation for every point on the corresponding elliptic curve". Not only is this a nice way of saying it, it takes into account the fact that you can select different values of the constant that still result in the same function because of its periodicity. Most importantly, we can conversely associate the point $(f(0), f'(0))$ on the curve to any solution $f(z)$ of the equation (4.4) (with the understanding that the point at infinity is associated to f if 0 is not in its domain).

Example 4.7 What differential equation is satisfied by the function

$$W(z) = a\wp(z; k_1, k_2) + b?$$

Solution Solving this for $\wp$ we find that $\wp(z; k_1, k_2) = (W(z) - b)/a$ and we know that this solves (4.4). Thus we know that

$$(\frac{1}{a}W')^2 = 4\left(\frac{W-b}{a}\right)^3 - k_1\frac{W-b}{a} - k_2.$$

Technically, this is an answer to the question already but we can write it in a nicer form as:

$$W'^2 = \frac{4}{a}W^3 - \frac{12b}{a}W^2 + \left(\frac{12b^2}{a} - ak_1\right)W - \frac{4b^3}{a} + abk_1 - a^2k_2.$$

Note that by selecting the four parameters a, b, k_1 and k_2 appropriately it is possible to obtain any desired cubic polynomial in W on the right side of this equation. It is in this sense that the assumptions for the form of the equation for an elliptic curve (that the leading coefficients are 4 and 0 respectively) are just a convenience which can be obtained from the general case by a change of variables.

4.2.5 The Group Law So far, we have seen that like the circle, the elliptic curve is the set of points whose coordinates satisfy a polynomial equation and that it is "swept out" by a parametrization involving a function and its derivative much in the same way that the circle is swept out by the trigonometric functions. Now, we will see that it also has the algebraic structure of a group. However, the group law on an elliptic curve is more geometrically interesting, extremely cool and also important.

To add points p and q on the curve, you draw a straight line

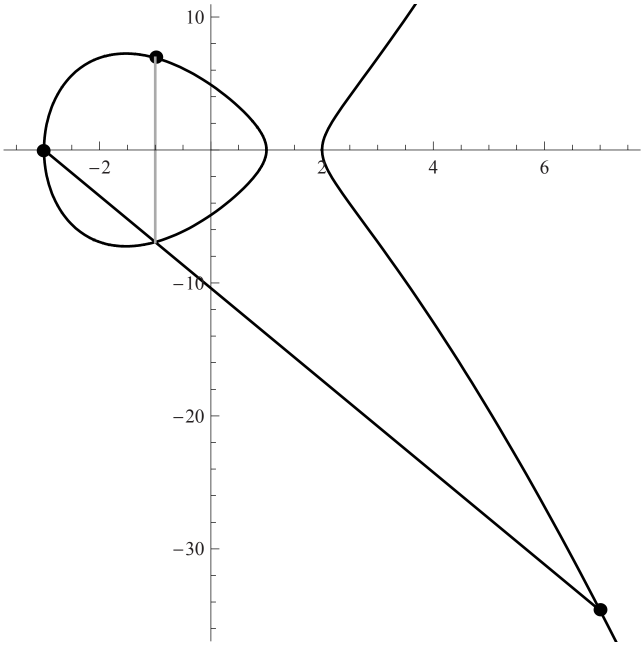


Figure 4.2-8: The sum of two points on an elliptic curve is given by the reflection of the third point of the curve lying on the straight line through the other two.

through them. The line will intersect the curve at one more point. Take that point and reflect it across the x-axis. The result is what we call $p+q$. (Well, it is possible that the line does not intersect the curve at another point. If that happens, then the "third point" is the point at infinity. The point at infinity stays the same when it is reflected across the x-axis and so that would be the sum in that case.) Using these rules makes the elliptic curve into an actual group according to the traditional definitions of algebra.

Example 4.8 A group needs an "identity element", which when added to a point leaves it the same. In this case, that identity element is the point at infinity. A group also needs an inverse for every element, which takes you back to the identity element. What is the inverse of a point p?

Solution Let $p=(x,y)$ be a point on an elliptic curve. If we add the point at infinity to it, we draw a vertical line though p since that is the line which intersects the curve at only two points (or once with multiplicity two if the vertical line happens to be tangent) and so the third intersection point is at infinity. The sum of p and the point at infinity is then the reflection of the third point of the curve on the line, which happens to be p again. So, the point at infinity is the identity element in this group rule.

Then, the inverse of p is $p^{-1}=(x,-y)$ (the reflection of p through the x-axis) because then the "third point" on the line containing p and p^{-1} is the point at infinity, which is its own reflection and is the identity element.

4.2.6 The ℘-function Respects the Group Law Suppose points P and Q on an elliptic curve have coordinates $(\wp(z_P),\wp'(z_P))$ and $(\wp(z_Q),\wp'(z_Q))$, respectively. The group law above gives us a way to add these two points to produce a points $P+Q$ using the geometry of the curve. Remarkably, it is possible to find the *same* point $P+Q$ in a more algebraic way using the numbers z_P and z_Q.

In particular, it turns out that the point $P+Q$ has coordinates $(\wp(z_P+z_Q),\wp'(z_P+z_Q))$. In other words, the ℘-function induces a group *homomorphism* between the usual addition of real numbers and the strange geometric addition law for elliptic curves. (It is not an *isomorphism* because there are many different choices of z_P that could be used to give P, for example.)

4.3 Traveling Wave Solutions to the KdV Equation

We have seen that the Weierstrass $\wp$-function satisfies a nonlinear ordinary differential equation. However, it is an equation that arises in a very geometrical way and it does not seem obvious at this point that this should have anything to do with the KdV Equation, a *realistic*, *partial* differential equation derived from hydrodynamics.

However, as we will see, the equation for an elliptic curve arises naturally if we just make a "Traveling Wave" assumption: *Suppose* $u(x,t)$ is a solution of the KdV Equation that has the form

$$u(x,t) = w(x+ct)$$

for some function w and some number c.

We already know from homework problem 4 in Chapter 1 that an animation of this solution will look like a fixed profile moving to the left at speed c, but we do not know what sorts of profiles can be selected that would produce a solution to the KdV Equation for any given value of c.

We bravely proceed, hoping that things will work in our favor, by merely substituting this definition for u into the KdV Equation (3.1) to obtain:

$$cw' = \frac{3}{2}ww' + \frac{1}{4}w'''. \tag{4.5}$$

Notice that we can integrate the entire equation (4.5) since every one of these things is a derivative of something we know. In this way we get

$$cw = \frac{3}{4}w^2 + \frac{1}{4}w'' + \gamma_1. \tag{4.6}$$

Here we have added an arbitrary constant, γ_1, as a result of our integration. It may at first look as if we cannot integrate again, because we do not know an antiderivative for w or w^2 in general. However, consider what happens if we multiply the equation through by a factor of w'. Then, we can again integrate the entire expression to get

$$\frac{c}{2}w^2 = \frac{1}{4}w^3 + \frac{1}{8}(w')^2 + \gamma_1 w + \gamma_2 \tag{4.7}$$

which rearranges to

$$(w')^2 = -2w^3 + 4cw^2 - 8\gamma_1 w - 8\gamma_2. \tag{4.8}$$

As this differential equation has $(w')^2$ on the left and a cubic in w on the right, we know from the Example 4.7 on page 81 that the general solution to this equation can be written in terms of a Weierstrass $\wp$-function. In particular, $w(z) = -2\wp(z+\omega; k_1, k_2)+2c/3$ is a solution for any constant ω and with

$$k_1 = \frac{4}{3}(c^2 - 3\gamma_1) \qquad \text{and} \qquad k_2 = \frac{8c^3}{27} - \frac{4c\gamma_1}{3} - 2\gamma_2.$$

But this means that

$$u_{ell(c,\omega,k_1,k_2)}(x,t) = -2\wp(x + ct + \omega; k_1, k_2) + 2c/3 \tag{4.9}$$

is a solution to the KdV Equation for **any choice** of ω, k_1, k_2 and c! (Note that the values of k_1 and k_2 do not matter here because there is no γ_1 or γ_2 in the KdV Equation.)

This is a rather remarkable statement, as it would mean that there are traveling wave solutions to the KdV Equation for any speed and whose profiles look like the graph of the $\wp$-function for any elliptic curve scaled vertically by a factor of -2 and shifted vertically by a term proportional to the speed. We just *have* to check that this is true using *Mathematica* because it seems hard to believe. Let us look at a few particular examples as animations to see what they look like and also plug it into the equation (numerically if necessary) to see that it really is a solution.

Example 4.9 Use *Mathematica* to verify that $u_{ell(3,0,2,4)}(x,t)$ is actually a solution to the KdV Equation and animate its dynamics.

Solution We define

```
uell[x_,t_,c_,omega_,k1_,k2_]:=
        -2 WeierstrassP[x+c t+omega,{k1,k2}]+2c/3
```

and use the program written in Problem 7 on page 64 to verify that it is a solution. Remarkably, *Mathematica* seems to recognize algebraically that this is an exact solution because it tells us that `KdV[uell[x,t,3,0,2,4]]` is `0`. (I was prepared for it to give us a complicated expression whose values were numerically evaluated to be very close to zero.)

We animate it using

```
MyAnimate[uell[x,t,3,0,2,4],{x,-10,10},
    {y,-5,5},{t,0,1},10]
```

and see a train of local maxima moving to the left at speed 3. This is as expected since the local minima have been turned into local maxima by the factor of -2 and because we have chosen $c = 3$.

We can easily see the role of the parameter c in this solution. It determines both the speed and the "vertical shift". So, in particular, if we repeat the last example with $c = 5$ we see the wave profile is higher (with the local maxima taking positive values) and also moving to the left at a greater speed. In contrast, with $c = -5$ the wave profile translates to the *right* at speed 5, but is translated down so far that we need to extend our viewing window to include more negative values of y in order to see it.

At first, it may seem that the parameter ω is relatively unimportant. It does not determine the speed (as does c) or the particular elliptic curve (which is fixed by k_1 and k_2, so these determine the overall shape of the profile). In fact, if it is chosen to be a real number, changing the value of ω merely shifts the initial profile to the left or right, and since the wave translates horizontally, this is equivalent to viewing the same solution at a different time. However, as the next example will illustrate, ω does have an important role to play if we allow it to take complex values.

Example 4.10 Of course, because of the singularities, the previous example is not a very realistic sort of wave for an equation modelling the motion of water on a canal. Select appropriate parameters c, ω, k_1 and k_2 so that the solution $u_{ell(c,\omega,k_1,k_2)}(x,t)$ is a *nonsingular* solution (i.e. continuous for all x) and animate the dynamics.

Solution Recall that if the curve has two components and we let ω be the imaginary half-period, then $\wp$ does not have a singularity (and that $(\wp, \wp')$ sweeps out the little "ring" part of the curve).

To implement this idea in *Mathematica*, we may simply tell *Mathematica* that we want one of the half-periods to be the imaginary number i and allow the program to select its own k_1 and k_2. (In other words, rather than asking it for the Weierstrass half-periods given k_1 and k_2, we will specify the half-periods and use the command `WeierstrassInvariants` to tell us what k_1 and k_2 must be.) Thus, we define:

```
u[x_,t_,omega2_]:=-2WeierstrassP[x + t + I,
              WeierstrassInvariants[{I,omega2}] ] + 2/3
```

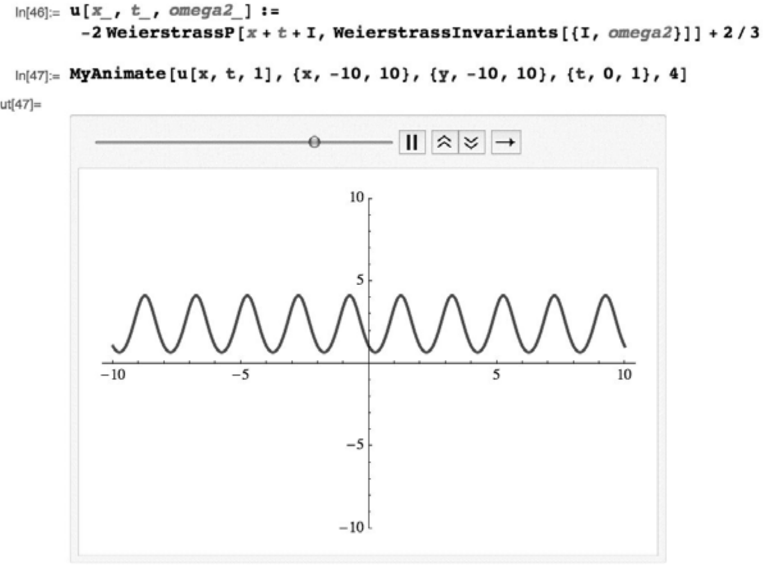
Note that we are using $c = 1$, adding i (which *Mathematica* calls `I`) to the x and do not know what the k_1 and k_2 are but they depend on this number `omega2`. Still, this must be a KdV solution because it has the proper form.

Now, we can view it for a few different values of `omega2`. The command

```
MyAnimate[u[x, t, 1], {x,-10,10}, {y,-10,10}, {t,0,1}, 5]
```

produces an animation of a train of local maxima and minima (looking very similar to a sine wave, although we know that it is actually made from a $\wp$-function) traveling left at speed one. (See Figure 4.3-9.)

Example 4.11 How is the solution affected by changing the value of `omega2`? In particular, what happens in the limit as `omega2` becomes very large?



```
In[46]:= u[x_, t_, omega2_] :=
          -2 WeierstrassP[x + t + I, WeierstrassInvariants[{I, omega2}]] + 2 / 3

In[47]:= MyAnimate[u[x, t, 1], {x, -10, 10}, {y, -10, 10}, {t, 0, 1}, 4]
Out[47]=
```

Figure 4.3-9: A nonsingular traveling wave solution to the KdV equation. It looks somewhat like a sine wave even though it is written in terms of a $\wp$-function.

```
In[48]:= MyAnimate[u[x, t, 3], {x, -10, 10}, {y, -10, 10}, {t, 0, 1}, 4]
Out[48]=
```

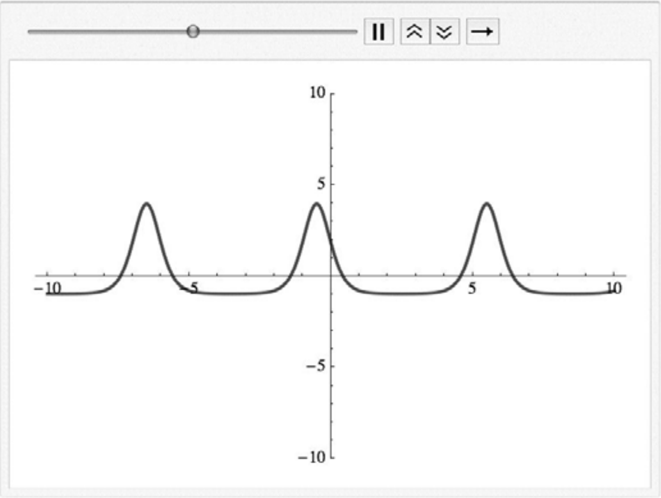


Figure 4.3-10: Another nonsingular traveling wave solution, this time corresponding to a different elliptic curve. Note that as we increased the value of `omega2`, flat regions have developed between the local maxima.

Solution What change do we expect? Note that we should not expect the speed to change, as the speed $c = 1$ was "hard wired" into this definition of `u[x,t,omega2]`. Instead, changing `omega2` should change the *curve* and therefore somehow affect the shape of the graph. In particular, we see in Figure 4.3-10 that for `omega2=3` we still have a solution translating the to left at the same speed, but now the local maxima are farther apart and there appears to be a long flat region in between each one (so that the graph no longer looks very much like a sine wave).

In general, as we choose larger and larger values for `omega2` the peaks get so far apart that we can only see one at a time in our viewing window and they look *essentially* like 1-solitons.

The moral of the story is that the "long-wave limit" of these periodic waves from elliptic functions is the solitary wave. That, in fact, was exactly what Korteweg and de Vries showed in their paper! *They* knew about the connection between elliptic curves and nonlinear waves back in 1895.

What about solitons themselves? Of course, the 1-solitons *must* be here because they are solutions to the KdV Equation whose profiles simply translate in time. But, to get one out of this construction in *Mathematica* we will have to make careful selections.

Example 4.12 Find values for the parameters so that the function $u_{ell(c,\omega,k_1,k_2)}(x,t)$ is a 1-soliton solution to the KdV Equation just like those we saw in the last chapter.

Solution Consider the case $c = 1$, $k_1 = 4/3$, $k_2 = -8/27$ and $\gamma = -\frac{i\pi}{2}$. Note that this solution will translate at speed $c = 1$ to the left. Note also that it is a *singular* elliptic curve because of the choice of k_1 and k_2.

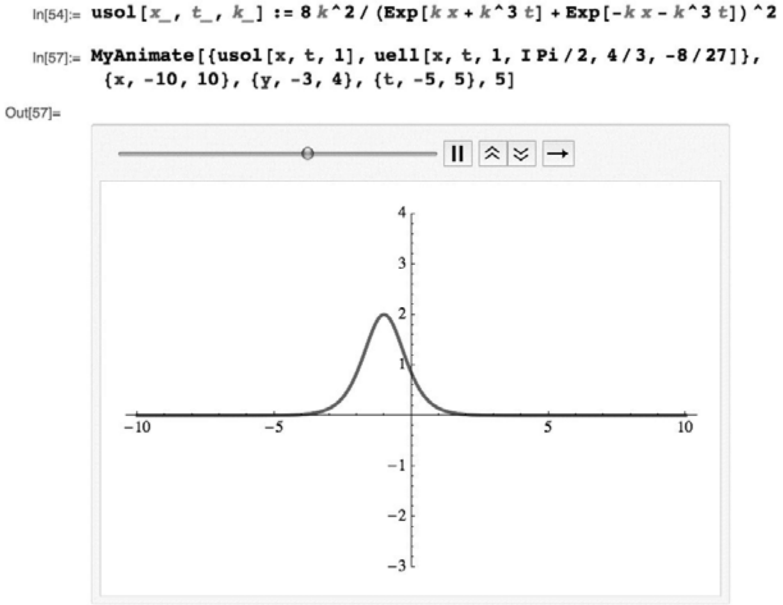
Animating this solution with the `MyAnimate[]` command produces something that is visually indistinguishable from the 1-soliton solution of speed one shown in Figure 3.5-1. Just to better compare them, we can animate the two solutions simultaneously, as in Figure 4.3-11. The fact that the animation appears to show only a single curve at all times attests to the fact that these two solutions are very nearly identical. In fact, although *Mathematica* does not seem to know it, they are mathematically identical; the $\wp$-function for this choice of parameters can be written exactly in terms of exponential functions and then the two formulas for this KdV solution coincide.

4.3.1 The Big Picture

The discovery of solitary wave solutions to a nonlinear PDE was a surprise in the 19th century. Here, we see a little bit of the "magic trick" that makes it work. In particular, one might get the impression that it is a complete coincidence that the KdV Equation just happens to look like the equation for an elliptic curve when one assumes the solution is a traveling wave, $w(x + ct)$. This is probably what experts would have thought after reading the paper by Korteweg and de Vries in 1895.

However, in the second half of the 20th century, it was discovered that the truth is much more complicated and interesting than that. It is not only the traveling wave solutions of the KdV Equation which are connected to algebraic geometry, and there are many other "soliton equations" which have share the algebro-geometric structure and particle-like solutions but look very different.

We are just glimpsing a tiny piece of a *huge* and important theory here. We will see a tiny bit more about the connection between curves



```
In[54]:= usol[x_, t_, k_] := 8 k^2 / (Exp[k x + k^3 t] + Exp[-k x - k^3 t])^2

In[57]:= MyAnimate[{usol[x, t, 1], uell[x, t, 1, I Pi / 2, 4 / 3, -8 / 27]},
          {x, -10, 10}, {y, -3, 4}, {t, -5, 5}, 5]

Out[57]=
```

Figure 4.3-11: A 1-soliton solution to the KdV Equation written in terms of exponential functions as in the last chapter and the solution written in terms of the $\wp$-function of a carefully chosen singular elliptic curve are exactly the same.

and solitons when we learn about differential algebra. Here, in case you are curious, is a description of how these ideas can be generalized beyond what will be covered in this book. We have seen that there is a solution to the KdV Equation associated to the choice of an elliptic curve and any point on that curve. Something like this is true on a much larger scale. Pick *any* algebraic curve (that's a big set). Associated to that curve is a group called its Jacobian Variety. (In the case of the elliptic curve it is a "coincidence" that the Jacobian and the curve are the same thing.) There is a solution to a soliton equation associated to each choice of a curve and an element of the associated group. If the curve is a hyper-elliptic curve, then it is a solution of the KdV Equation. Otherwise, it is a solution of the KP Equation that we will see in Chapter 9.

Chapter 4: Problems

1. In this question we will consider the elliptic curve with equation

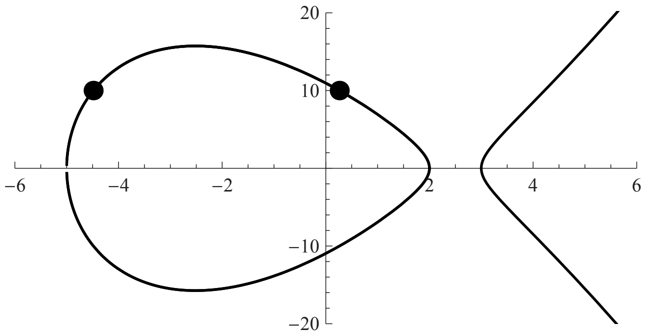
$$y^2 = 4x^3 - 28x + 24.$$

(a) There are two points on the curve with x-coordinate equal to 3. What are the y-coordinates of those points?

(b) Find the sum of the points $p = (2, 0)$ and $q = (0, 2\sqrt{6})$. (That is, apply the geometric method of adding points to find the third point on the curve which is their sum. This will involve finding the equation of the line containing those points and solving for the third point. Show all steps and explain what you are doing.)

2. Consider the elliptic curve: $y^2 = 4x^3 - 76x + 120$.

(a) Here is a graph of part of that elliptic curve. There are two points on the "egg" with y-coordinate equal to 10, indicated in the figure by "dots". By drawing one more "dot", show approximately where the *sum* (in the sense of the elliptic group law) of these two points would be located.



(b) What can we choose for the parameters k_1 and k_2 so that the point

$$(x, y) = (\wp(\alpha; k_1, k_2), \wp'(\alpha; k_1, k_2))$$

is sure to lie on that curve for any α in the domain of the function?

(c) Letting k_1 and k_2 be as in your answer to (b), we know that

$$P = (\wp(2; k_1, k_2), \wp'(2; k_1, k_2)) \quad Q = (\wp(8; k_1, k_2), \wp'(8; k_1, k_2))$$

are the exact coordinates of two points (P and Q) that lie on the curve. What are the exact coordinates of the other point on the curve which lies on the same straight line as P and Q? (Hint: Your answer will involve "$\wp$".)

3. What would you do to add a point on the elliptic curve to *itself*? Use concepts from Calc 1 in a well-argued paragraph to explain why this method makes sense.

4. (a) The function

$$f(x) = 3\wp(x + 9; 2, -5) + 8$$

satisfies the differential equation $(f')^2 = Af^3 + Bf^2 + Cf + D$. What are the constants A, B, C and D?

(b) Find a formula for a nonconstant solution $\phi(x)$ to the differential equation

$$(\phi' + \phi)(\phi - \phi') = \phi^3$$

written in terms of a Weierstrass $\wp$-function. Verify your answer using *Mathematica*.

5. If $k_1 = k_2 = 0$, then $\wp(z; k_1, k_2)$ actually has a simple formula, which *Mathematica* will show you. What is the general form of the solution $u_{ell(c,\omega,0,0)}(x, t)$ and what can you select for c so that this is a solution you've seen before in a homework problem from a previous chapter?

6. Use *Mathematica* to watch the dynamics in the case of elliptic solution u_{ell} with the choices $c = -1$, $k_1 = 4/3$, $k_2 = -8/27$ and $\omega = -\frac{i\pi}{2}$. Notice that it looks like our usual 1-soliton solution $u_{sol(1)}(x, t)$ but shifted vertically and going to the right with speed 1 instead of the left. Using your answer to Problem 8 on page 64, write an equation that shows how these two solutions are related.

7. In this question we will try to make an animation showing the deformation of a nonsingular elliptic curve into a singular one. If necessary, refer to the appendix on *Mathematica* commands and programming.

(a) In *Mathematica* define the function `f[x,a]` as

```
f[x_,a_] := 16a + 8a^2 - 16x - 8a x - 4a^2 x + 4x^3
```

What are the roots of this cubic polynomial? If $-4 \leq a \leq -3$, list the roots in order and counted according to their multiplicity.

(b) Now define a command `showthecurve[a]` which plots the elliptic curve $y^2 = 16a+8a^2-16x-8ax-4a^2x+4x^3$ on the window $-4 \leq x \leq 4$ and $-12 \leq y \leq 12$. (My advice for this is to plot the function `Sqrt[f[x,a]]` to generate the top of the curve and `-Sqrt[f[x,a]]` to generate the bottom. You will have to be careful, however, to only do this where the argument of the square root is positive. Then, use the `Show[]` command to put them all together and specify the range on which they should be plotted.)

(c) Finally, make an animation showing elliptic curves corresponding to $-4 \leq a \leq -3$. (Make sure it looks like a smooth deformation and not as if it is suddenly changing from one shape to another.)

8. Note that the constant solution $u(x,t) \equiv k$ (for constant k) *is* a solution to the KdV Equation (3.1). In a certain trivial sense, this also is a traveling wave solution since it is of the form $w(x+ct)$ with $w(x) \equiv k$. Thus, it should be possible to choose parameters c, ω, k_1 and k_2 so that $u_{ell(c,\omega,k_1,k_2)}(x,t)$ is an arbitrary constant (independent of x and t). Find such a choice of parameters and explain how this relates to the discussion of the arrangements of roots of cubic polynomials in Example 4.2 on page 70.

Chapter 4: Suggested Reading

Consider consulting the following sources for more information about the material in this chapter.

- The book by McKean and Moll *[58]* is a good source for information about elliptic curves for those without any advanced mathematical training.
- Silverman's book on the *arithmetic* of elliptic curves *[81]* will expect familiarity with algebra and algebraic geometry beyond the preliminaries for this book, but is a classic and worth looking at for whatever one may get from it.
- To learn more about algebraic geometry in general, rather than just about elliptic curves, the books by Miles Reid *[71]* and Klaus Hulek *[41]* are good introductions for undergraduates, and Hartshorne *[39]* is a traditional graduate text.

- Finally, to learn more about the connections between soliton theory and the algebraic geometry of curves, study the review paper by Previato *[69]*, or the textbooks by Belokolos, Bobenko, Enol'skii, Its and Matveev *[5]* or Gesztezy and Holden *[30]*.