Introduction to Maple (Math 502) Assignments

Spring Semester, 2008

Thu., May. 8:

Final Examination: 4:00 – 6:00

Blog of last minute questions[1] (PDF[2] for printing —classical HTML[3] for terminal window browsing)
Note: this page may have changed since the last time you looked at it. Therefore, **reload** it each time you look at it.

Wed., May. 7:

Office hours: 3:00 – 5:00

Tue., May. 6:

Last regular class meeting. **Bring questions** for review.

Thu., May. 1:

Written Assignment No. 5[4] (PDF[5] for printing —classical HTML[6] for terminal window browsing) is due.

Tue., April. 29:

1. Convert the word "sage" to its vector of ASCII codes and then use El Gamal encryption for multiplicative arithmetic modulo the prime 257 to encrypt these values using the formula
$$x \mapsto [b^k, x \cdot c^k] \pmod{257}$$
where $b = 102$ and $c = 150$ employing for the 4 characters the 4 successive values $k = 11, 12, 13, 14$.
2. How can the word "sage" be recovered from the four pairs of values modulo 257 that were obtained in the preceding exercise?
3. A message is waiting for you at the url

   `http://math.albany.edu/~hammond/maple/pvc` .

   The El Gamal key for decoding it as 950. What is the content of the message?

Added after the class: Solution of Exercise 3[7] (PDF[8] for printing —classical HTML[9] for terminal window browsing).

Thu., April. 24:

Do these these exercises[10] (PDF[11] for printing —classical HTML[12] for terminal window browsing).

[1] URI: raq502s2008.xhtml
[2] URI: raq502s2008.pdf
[3] URI: raq502s2008.html
[4] URI: ampl080501.xhtml
[5] URI: ampl080501.pdf
[6] URI: ampl080501.html
[7] URI: msol080429.xhtml
[8] URI: msol080429.pdf
[9] URI: msol080429.html
[10] URI: mp080424.xhtml
[11] URI: mp080424.pdf
[12] URI: mp080424.html

Tues., Apr. 22:

Read: §§ 10.5, 10.6

224: 3 – 5
260: 3 – 5
And this:
For the cubic curve $y^2 = x^3 - 43x + 166$:

(a) Find a point with rational coordinates that has order 7.
(b) How many points lie on this curve in the field $\mathbf{Z}/41\mathbf{Z}$?
(c) Find examples of points on the curve in the field $\mathbf{Z}/41\mathbf{Z}$ having the orders 2, 3, 6, 7, 14, 21, and 42.

Thu., April. 17:

Written Assignment No. 4[13] (PDF[14] for printing —classical HTML[15] for terminal window browsing) is due.

Tue., April. 15:

Become familiar with the functions for cubic curves found at the course's code archive, `http://www.albany.edu/~hammond/maple/`.

Use this introduction[16] (PDF[17] for printing —classical HTML[18] for terminal window browsing) as a beginning guide.

Thu., April. 10:

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

Tue., Apr. 8:

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 $y^2 = x - x^3$.

Thu., Apr. 3:

Written Assignment No. 3[19] (PDF[20] for printing —classical HTML[21] for terminal window browsing) is due.

Tue., Apr. 1:

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

Tue., Thu., Mar. 25, 27:

No classes: university recess.

Thu., Mar. 20:

Read: §§ 7.4 – 7.6, 8.6 – 8.8

[13] URI: ampl080417.xhtml
[14] URI: ampl080417.pdf
[15] URI: ampl080417.html
[16] URI: mp080415.xhtml
[17] URI: mp080415.pdf
[18] URI: mp080415.html
[19] URI: ampl080403.xhtml
[20] URI: ampl080403.pdf
[21] URI: ampl080403.html

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.
   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?

Tue., Mar. 18:

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,
 1786621100356707079804781015651798041041290004401049203827247506,
 1782184643903441535885937756067735301974983951149305281678962346,
 1639000008839632707546680167815675641387259213687418193657940006,
 1535960089185549654706004534787094483505037489361312984436350635,
 1195799297844909964188410557114692983427064185633447219054911622,
 1529236902471918734371483225353942522875473990416411009757742702,
 409979669999633360347425246927425729369778446996539051720679885,
 1805600608974788719838347443426498779266916648865325622675849897,
 1058983644708927766918309320955981103594250701210512127725439642]
```

(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?

A *Maple*-readable file containing values for m and d may be found at

`http://www.albany.edu/~hammond/maple/mud.`

Thu., Mar. 13:

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

$$m \;=\; 2468256835981809063232453773840873253369376547681693188080273739$$

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

Tue., Mar. 11:

Midterm Test (in class)

Thu., Mar. 6:

Bring **review questions**
Read: §§ 5.3 – 5.4

151: 3 – 5
And this: Conduct some experiments in cryptography using computers[22] (PDF[23] for printing —classical HTML[24] for terminal window browsing).

Tue., Mar. 4:

Written Assignment No. 2[25] (PDF[26] for printing —classical HTML[27] 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/`.

Thu., Feb. 28:

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 $j \geq 0$.

Tue., Feb. 26:

Announcement: The midterm test will be held on Tuesday, March 11.
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.

Use the function *bdc* provided in the code archive at `http://www.albany.edu/~hammond/maple/` to compute the base 10 vector triple for the rational number

$$\frac{23558948078476687}{249999999997500}\,,$$

and then use the code you have written to reconstruct the rational number.

Thu., Feb. 21:

Read: §§ 8.1 – 8.4
Exercises:

[22] URI: cbc.xhtml
[23] URI: cbc.pdf
[24] URI: cbc.html
[25] URI: ampl080304.xhtml
[26] URI: ampl080304.pdf
[27] URI: ampl080304.html

1. Study the formulas and do the exercise found in this web page[28] (PDF[29] for printing —classical HTML[30] for terminal window browsing).
2. What rational number is represented in base 8 by the vector triple

$$(u, v, w) \;=\; ([2], [1], [1, 5, 4, 6, 6, 3, 3])\ ?$$

Tue., Feb. 19:

No class; the University will be in recess.

Thu., Feb. 14:

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

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

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

Tue., Feb. 12:

Written Assignment No. 1[31] (PDF[32] for printing —classical HTML[33] for terminal window browsing) is due.

Thu., Feb. 7:

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 $s_{77}(27) \;=\; 9232$.

Tue., Feb. 5:

Read: §§ 2.5 – 2.6
Exercises:

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

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

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.

Online slides (Firefox or IE+MathPlayer or PDF) for the class are available.

[28] URI: codeproblem.xhtml
[29] URI: codeproblem.pdf
[30] URI: codeproblem.html
[31] URI: ampl080212.xhtml
[32] URI: ampl080212.pdf
[33] URI: ampl080212.html

Thu., Jan. 31:

Read: §§ 2.1 – 2.4
Exercises:

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

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

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.

Post assignment: online slides (Firefox or IE+MathPlayer or PDF) for the last exercise are available.

Tue., Jan. 29: Acquire the textbook[34]. 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 [35]
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 [36]
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.

SAGE [37]
SAGE is something relatively new that is not a computer algebra system but rather a free unifying framework for various computer algebra systems, free and non-free, such as *Maple*, *Mathematica*, *Axiom*, *Maxima*, and a number of specialist systems. *SAGE* can be operated, even across the network (though usually not without permission), in the window of a web browser.

Thu., Jan. 24:

First meeting: No assignment.

---

[34] URI: ../i502s2008.html#textbook
[35] URI: http://savannah.nongnu.org/projects/axiom
[36] URI: http://maxima.sourceforge.net/
[37] URI: http://www.sagemath.org/