Introduction to Maple (Math 502)

Assignments

Spring Semester, 2007

End of Semester Schedule

Wed., May. 16:

Final Examination: 4:00 – 6:00 p.m.

Tue., May. 15:

Office Hours: 5:30 – 6:30 p.m.

Mon., May. 14:

Office Hours: 3:30 – 4:30 p.m.

Fri., May. 11:

Office Hours: 2:30 – 3:30 p.m.

Assignments are listed by the **date due**.

If your browser is prepared to handle MathML, you should use the XHTML version of this page; if not, you should view the classical HTML version. PDF and DVI (requires *TeX*[1] software) versions of this page are available for printing.

Most of these assignments are simply casual exercises designed to prepare you for tests and the written assignments. While you may find it helpful to discuss the casual exercises with others, **no collaboration is permitted on the written assignments**.

Mon., May. 7:

Written Assignment No. 5[2] (PDF[3] for printing —classical HTML[4] for terminal window browsing) is due.

Wed., May. 2:

Exercises: Let E denote the cubic curve $y^2 + xy + 2y = x^3 + 3$.

1. Find a point on E over the field $\mathbf{Z}/5\mathbf{Z}$ of largest possible order.
2. Can every one of the printable ASCII codes (range 32 – 127) actually be represented by a point of E in the field $\mathbf{Z}/1283\mathbf{Z}$ by the method described in class (and on the next assignment sheet) when up to 10 attempts are made for each value? If not, which characters cannot be represented? What happens if 11 attempts are made for each value?
3. Continuing in the vein of the previous exercise represent the 3 character string `"abc"` as a point on E in the field $\mathbf{Z}/1283\mathbf{Z}$ with up to 10 attempts at representation for each value and then encrypt the resulting sequence of 3 points on E using the public key
$$b = [147, 376] \quad c = [706, 905] \quad .$$
4. What secret key was used to construct the public key of the previous exercise?

---

[1] URI: http://www.tug.org/
[2] URI: ampl070507.xhtml
[3] URI: ampl070507.pdf
[4] URI: ampl070507.html

Mon., Apr. 30:

Exercises from the text:

262: 6, 7, 12 – 14, 16, 17, 20, 21, 24, 25

Wed., Apr. 25:

Read: §§ 10.5, 10.6

224: 3 – 5
260: 3 – 5

Mon., Apr. 23:

Written Assignment No. 4[5] (PDF[6] for printing —classical HTML[7] for terminal window browsing) is due. (The due date had previously been set as Wednesday, April 18.)

Code for addition of points on cubic curves will be added to the web at `http://www.albany.edu/~hammond/maple/` after this class meeting.

Wed., April. 18:

Study the slides (also available as PDF or DVI or classical HTML) about addition of points on cubic curves.

The slides now incorporate material from our class on April 18 as well as the class on April 16. They were last revised on April 19.

Mon., Apr. 16:

Read: §§ 10.1 – 10.2

260: 1, 2
And this: Find the area enclosed by the loop of the cubic curve $y^2 = x^3 - x$. Repeat for the cubic curve $y^2 = x - x^3$.

Wed., Apr. 11:

Read: §§ 9.1 – 9.2

224: 1, 2
And this: Find the polynomials $p_n(x)$ such that

$$\frac{d^n}{dx^n} \exp(-1/x^2) \;=\; \frac{p_n(x)}{x^{3n}} \cdot \exp(-1/x^2)$$

for $1 \leq n \leq 7$. Can you give a general recursive formula for $p_n(x)$?

Apr 2 – 9

University Recess: no classes

Wed., Mar. 28:

Written Assignment No. 3[8] (PDF[9] for printing —classical HTML[10] for terminal window browsing) is due.

Mon., Mar. 26:

Read: §§ 7.4 – 7.6, 8.6 – 8.8

1. Do these: **188:** 3, 4, 5
2. Explore the *Maple* function for finding primitive roots mod m, which is `numtheory[primroot]`.

   a. Find the smallest primitive root modulo 289 that is larger than 100.
   b. Find the smallest positive non-prime primitive root mod 40487.

[5] URI: ampl070418.xhtml
[6] URI: ampl070418.pdf
[7] URI: ampl070418.html
[8] URI: ampl070328.xhtml
[9] URI: ampl070328.pdf
[10] URI: ampl070328.html

c. Find the smallest positive number that is primitive modulo both 101 and 103. Is it primitive mod $101 * 103$?
d. If c is primitive modulo both 101 and 103, what congruence condition on integers $j, k \geq 0$ is equivalent to the condition that $c^j \equiv c^k \pmod{101 * 103}$?

3. Let p be the prime $128^{15} + 39$. Without trying to solve determine which of the following two congruence equations is solvable:

$$2^m \equiv 11 \pmod{p} \quad \text{and} \quad 11^n \equiv 2 \pmod{p} \quad .$$

Are you able to solve the solvable one?

Wed., Mar. 21:

Read: §§ 7.1 – 7.3

174: 5
188: 1, 2
And this: Continuing in the context of the last exercise in the previous assignment, you are now being told that the squeezed vector

```
[712147006187606979338143444233878549915653153140991743218564586,
 178662110035670707980478101565179804104129000440104920382724 7506,
 178218464390344153588593775606773530197498395114930528167896 2346,
 163900000883963270754668016781567564138725921368741819365794 0006,
 153596008918554965470600453478709448350503748936131298443635 0635,
 119579929784490996418841055711469298342706418563344721905491 1622,
 152923690247191873437148322535394252287547399041641100975774 2702,
 409979669999633360347425246927425729369778446996539051720679 885,
 180560060897478871983834744342649877926691664886532562267584 9897,
 105898364470892776691830932095598110359425070121051212772543 9642]
```

(where k is maximum, as before, for the given modulus m) may be decrypted with the exponent

$$d \;=\; 679417638057246102387290084428241348920601574129013039486178441 \quad .$$

A. Decrypt it, expand its terms in base 128, and convert the resulting vector, regarded as a sequence of ASCII codes, to a string.

B. Can you determine what the encrypting exponent was?

Mon., Mar. 19:

Read: §§ 6.1 – 6.3

174: 1 – 3; disregard the last sentence in exercise 1.
And this: Given a vector of digits in base 128 what is the largest block size k for squeezing the vector into a vector of digits for base 128^k so that the resulting squeezed vector can be faithfully encrypted by taking a suitable power of each entry modulo the integer

$$m \;=\; 24682568359818090632324537738408732533693765476816931880802737 39$$

under the hypothesis, which is satisfied here, that the integer m is square-free?

Wed., Mar. 14:

Midterm Test in class

Mon., Mar. 12:

A light assignment prior to the midterm test:

- **Bring review questions.**
- Use network resources to find *Maple* code for solving *Sudoku* puzzles, and then find out how long it takes *Maple* to solve this one:

		8				1		2
	7		1				9	4
			3			5		
	8			4		9		
			8	1	5			
		1		6			4	
		5			7			
7	9				6		1	
6		4				2		

WARNING: Be careful when downloading code from the network. First make sure a location where you find code is trustworthy, and then look over any code before running it.

Wed., Mar. 7:

Written Assignment No. 2[11] (PDF[12] for printing —classical HTML[13] for terminal window browsing) is due.
Code for vector shifting of the type used in problem 5 may be found at `http://www.albany.edu/~hammond/maple/`.

Mon., Mar. 5:

Read: §§ 5.3 – 5.4

151: 3 – 5
And this: Conduct some experiments in cryptography using computers[14] (PDF[15] for printing —classical HTML[16] for terminal window browsing).

Wed., Feb. 28:

Announcement: The midterm test will be held on Wednesday, March 14.
Read: §§ 5.1 – 5.2

151: 1, 2
And this: Write a Maple procedure that given a univariate polynomial $f(x)$ and a polynomial $b(x)$ of degree at least 1 returns the vector of coefficients $c_j(x)$ for the b-adic expansion of $f(x)$

$$f(x) \;=\; \sum_{j\geq 0} c_j(x) b(x)^j$$

where $\deg(c_j(x)) < \deg(b(x))$ for each $j \geq 0$.

Mon., Feb. 26:

Scan: Chapter 4
Exercises:

137: 1, 4
And this: Write a Maple procedure that given a base $b \geq 2$ and a triple of vectors equivalent to the base b representation of a positive rational number — each vector consisting of digits relative to the base b, with the vectors in order being (a) the digit sequence (possibly empty) to the left of the decimal point, (b) the digit sequence (possibly empty) to the right of the decimal point before the repetition pattern, and (c) the digit sequence (if any) that repeats — returns the positive rational number as a fraction m/n where m and n are positive integers without common divisor.

Week: Feb 19 – 23

University Recess: no classes

[11] URI: ampl070307.xhtml
[12] URI: ampl070307.pdf
[13] URI: ampl070307.html
[14] URI: cbc.xhtml
[15] URI: cbc.pdf
[16] URI: cbc.html

Wed., Feb. 14:

No meeting. The University has announced that, due to severe snow conditions, all day and evening classes on February 14 are cancelled.

Comment on exercise **93:** 6[17] (PDF[18] for printing —classical HTML[19] for terminal window browsing)

Mon., Feb. 12:

Read: §§ 3.4 – 3.6
Exercises:

93: 6 – 10
And this: Write a Maple procedure that when given a finite continued fraction, presented as the vector $[a_0, a_1, a_2, a_3, \ldots, a_n]$ representing

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ldots + a_n}}} \ ,$$

with the a_i all integers and $a_i \geq 1$ for $i \geq 1$, returns the rational number it represents.

Wed., Feb. 7:

Written Assignment No. 1[20] (PDF[21] for printing —classical HTML[22] for terminal window browsing) is due.

Mon., Feb. 5:

Read: §§ 3.1 – 3.3
Exercises:

63: 12, 13
93: 1 – 5
And this: Examine all iterates of the Syracuse function applied to each integer n up to $10,000$ and find the integer n in that range having an iterate $s_k(n)$ for which the ratio $s_k(n)/n$ of the iterate to the starting integer is largest. *Hint:* If the problem is modified to consider only integers n up to 100, then the integer in that smaller range having an iterate with largest ratio is 27, and the iterate presenting the largest ratio is $s_{77}(27) = 9232$.

Wed., Jan. 31:

Read: §§ 2.5 – 2.6
Exercises:

63: 6 – 11
And this: ssq will be the name for the function defined by

$$\text{ssq}(n, b) \ = \ 1 + \ \text{(sum of the squares of the base } b \text{ digits of } n) \quad .$$

Maple code for this function may be found at `http://www.albany.edu/~hammond/maple/`. In that code if the second variable b is not specified, then it is understood to be 10.

Conduct experiments with the base b having the values 2, 3, 5, and 6 to try to determine what happens when ssq is iterated starting from various positive integers n.

Mon., Jan. 29:

Read: §§ 2.1 – 2.4
Exercises:

[17] URI: recurunassign.xhtml
[18] URI: recurunassign.pdf
[19] URI: recurunassign.html
[20] URI: ampl070207.xhtml
[21] URI: ampl070207.pdf
[22] URI: ampl070207.html

63: 1 – 5
And this: The Syracuse function s is defined for integers n by

$$s(n) \;=\; \begin{cases} 1 & \text{if } n \le 1 \\ 3n+1 & \text{if } n > 1 \text{ is odd} \\ n/2 & \text{if } n > 1 \text{ is even} \end{cases}$$

The *iterates* of s are

$$s_1(n) \;=\; s(n),\; s_2(n) \;=\; s(s(n)),\; s_3(n) \;=\; s(s(s(n))), \ldots \quad .$$

For example, $s_1(6) = s(6) = 3$, $s_2(6) = s(3) = 10$, $s_3(6) = s(10) = 5$, $s_4(6) = s(5) = 16$, $s_5(6) = s(16) = 8$, $s_6(6) = s(8) = 4$, $s_7(6) = s(4) = 2$, $s_8(6) = s(2) = 1$. Since the 8th iterate of s applied to 6 is 1, all higher iterates of s applied to 6 are 1.

Find the 5 smallest values of n for which the first $2n+1$ iterations of s applied to n fail to yield 1.

Wed., Jan. 24: Acquire the textbook[23]. Read through chapter 1, and try some of what is sketched there for yourself in *Maple*.

About free *general purpose* computer algebra systems: The following items were found through a web search, but none of them have been reviewed.

Axiom [24]

Axiom has been in development since 1973 and was sold as a commercial product. It has been released as free software under the Modified BSD License. It is sponsored by CAISS, the Center for Algorithms and Interactive Scientific Software, at The City College of New York.

Maxima [25]

Maxima is a descendant of *Macsyma*, the computer algebra system developed in the late 1960s at the Massachusetts Institute of Technology. It is free under the GNU General Public License subject to some export restrictions from the U.S. Department of Energy. A proprietary version of *Macsyma* is also available.

Mon., Jan. 22:

First meeting: No assignment.

UP | TOP | Department

[23] URI: ../i502s2007.html#textbook
[24] URI: http://savannah.nongnu.org/projects/axiom
[25] URI: http://maxima.sourceforge.net/