

**NOTE:** Each exercise is worth 10 points and can be turned in at any time before its “expiration date”. At the end of the semester, I will expect you to have turned in at least 1/2 of the exercises assigned. If you do more, I will pick your best grades. If you do less, the missing grades will be counted as zeros. Altogether, these will count the same as one project.

Many of these problems will require you to use the help system and/or read the text to figure out what commands you need to use and how to use them.

1. (expires 2/6) If  $p(x)$  is a complex polynomial with real coefficients, it is well known that it can be factored into a product of linear and quadratic terms with real coefficients, or into a product of linear terms only if the coefficients are allowed to be complex.

First, use `Maple` to write  $q(z) = x^5 - 3x^4 - 3x^3 + 9x^2 - 10x + 30$  as a product of *exact* linear and quadratic factors with real coefficients. By exact, I mean you should leave any non-rational factors expressed as radicals; do not approximate terms like  $\sqrt{3}$  as 1.73205, etc.

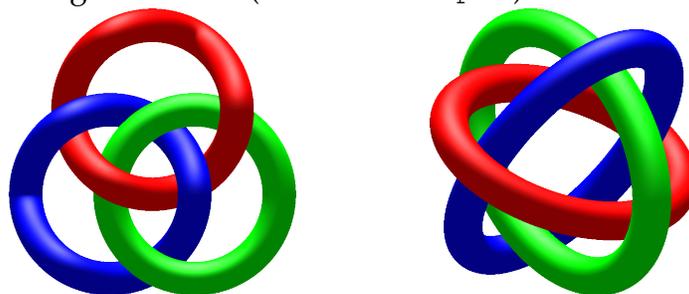
Then write  $q(x)$  as a product of only linear factors (which will involve complex numbers). Finally, do the same for product  $p(x) = x^5 - 2x^4 - 10x^3 + 20x^2 - 16x + 32$ .

*Hint:* Note that this question asks for four different answers, two for each polynomial. While the maple command `factor` is relevant, it will need a little assistance to be able to answer all four parts. Alternatively, there are other ways to do this.

2. (expires 2/6) Draw a graph showing both  $\cos(x)$  and its fifth Taylor polynomial (that is,  $1 - \frac{1}{2!}x^2 + \frac{1}{4!}x^4$ ) for  $x$  between  $-4$  and  $4$ . What degree of Taylor polynomial seems to be needed to get good agreement in this range? *Hint:* use a variation of the command `convert(taylor(cos(x), x, 5), polynomial)` to make this work. Think of a suitable way to demonstrate that the approximation you have taken is “good” – what is a good definition of “good” here? Be sure to **explain** your choice of the meaning of “good”.
3. (expires 2/13) The Borromean rings are a set of three mutually interlocked rings, arranged so that if one ring is removed, the other two become unlinked.

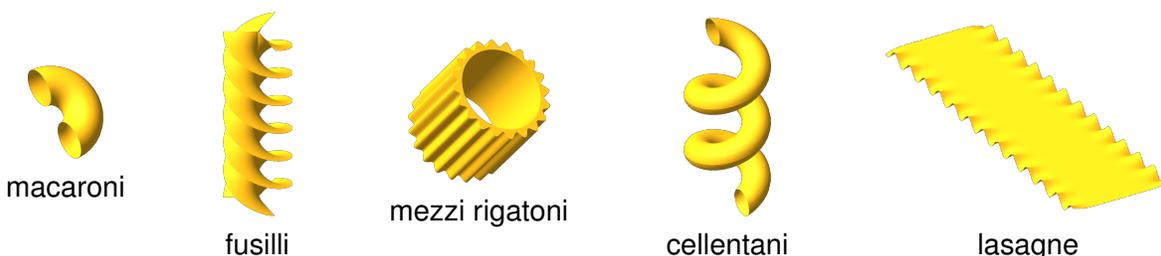
Use `Maple` to make an image of the Borromean rings in  $\mathbb{R}^3$ . *Hint:* I suggest using `tubeplot` from the `plots` package. The real challenge of this problem is figuring out how to parameterize the three curves.

Note that the Borromean rings can not be made from flat, round rings. Either some of the rings have to be bent a little to weave through each other, or flat rings which are elliptical can be used. See the figures below (made with `Maple`).



4. (expires 2/13) Plot the function  $f(x) = 2 \sin x - x^3 - 1/5$ , for  $x \in [-4, 4]$ . Find all the zeros of the function with an accuracy of 20 decimal digits. *Hint:* See `Digits`, `fsolve`.

5. (expires 2/20) Consider the planar curve  $\gamma$  defined by  $x^2y^3 + y^2 + y - 2e^x = 0$ . Using **Maple**, find the slope of the tangent line to the curve at  $(0, 1)$ . Then plot the curve and the tangent line on the same graph.  
*Hint: you might want to use `implicitplot` from the library `plots`. You might find `implicitdiff` helpful, too.*
6. (expires 2/20) Define a **Maple** function  $g$  that, given a positive integer  $k$  yields the sum of the first  $k$  primes. What is  $k$  such that  $g(k) \leq 100,000$  but  $g(k + 1) > 100,000$ ? You might find `sum` and `ithprime` helpful.
7. (expires 2/20) Use the Maclaurin series for  $\arctan x$  (that is, the Taylor series about  $x = 0$ ) evaluated at  $x = 1/\sqrt{3}$  to compute the value of  $\pi$  to 30 places. How many terms are needed to compute the value of  $\pi$  to 50 places?
8. (expires 2/20) Use **Maple** to make pictures of the following pasta.



Here are some relevant equations, in no particular order.

$$z = \sin(2y) \left(1 - e^{-(x/6)^8}\right) \quad -6 \leq x \leq 6, \quad -20 \leq y \leq 20$$

$$\tau = 1 \quad 0 \leq \phi \leq \pi, \quad -\pi \leq \sigma \leq \pi \quad (\text{toroidal coordinates})$$

$$x = \left(1 + \frac{\cos(s)}{2}\right) \cos(t) \quad y = \left(1 + \frac{\cos(s)}{2}\right) \sin(t) \quad z = 0.4t + \frac{\sin(s)}{2} \quad \begin{array}{l} 0 \leq s \leq 2\pi \\ \frac{\pi}{2} \leq t \leq \frac{11\pi}{2} \end{array}$$

$$\left\{ \begin{array}{l} x = r \sin(t) \quad y = r \cos(t) \quad z = t/2 \\ x = r \sin\left(t + \frac{2\pi}{3}\right) \quad y = r \cos\left(t + \frac{2\pi}{3}\right) \quad z = t/2 \\ x = r \sin\left(t - \frac{2\pi}{3}\right) \quad y = r \cos\left(t - \frac{2\pi}{3}\right) \quad z = t/2 \end{array} \right. \quad \begin{array}{l} 0 \leq r \leq 1 \\ 0 \leq t \leq 4\pi \end{array}$$

$$6 \leq r \leq 7 + \sin(20\theta)/2, \quad 0 \leq \theta \leq 2\pi, \quad 0 \leq z \leq 14 \quad (\text{cylindrical coordinates})$$

To help you get started, the **Maple** worksheet called [pasta.mw](#) draws Mezzi Rigatoni. For full credit, your pasta should look like pasta, with appropriate coloring, viewpoint, smoothness, and lighting. Sauce is optional.

9. (expires 2/27) Given the set of points

$$(0, 3), (1, 0), (2, 4), (3, 4), (4, -1), (6, 4), (7, 0), (9, 2), (10, 10),$$

Find the polynomial of degree 8 that passes through all of them. If you wish, you can use `CurveFitting[PolynomialInterpolation]`, or you can calculate all of the relevant equations.

Then find the polynomial of degree 9 which passes through these points and also has a critical point at  $x = 6$ , and the polynomial of degree 10 passing through the points with critical points at both  $x = 1$  and  $x = 6$ .

Finally, make a plot displaying all three graphs, together with the data points.

If you don't want to type the points, you can load them from the web at <http://www.math.sunysb.edu/~scott/mat331.spr14/problems/polydata.txt>, which defines a list called `polydata` containing these points.

10. (expires 2/27) Using the [same data](#) as the previous problem, find the "natural" cubic spline which interpolates the data. Also calculate the cubic spline which has derivative 0 at  $x = 0$  and  $x = 10$ , and make a plot showing the data points and these two curves on the same axes. (You will probably have to read the help page on [Spline Continuity and End Conditions](#) to see how to adjust the derivatives at the endpoints.)

11. (expires 2/27) In class on [February 11](#), we created a graph with an interactive slider control. Write a maple worksheet with one or more interactive controls that does the following:

- (i) Given a function  $base(x)$ , generate a list of points  $(i, base(i))$  for integer  $i$ ,  $0 \leq i \leq 10$ .
- (ii) Find the interpolating polynomial of least degree which passes through the points in the above list and also the point  $(a, b)$ .
- (iii) Find the cubic spline which passes through the points in the above list and also the point  $(a, b)$ .
- (iv) Plot the data points (including  $(a, b)$ ), together with the interpolating polynomial and the cubic spline on the same graph.
- (v) There should be an interactive control which allows the user to adjust both the  $x$ - and  $y$ -coordinates of the point  $(a, b)$  and the plot should automatically update itself as the point is adjusted.

To help you get started, there is a worksheet called [sliderfit.mw](#) containing just the relevant parts from that class.

12. (expires 3/4) Fit the set of points

$$(1.02, -4.30), (1.00, -2.12), (0.99, 0.52), (1.03, 2.51), (1.00, 3.34), (1.02, 5.30)$$

with a line, using the least square method. You will see that this is not a good fit. Think of a better way to find a line which *is* a good fit and use Maple to do it. Explain in your solution why you think your better way is indeed better.

You can load these data points from the web at <http://www.math.sunysb.edu/~scott/mat331.spr14/problems/fit6.txt>, which defines a list `fit6` containing these points.

See the page on [loading a file from the web](#) from the class web page for more details.

13. (expires 3/4) The file <http://www.math.sunysb.edu/~scott/mat331.spr14/problems/fitexp.txt> defines 21 data points that approximates an exponential curve of the form  $y = ae^{bx}$ . This data is called `fitexp`.

Find  $a$  and  $b$  by taking the appropriate logarithm, then use `LeastSquares` to find the resulting “best” line. Transform this line appropriately to get an exponential curve.

Plot the exponential and the `fitexp` data on the same axes.

14. (expires 3/4) Fit the points  $(-1.9, -4.7), (-0.8, 1.2), (0.1, 2.8), (1.4, -1.2), (1.8, -3.5)$  by means of a quadratic function  $f(x) = ax^2 + bx + c$ , using the least square method.

You can load these data points from the web via the link at [fitquad.txt](#) which defines a list `fitquad` containing these points.

See the page on [loading a file from the web](#) from the class web page for more details.

15. (expires 3/4) In this problem we will estimate the charge of the electron.

If an electron of energy  $E$  is thrown into a magnetic field  $B$  which is perpendicular to its velocity, the electron will be deflected into a circular trajectory of radius  $r$ . The relation between these three quantities is:

$$B r e = \frac{E^2}{m^2 c^4} \sqrt{E^2 - m^2 c^4}, \quad (1)$$

where  $e$  and  $m$  are, respectively, the charge and the mass of the electron, and  $c$  is the speed of light. The rest mass of the electron is defined as  $E_0 = mc^2$ , and is about equal to  $8.817 \cdot 10^{-14}$  Joules. In our experimental set-up the energy of the emitted electrons is set to be  $E = 2.511E_0$ .

The file [electron.txt](#) defines a list called `electron`. Each element of the list is a pair of the form  $[B_i, r_i]$ , and these quantities are expressed in Teslas and meters. Use least square fitting to determine the best value for  $e$ .

[Hint: Notice that the right hand side of eqn (1) is just a constant—calculate it once and for all and give it a name. Then eqn (1) becomes an equation which is linear in the unknown  $e$ . To verify your solution:  $e \approx 1.602 \cdot 10^{-19}$  Coulomb]. Physical constants courtesy of N.I.S.T.

16. (expires 3/6) The set of twelve points

$$\begin{array}{cccc} (-2.256, 0.879) & (-1.764, 5.800) & (-0.684, -0.854) & (-0.776, 6.750) \\ (3.718, 7.394) & (0.081, -1.315) & (-2.357, 4.534) & (6.485, 4.021) \\ (6.518, 3.999) & (2.818, 7.689) & (1.788, -1.668) & (-2.720, 2.719) \end{array}$$

approximate a circle with an unknown radius and center at  $(2, 3)$ . What is the “best” value for  $r$  corresponding to this data? Explain your answer. Plot the resulting circle and the data points on the same graph.

(Note that if you fit the data using the method described in section 6 of the notes, you’ll get a somewhat different radius. Using an unknown center gives one at approximately  $(1.970, 3.002)$  due to the noise in the data.)

If you don’t want to retype the points, you can load them from the file [circddata.txt](#) on the problems area on the class web page, which defines a list called `data`.

**NOTE:** Neither of the next two problems intrinsically involve Maple, except as a word processor to write your solution (although you can use it to help with calculations if you want). If you prefer, you are welcome to turn in your solution as a PDF file, which you can produce with a word processor or by scanning a hand-written version. A worksheet is slightly preferred.

17. (expires 3/6) Following Section 6 (Fitting a Circle) of the notes, prove that if we describe the circle of center  $(a, b)$  and radius  $r$  using the parameters  $(a, b, k)$ , with  $k = a^2 + b^2 - r^2$ , rather than the more natural parameters  $(a, b, r)$ , then the function  $H(a, b, k) = E(a, b, \sqrt{a^2 + b^2 - k})$  is quadratic in  $a, b$  and  $k$ . What does this imply about the number of critical points?
18. (expires 3/6) With reference to the previous problem, show that for  $r > 0$ , the transformation  $(a, b, r) \mapsto (a, b, k)$  is a valid change of variables, that is, it is a diffeomorphism (a one-to-one function with continuous nonzero derivatives). This should help you prove that  $E(a, b, r)$  has only one “physical” critical point, which is a minimum, and is mapped, through the transformation, into the unique critical point of  $H(a, b, k)$ .

19. (expires 3/13) The text below was encrypted with a substitution cipher. Only the letters (both upper-case and lower-case) were substituted, leaving punctuation and spaces alone. Figure out what the original message was.

"wA'r aBeD WUeK AP XNaB NM U rALKNP USUeAJBMA NM zUM nPrB ZNAW  
 U JUM ZWP'r XBUeMNMO AP SXUD AWB aNPXNM." yWUA'r ZWUA rWB APXK  
 AWB SPXNCB ZWBM rWB WUMKBK AWBJ AWB BJSAD eBaPXaBe.  
 lNCWUeK heULANOUM, "yWB zCUeXUAAN yNXA"

If you wish, you can find the encrypted text on the class web page at <http://www.math.sunysb.edu/~scott/mat331.spr14/problems/subscript.txt>.

If you want to put the message into a maple string, you'll either have to read it from a file via a command like

```
Crypto:=HTTP[Get] ("www.math.sunysb.edu/~scott/mat331.spr14/problems/subscript.txt") [2];
```

or prefix the quotation marks with a backslash (i.e., `\`) when typing them.

Note also that I am not asking you to write Maple that solves *every* such problem; the easiest way to do this problem involves some guesswork as well as knowledge of how English sentences are structured.

*Hint: you might find `CountCharacterOccurrences` or `CharacterFrequencies` from the library `StringTools` helpful. Depending on how you do things, `CharacterMap` could also be useful.*

20. (expires 3/13) The cryptography chapter in the notes is called "fsqFsHn sGGousG", which is actually the result of applying a Caesar cipher to its original title. A 53-character alphabet consisting of all the upper-case letters, a space, and all the lower-case letters was used; consequently the space in the middle might or might not correspond to a space in the title. Determine what the original title was.

21. (*expires 3/27*) The string below was encrypted using an affine cipher on the 27 letter alphabet “abcdefghijklmnopqrstuvwxyz” (there is a space in the 0<sup>th</sup> position.) Decrypt it.

fmw segjaweooouanerj a ceyqrype aswaheoaqbrqabeafrua eeaojerf afmjeayperjpu

Hint: this phrase follows the the typical pattern in English where there are (almost) as many spaces as words (and so spaces are very common), and the letter “e” is also very common. You can use the technique described in section 7 of the [cryptography chapter of the notes](#).

If you wish, the encrypted text can be loaded from the file [afftext.txt](#). A version of the the affine cipher can be found on the website in the worksheet [Crypto.mw](#), or you can write your own.

22. (*expires 3/27*) The method we have been using to convert text to numbers (the procedure `StringToList`) doesn’t deal well with letters that don’t appear in the given `Alphabet` (it converts them to `-1`, which then becomes the final character in the alphabet).

Modify `StringToList` to remove any characters in the input string which do not appear in the global variable `Alphabet`. If you like, you can give a warning about such characters, or just silently discard them.

(As before, you can steal `StringToList` from the worksheet [Crypto.mw](#).)

23. (*expires 3/27*) The text below was encrypted using a Vignère cipher on the 28-letter alphabet consisting of the standard English alphabet, a space, and a period (that is, “abcdefghijklmnopqrstuvwxyz .”). The keyword is known to be four characters long. Decrypt the message given below, and determine the encrypting keyword.

The second two lines in the encrypted text begin with a space; linebreaks are not significant in the message. To make it easier to see the spaces, they have been written here as underscores (.).

```

xvlfpbepbud.ijxhw.tlxcq-wiv.ijgsw.guofpoi.wijii_fmjbbjh_.pj
_gppnrupdm._dcduw.wijii_fmjbc.ihh.hefpcdbsjlh.dfbgzgkupcovs
_ltpyrvpdr.cow.iaolpaepjtbgzgkupcovs.

```

Hint: as in the earlier problem, the message follows the rules of ordinary English, so spaces are quite common. Periods come at the end of sentences, so while they are not common, this can be a clue.

The encrypted text (with the spaces left as spaces) can be found in the file [vignere4.txt](#).)

24. (*expires 3/27*) Modify the implementation of the Vignère cipher as used in class (or in [Crypto.mw](#)) to use the contents of a webpage for the keyphrase. That is, be able to encrypt some text with a command like

```
WebVignere(text, "http://xroads.virginia.edu/~hyper/poe/gold_bug.html")
```

Be careful to account for the situation where the webpage may contain characters not in the `Alphabet`.

25. (*expires 4/3*) Historically, “pen and paper” encryption (that is, what was mostly done prior to about 1980) would first rewrite a message to be encrypted in all upper-case letters, omitting all punctuation and spaces, and then writing out the message in blocks of five letters. For example, the message `Mr. Watson, come here - I want to see you!` would be transcribed as `MRWAT SONCO MEHER EIWAN TTOSE EYOU` prior to encrypting. If the message was sufficiently long (longer than 50 characters or so), the blocks of letters would be continued on a new line.

Write a pair of Maple procedures to accomplish this goal (in slightly more general terms).

The first should take as input a string, convert all lower-case letters to upper case, and afterwards, remove any characters that are not in a global variable called `Alphabet`. For this, consider using `UpperCase` and `Select` from the `StringTools` package. The second procedure should print this out in a format as described above (blocks of 5 letters, separated by spaces). I suggest `printf` for this.

As usual, demonstrate that your routines work with some appropriate test cases, with at least one short message as above, and another message of perhaps 100 characters or so. Note that your routine should work with a variety of alphabets.

26. (*expires 4/3*) The encrypted text below is a quote from Albert Einstein:

```
EINsteinc+eoplWcaewXoy.wNRjUkOeQaQQDARUZypyrmaFdnhZSdr-RaUzxpOvXc,Lv,lNLSTEINein
```

The encrypted text can be found in the file `einsteincrypt.txt`. It was encrypted using the `BigAffine` cipher we wrote in class (see the worksheet `Crypto.mw`). The alphabet used was 57 characters long, consisting of a space, the upper-case letters A-Z, a plus, the lower-case letters A-Z, a comma, a period, and a hyphen. That is (the first character is a space):

```
ABCDEFGHIJKLMNOPQRSTUVWXYZ+abcdefghijklmnopqrstu vwxyz.,-
```

`BigAffine` was used encrypting in blocks of eight letters at a time, and the name “Albert Einstein” appears in the plaintext (fortunately for you, it is in a convenient location, or this would be much harder).

Decrypt the quotation.

27. (*expires 4/3*) Modify the `BigAffine` cipher (see the worksheet `Crypto.mw`) so that instead of using a pair of large numbers  $a$  and  $b$  and a blocksize  $k$  as keys, these will be constructed from a passphrase, as follows.

First, split the passphrase into two halves (if the length of the phrase is odd, use the longer part to construct the shift  $b$ ). Then, choose the blocksize  $k$  so that the passphrase can be represented as two large integers.

As an example, if the passphrase is “TSEliot”, and with the 57-character alphabet of the previous problem, we take  $k = 4$ , and use  $a = 17348$  (corresponding to “TSE”) and  $b = 8842620$  (corresponding to “liot”). The following passage (using the key “TSEliot” and separating each line by a space)

```
Let us go then, you and I,
When the evening is spread out against the sky
Like a patient etherized upon a table.
```

```
encrypts to      xzLscDvHXxIHyw.VzAnHbcINu-ND,oOsJwNCylgnRN,OR oSqAPseIV-J
                  g,Sbq,QJgiHyawtzPthAqInlnIvREUQlvEDyPjyyUoiq,WpbHvjvIzS
```

(In the above crypttext, ignore the newlines. There is only one space.)

28. (expires 4/10) A Vignère cipher can be interpreted as a Caesar-like cipher on  $n$ -vectors, where  $n$  is the length of the key phrase. Can every affine encipherment on digraphs (two-character codes) be interpreted as an affine matrix encipherment on 2-vectors? That is, suppose I encode a message by affine enciphering on digraphs. Can I always get the same ciphertext from the same plaintext using an affine matrix enciphering (using a  $2 \times 2$  matrix) on 2-vectors?

If your answer is yes, prove it. If no, give a counterexample that cannot be so interpreted.

29. (expires 4/10) It was mentioned in class that the implementation of the `AffineMat` cipher (see `Crypto.mw`) could be adjusted to that if the shift vector  $b$  is omitted, the zero vector is used instead. Write a version of `AffineMat` that does this. More specifically, change the code so that `AffineMat(text, A)` works exactly the same as `AffineMat(text, A, b)` where  $b$  is the appropriate zero vector. Keep in mind that  $A$  may be of any size.

30. (expires 4/10) The difficulty of breaking a cipher can be increased by inserting some random characters (or noise) into a known part of the plain text in such a way that it will interact with the actual text (sometimes this insertion of randomness is called “salting the plaintext”).

As an example of this, recall that we discussed that if our character set came from an alphabet of length  $n$ , we could represent blocks of  $k$ -characters as numbers base  $n^k$  (for example, in the 53-character alphabet consisting of a space, upper-case letters and lower-case letters, the word `Hi` is represented by  $8 + 35 \cdot 53 = 1863$  if we use 2-character blocks).

If we agree that the first character of each block will be randomly chosen (and just ignored when we decrypt), breaking the encryption becomes much, much harder.

Modify the encryption scheme in `BigAffine` from `Crypto.mw` so that it can encrypt and decrypt including salt as the first character of each block.

As an explicit example, we encode the string `Zombie Apocalypse` using the 53-character alphabet and 3-character blocks (where the first character of each block is random noise). The given string corresponds to the list of character codes

[26, 41, 39, 28, 35, 31, 0, 1, 42, 41, 29, 27, 38, 51, 42, 45, 31]

which, when grouped into pairs and with a random character added as salt, gives me

[116551, 80721, 88936, 2842, 117404, 77428, 145275, 128676, 1652]

(your numbers may differ by up to 53 because of the salt); viewing these as 3-graphs including the salt, corresponds to `DZoBmbBieg AIpovcaBlyspIe`. If we encrypt this using the affine encryption  $x \mapsto 12347x + 56890 \pmod{53^3}$ , we get

[67005, 136439, 32930, 12092, 28729, 121189, 97219, 4118, 57985]

or `MsWQdvQlKHPDCLJeGqQfhkXACHT` (unless you used the same salt, your encryption will differ significantly, but both should decrypt just fine.)

If you were able to make this work, you should be able to decrypt the string<sup>1</sup>

`MWLiuWVckaMOpfHuWPgGuWlyQovqkwBwWV nLZYhrySYihTUSFqFJuGxEtvxCWNxPxstkPwkKxo`

which was encrypted using salted pairs (that is, 3-character blocks including salt) from the 53-character alphabet above, and applying the affine mapping  $x \mapsto 47x + 31415 \pmod{53^3}$ .

<sup>1</sup>also available as `zombiecrypt.txt` so you don't have to worry about typing errors.

31. (*expires 4/17*) When we implemented RSA in class, we represented our encrypted messages as a list of large numbers, rather than converting them to printable text. Sometimes we want a text representation. One way to do this is to use a base-64 representation, where the message  $m$  is converted to a base 64 number. This base 64 number is commonly represented with the upper-case characters A–Z representing digits 0 through 25, lower-case a–z representing digits 26 through 51, the characters 0–9 representing 52 through 61, and + and / representing 62 and 63, respectively.

If the message is longer than 64 characters, the encoded line is broken there (i.e., a newline is inserted). In some implementations, padding characters (usually =) are also added to ensure that the encoded text is of a length divisible by 4 (if the input is base 256 ASCII, this means three input characters correspond to four encoded characters). There are several variations of the base-64 encoding in common use.

Write a generalized implementation of this conversion process. Specifically, assume there is a global called `AlphabetOut` which contains the allowed characters in the encoding, ordered appropriately. Your procedure should take as input two arguments: a list of numbers in base  $n$ , and the base  $n$ . Your procedure should return a string representing the message in base  $b$ , where  $b$  is the length of `AlphabetOut`. Also write another procedure which undoes this conversion. Don't worry about inserting padding characters.

As an example<sup>2</sup>, the following `list of numbers` represents some text converted from ASCII (base 256) to base  $10^{47}$  (that is, without encryption):

```
6669013858395040150291124122141963456189571137, 79085785195062207278272120198122975492318184082,
15624867350544934942834543866565863795868490456, 55387683611779270304689525842891535523935500393,
23896957611465431133603100420167106476881540779, 78091587231828327640146863695263953922927490912,
9764606424846784132731915166644883269708742761, 24147181471923289394456210178528341598920602555,
59677642432524170063171614096094265077340147036, 101708358765089971113312874866
```

When transcribed into the base 64 encoding described above, we get:

```
BBCbv52ZgQXatVGIhd2bsASauBSYgcWYsFGe5BiZhJHLgYWYyBSY3FWeu4iLKoQS
0BSazBSYgAXZyl2bkBybmByYpZXasBydhJnLgIVZiVGBgowcwF2YlNHapB3csAyc
0JXarlmbnBiZy9WbgEGIoIGZkVmbgogYhNXZsACahZXZgc3buBCdoVWayBiZpJ3c
0BidpNGdvJXegoQYnFWauNHdgQHalBSZ2lGbgcUYsF2Y0l2YgUUbwlmcl5C
```

By the way, this text is from the opening to a well-known movie.

32. (*expires 4/17*) The procedures `StringToKgraph` and `KgraphToString` as defined in `Crypto.mw` have the following defect. Let  $\alpha$  represent the first character of the `Alphabet`. Then any occurrences of  $\alpha$  that appear at the end of a string are lost when converting to  $k$ -graphs and back.

For this problem, you should think of a way to fix this issue. You need to both implement and explain your solution.

As a concrete example, suppose we use the 10-letter alphabet `*123456789`. Then the command `StringToKgraph("*12***98*456***", 3)` gives the result `[210, 0, 89, 654]`, which `KgraphToString` converts back to `*12**98*456`.

There are a number of ways to solve this issue. Think of one, implement it, and explain why your way works, including some examples.

<sup>2</sup>Using Maple's convention of least-significant digit first, so the decimal number 123 is [59,1] (or 7B) in base 64.

33. (*expires 4/17*) The message below was encrypted using RSA with a key having the base

$$n = 27606985387162255149739023449107931668458716142620601169954803000803329$$

and the exponent

$$e = 95541407564551142884433930859007846184688349517132011538195190379009$$

The plaintext was represented in printable ASCII (base 128) in blocks of 32 letters at a time, and no padding.

[763135969033211128596541748452730974762878358020265079326172641096139,  
 20879815087895860022209511826785258055291427630017621830659043784235896,  
 5574407969259647015040456167101346596832809056832375987068556624523356,  
 21224197154621559219944504912186017011922165030059099210273090531937808,  
 12551200560613077704270621749705141076270903046687425935996313400405711,  
 18867900358254708499609170144443800027105466906756657749060030225245438,  
 4496337993898968047719657088708600524228317595964529102107251777431690,  
 9235737130358789283717978176700453123390494678379655510638922958288836,  
 3231140561089428768657095292397775917600836123018152094745253390870101,  
 82840704708021038125667422565345512548754665959685316382831252550171,  
 21039656037112093852283327710959368295150841772122729298435513871462186,  
 12041411940954720052070811665940863639535876777498117250838013124490438,  
 9413438705357919431318689662458482172376428983918258919377408820020874,  
 24344582781105714296470393649838967454596532389718150304278089340495219,  
 11666627210237277694133981546667501319351377137704324464898696799000305,  
 7678728878370382868719828867510796171125030253163810615836093095505785,  
 5850521474451619072915665399042845983658256530488470900878348493299278,  
 12796063700367369818580350073200291698274548230387522514837595194567646,  
 991710678121376154332316965121228090363454988579278882664135678580849,  
 5448263916134504769205437219736103649161232816051564930186689344069733,  
 331683831213526862116612352660410874927161591545716084674509520546695,  
 20911409982862166039437808848985365838241145413477157865204152349571315,  
 8446725165717024647474699066623651985526914825302054942325942578083958,  
 14694800659219414119256346254478510304289471490144936213050026188930109,  
 7890485067636181638866077827274071592238401748222991089801197812460720,  
 21236486045506721843702186793969054222520252187939247582471851381880906,  
 26957526821518528986780575261941374306276897675892965905302075045418371,  
 24677240511277808315835169523848692305481480201233529864615262657333913,  
 23499633482301313755682672041801597278928819855701032620066320680181087,  
 372227370145476230598908963364257918250207931059342487415859925223516]

Decrypt the message. (Hint: 70 decimal digits is too small to be secure.) So you don't have to retype everything, the values of  $n$ ,  $e$ , and the encrypted message are in the file [formulacrypt.txt](#).

34. (expires 4/24) Find a formula for all the solutions to the differential equation

$$\frac{dx}{dt}(t) = -2x(t), \quad t \in \mathbb{R}.$$

Among them, single out the one for which  $x(0) = 3$ . [Hint: read the help page for `dsolve`, or just do it in your head. It is that easy.]

35. (expires 4/24) Have Maple find analytic solutions to the following system of differential equations,

$$\begin{cases} y''(t) - z(t) = e^t, \\ z'(t) - y(t) = 0, \end{cases}$$

with initial conditions:  $y(0) = 1$ ,  $y'(0) = 0$ ,  $z(0) = k$ . Let us denote the solutions by  $y_k(t)$ ,  $z_k(t)$  (since they depend on the parameter  $k$ ).

For  $k$  taking all integer values from -10 to 10, and  $t \in [-4, 2]$ , plot the functions  $y_k$  in blue, and the functions  $z_k$  in red, all on the same graph. (Yes, you will then have 42 functions plotted on the same graph.) [This is certainly a case when you don't want to retype the functions that Maple finds. You will almost certainly need to read the help page for `dsolve`. I also found `subs`, `unapply`, and `seq` useful.]

36. (expires 4/24) For the functions  $y_k(t)$  and  $z_k(t)$  found in the previous problem, plot the parametric curves  $\varphi_k(t) = [y_k(t), z_k(t)]$  for integer values of  $k$  between  $-5$  and  $5$  and  $-6 < t < 4$  on the same graph. Use the `view` option of `plot` to only show what lies in the region  $-10 < y < 10$ ,  $-10 < z < 10$ , and use a sequence of colors so that each solution is a different color. [HINT: you might find something like `seq(COLOR(HUE, i/11), i=0..10)` useful for the latter.]

**NOTE:** The fact that there are various notations for differential equations is purely intentional.

37. (expires 5/4) Find all the fixed points of the system

$$\begin{cases} \dot{x} = x^2 + y, \\ \dot{y} = x(y^2 - 1), \end{cases}$$

where a “fixed point” is a solution for which **both**  $x(t)$  **and**  $y(t)$  are constant. For each of these solutions you find, describe the behavior of the solutions that have initial conditions nearby. You can use `Maple` to figure out what happens for nearby points, or you can use more mathematical methods.

38. (expires 5/4) Consider the differential equation  $\dot{\mathbf{z}}(t) = \mathbf{F}(\mathbf{z}(t))$ , where the vector  $\mathbf{z}(t) = (x(t), y(t))$  and the field  $\mathbf{F}(x, y) = (-y, x - y)$ . Plot a few solutions. What happens to them when  $t \rightarrow +\infty$ ? Give a “Maple-proof” that this is a general fact for *every* solution. [A “Maple-proof” is an argument that is rigorous once we accept Maple results as incontrovertibly true.]

39. (expires 5/4) For the equation  $\dot{\mathbf{z}} = \mathbf{F}(\mathbf{z})$ ,  $\mathbf{z} = (x, y)$ , with the vector field

$$\mathbf{F}(x, y) = \langle -x(x^4 + y^4) - y, x - y(x^4 + y^4) \rangle,$$

prove that the origin is an attractor in the future, i.e., every solution verifies

$$\lim_{t \rightarrow +\infty} \mathbf{z}(t) = 0.$$

Note that in this case, while you can (and probably should) use `Maple` to get an understanding and do calculations, you should format your answer as a regular mathematical proof.

40. (expires 5/4) We will study the Lotke-Volterra predator-prey equations: In a very simple ecosystem, at the time  $t$  (which is expressed, say, in years), there is a population of  $f(t)$  foxes and  $r(t)$  rabbits. The evolution of these quantities obeys the system

$$\begin{cases} \dot{f}(t) = G_f f(t) + E f(t) r(t), \\ \dot{r}(t) = G_r r(t) - E f(t) r(t); \end{cases}$$

where  $G_f$  and  $G_r$  are the growth rates for the foxes and the rabbits, respectively, in the absence of each other.  $E$  is the probability of a fatal encounter between a fox and a rabbit (normalized per number of foxes and rabbits).

First, write some words to explain why these equations make sense. Then, fix  $G_f = 0.4$ ,  $G_r = 2.4$  (it’s well-known that rabbits have the tendency to reproduce quickly) and  $E = 0.01$ . For a few initial conditions of your choice, plot the trajectories in the  $(f, r)$ -plane (say, with  $0 \leq f \leq 1000$  and  $0 \leq r \leq 1000$ ). For the same initial conditions, plot the actual solutions too (i.e,  $f(t)$  against  $t$ , and  $r(t)$  against  $t$ ). Write some comments interpreting how the behaviour of the solutions relates to what happens to the two species.

Finally, repeat the same procedure with  $G_f = -1.1$ . Things change substantially. Again, what is the “physical” interpretation of this?