Modern Computing for Mathematicians (Math 587)

Assignments

Spring Semester, 2009

Assignments are listed in reverse chronological order, i.e., most recent first, and labeled by the date due.

Tue., May. 5:

> **Written Assignment No. 5**[1] (PDF[2] for printing —classical HTML[3] for terminal window browsing) is due.
>
> > Bring wrap-up questions

Thu., Apr. 30:

> Review the *Sage*[4] code for functions related to the use of the El Gamal technique with an elliptic curve over a prime field $\mathbf{F}_p$. Note, however, that the task of writing functions for the actual encryption and decryption of point sequences is left to the reader.
>
> 1. Write *Sage* functions for encrypting and decrypting point sequences on an elliptic curve over $\mathbf{F}_p$. For the purpose of being able to compare answers use the provided function *randfake*, rather than an actual random number generator, with first argument the number of points on the curve and second argument the sequence-postion (beginning with 1) of the current point in the sequence.
>
> 2. With the curve $y^2 = x^3 + 43x + 13$ over the prime field of size 1283 use the provided function *codestopoints* with 10 "tries" to generate a point sequence corresponding to the list of ASCII codes
> $$[1, 2, 3, 4, \ldots, 126, 127] \quad .$$
> What is the smallest number of "tries" that will provide a list of 127 points for this code sequence?
>
> 3. Test your functions by encrypting and then decrypting the point sequence obtained in the previous exercise with 10 "tries" on the curve $y^2 = x^3 + 43x + 13$ in the field $\mathbf{F}_{1283}$. For this purpose use as base point $b = [0, 36]$ and as secret key the integer 97.
>
> Schedule for this class:

Time	Presenter	Topic
4:15	A. L.	Singular
4:40	W. H.	elliptic El Gamal

Tue., Apr. 28:

> Read about the use of El Gamal on Elliptic Curves[5] (PDF[6] for printing —classical HTML[7] for terminal window browsing).
>
> A message encrypted by a list of pairs of points on an elliptic curve is waiting for you at the url
>
> > `http://math.albany.edu/pers/hammond/course/mat587s2009/assgt/psrt` .

---

[1] URI: amcm090505.xhtml
[2] URI: amcm090505.pdf
[3] URI: amcm090505.html
[4] URI: sage/elgell.sage
[5] URI: http://math.albany.edu/pers/hammond/course/mat587s2009/eelg.xhtml
[6] URI: http://math.albany.edu/pers/hammond/course/mat587s2009/eelg.pdf
[7] URI: http://math.albany.edu/pers/hammond/course/mat587s2009/eelg.html

The El Gamal key for decoding it is 950.

1. What sequence of points on the curve was encoded?

2. What is the content of the message?

3. Re-encrypt the message relative to $[1, 338]$ as base point using the public key determined by the same secret key, and then decode that.

Note: In *Sage* the function *chr()* is inverted by the function *ord()*. See the *Python* documentation[8] about built-in functions. See also *unichr()*.

Schedule for this class:

Time	Presenter	Topic
4:15	A. M.	Texmacs
4:40	J. Y.	R
5:05	W. H.	elliptic El Gamal

Thu., Apr. 23:

Read this primer on group theory in *Sage*.

What built-in function in *Sage* will, for a given pair (a, b) of integers, produce integers (r, s) such that $\gcd(a, b) = ra + sb$?

Write a function for *Sage* that, given a list of integers representing a finite continued fraction, returns the rational number having that continued fraction expansion without using a built-in function. What built-in function can be used for the same task?

Schedule for this class:

Time	Presenter	Topic
4:15	B. S.	Texinfo
4:40	W. H.	Sage

Tue., Apr. 21:

Read the third group of 3 sections of the *Guided Tour* in the online *SAGE* Tutorial.

Review for the purpose of comparison code for sifting primes[9] (also available as PDF[10] or DVI[11]) smaller than a given bound in the languages of (1) *gp* and (2) *sage*.

Schedule for this class:

Time	Presenter	Topic
4:15	W. K.	Octave
4:40	M. G.	Kash
5:05	W. H.	Sage

Thu., Apr. 16:

Read the second group of 3 sections of the *Guided Tour* in the online *SAGE* Tutorial.

Schedule for this class:

Time	Presenter	Topic
4:15	postponed	
4:40	J. P.	Maxima
5:05	W. H.	Sage

Tue., Apr. 14:

Read the first 3 sections of the *Guided Tour* in the online *SAGE* Tutorial[12].

Schedule for this class:

---

[8]URI: http://docs.python.org/library/functions.html
[9]URI: ../sifting.html
[10]URI: ../sifting.pdf
[11]URI: ../sifting.dvi
[12]URI: http://www.sagemath.org/doc/tutorial/index.html

Time	Presenter	Topic
4:15	A. B.	Open Office math
4:40	K. D'A	GAP
5:05	W. H.	Sage

Tue., Apr. 7:

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

Updated student presentation schedule[16] (PDF[17] for printing —classical HTML[18] for terminal window browsing).

Thu., Apr. 2:

The GELLMU Project[19] offers the use of LaTeX-like markup to write for an SGML document type. Begin to become familiar with the *Manual* (also available as PDF or DVI or classical HTML) and the *Introductory User's Guide to Regular* GELLMU (also available as PDF or DVI or classical HTML). My honors calculus notes on the Gamma function provide an example. The following files are in the production chain: generalized LaTeX source, equivalent SGML, which should have line-by-line alignment with the source, under this SGML DTD[20], XML shadow under this XML DTD[21], spawned XHTML + MathML, spawned LaTeX, and PDF made from the spawned LaTeX.

Re-do the exercise of the previous assignment by preparing a single "regular" GELLMU source file and then, on `chern`, run the command `gellmu` on that file.

Demo files used in class on March 31: *ghtml* (HTML) is in the open directory `glm/`. *ghack4* (hack) is in the open directory `hack/`. *gamma* ("regular") is in the open directory `http://math.albany.edu/pers/hammond/course/calcnotes/`.

Updated student presentation schedule[22] (PDF[23] for printing —classical HTML[24] for terminal window browsing).

Tue., Mar. 31:

Begin to become familiar with Mathematical Markup Language (MathML)[25]. Note that under the current specification, incorporated in an XML document type definition[26], MathML may be included only in the XML form of HTML and then only using the MathML namespace. (The online form of this assignment sheet is an example.)

1. What elements in the document type definition[27] for *hack* have yet to receive suitable treatment in the *sgmlspl* script `hack/hack2html.pl`? Add text to your copy of hack/hack3.sgml[28] so that these are exercised, and extend the code in the *sgmlspl* script to accommodate them.

2. Prepare two small documents, one PDF and the other XHTML+MathML that typeset the formula
$$\frac{\pi}{2} \;=\; \int_0^1 \frac{dx}{\sqrt{1-x^2}}$$
in a display (as here). Be sure to use (on `chern`) the program `sp-utf8-xmlvalid` to validate the XHTML+MathML

---

[13]URI: amcm090407.xhtml
[14]URI: amcm090407.pdf
[15]URI: amcm090407.html
[16]URI: ../pressch.xhtml
[17]URI: ../pressch.pdf
[18]URI: ../pressch.html
[19]URI: http://www.albany.edu/~hammond/gellmu
[20]URI: gellmudtd.txt
[21]URI: axgellmudtd.txt
[22]URI: ../pressch.xhtml
[23]URI: ../pressch.pdf
[24]URI: ../pressch.html
[25]URI: http://www.w3.org/Math/
[26]URI: http://www.w3.org/Math/DTD/mathml2/xhtml-math11-f.dtd
[27]URI: hack/hackdtd.txt
[28]URI: hack/hack3.txt

Updated student presentation schedule[29] (PDF[30] for printing —classical HTML[31] for terminal window browsing).

Thu., Mar. 26:

Examples of SGML/XML processing based on *sgmlspl* may be found in the GELLMU[32] distribution as well as in the *sgmlspl* distribution from CPAN that was referenced in the previous assignment.

1. hack/hack2.sgml contains the document instance associated with the previously considered hack/hack1.sgml but with a reference in its prolog to the separate (and expanded) document type definition hack/hack.dtd. What differences do you find in the ESIS output obtained by parsing hack1 and hack2 with *onsgmls*?

2. Morph the separate document type definition hack/hack.dtd into an XML document type definition shadowing it but using lower case names.

3. Write an *sgmlspl* script for translating documents under hack/hack.dtd to an XML document type shadowing it but using lower case names.

   (a) Use this script to translate hack/hack2.sgml to the XML shadow document type.
   (b) Use the program `sp-xmlvalid` found on `chern` (or on `itsunix`) to validate your XML version of hack2 after making sure that the XML version has a SYSTEM reference in its prolog to your XML document type definition.
   (c) What modifications would be needed to your *sgmlspl* script for translation to HTML so that it can be used with your XML version of hack2?

Tue., Mar. 24:

1. Read about the use of *sgmlspl*[33] for translating SGML (or XML) documents. There is also a chapter on *sgmlspl* in *The LaTeX Web Companion.*

2. Use *sgmlspl* (for example, on `chern`) with the script `hack/skel.pl` (from the *sgmlspl* distribution) to create a skeleton *sgmlspl* script for translation of the SGML document hack/hack1.sgml.

3. Fill in the skeleton script to morph it into an *sgmlspl* script for translation of hack1.sgml to an HTML document.

Thu., Mar. 19:

Written Assignment No. 3[34] (PDF[35] for printing —classical HTML[36] for terminal window browsing) is due.
student presentation[37] (PDF[38] for printing —classical HTML[39] for terminal window browsing) schedule.

Tue., Mar. 17:

Student Presentation Topic Auction[40]

Thu., Mar. 12:

Use `gp-2.3` for the following:

1. For the curve $y^2 + y = x^3 + x^2$ compute the points kA for $2 \leq k \leq 10$ when A is the rational point $A = [0,0]$.

---

[29] URI: ../pressch.xhtml
[30] URI: ../pressch.pdf
[31] URI: ../pressch.html
[32] URI: http://www.albany.edu/~hammond/gellmu/
[33] URI: http://cpansearch.perl.org/src/DMEGG/SGMLSpm-1.03ii/DOC/HTML/sgmlspl/sgmlspl.html
[34] URI: amcm090319.xhtml
[35] URI: amcm090319.pdf
[36] URI: amcm090319.html
[37] URI: ../pressch.xhtml
[38] URI: ../pressch.pdf
[39] URI: ../pressch.html
[40] URI: ../projs.html

2. Determine the isomorphism class of the group of points on the curve $y^2 = x^3 - 1$ in the field $\mathbf{F}_p$ for the following values of the prime p: $11, 13, 37, 47, 61, 107, 109$.

Some of the auxiliary routines in `code/ell` may be helpful.

Tue., Mar. 10:

Continue reading about the arithmetic on an elliptic curve. Use the native routines available in `gp-2.3` to perform the following operations in the arithmetic of the elliptic curve $y^2 = x^3 - 7x + 10$:

1. $[-1, 4] + [2, 2]$
2. $[5, 10] - [3, 4]$
3. $6 \cdot [1, 2]$

Thu., Mar. 5:

Begin to become familiar with arithmetic on an elliptic curve by looking over these items:

1. *Wikipedia article*[41]
2. Course slides: `addelli.xhtml` (PDF for printing).
3. Sections of the *Pari/GP Tutorial* and *User's Guide* on elliptic curves. (Copies of the *Pari/GP* documents may be found on `chern` in `/math/local/doc/apps/pari`.)

Tue., Mar. 3:

Written Assignment No. 2[42] (PDF[43] for printing —classical HTML[44] for terminal window browsing) is due.

Thu., Feb. 26:

LaTeX-related examples for study in connection with Written Assignment No. 2 may be found in the course web at `assgt/tex/` in the items having names that begin with `"assgt2-example"`. (The XHTML + MathML files were made from LaTeX source using `mzlatex`.)

Exercises:

1. No LaTeX source is provided for the variant form `assgt/tex/assgt2-examplea.pdf`. Try creating LaTeX source that may be used to generate this variant.
2. Use `gp` to assist with investigations of the iterative behavior of certain generalizations of the Syracuse function described in this handout: `assgt/linmadecoprime.xhtml` (or `assgt/linmadecoprime.pdf`)

Tue., Feb. 24:

Tasks:

1. Explore the web for free software that can be used to translate HTML to LaTeX.
2. Explore the web for free software that purports to translate LaTeX to HTML.
3. Try using the *tex4ht* commands `htlatex` and `mzlatex` (as found on chern) to translate the documents found in the course web at `assgt/tex/`.
4. Try out El Gamal cryptography using the *gp* code from the file in the course web at `assgt/code/elg`.

Thu., Feb. 12:

Reading about (1) LaTeX and (2) topics in cryptography:

1. LaTeX
   Some introductory things available at the *Comprehensive TeX Archive Network* – CTAN[45] (for which local copies are available):

---

[41]URI: http://en.wikipedia.org/wiki/Elliptic_curve
[42]URI: amcm090303.xhtml
[43]URI: amcm090303.pdf
[44]URI: amcm090303.html
[45]URI: http://www.ctan.org

> *Very short guide*[46]
> *Formatting information*[47]
> *Not so short introduction*[48]

    2. Cryptography

        Diffie Hellman key exchange[49] (at Wikipedia)

        El Gamal encryption[50] (at Wikipedia)

Tasks:

1. Rewrite your HTML response to assignment no. 1 in LaTeX. Then (a) use the program `latex`, e.g., on chern, to make a DVI file (viewable with a DVI reader such as `xdvi`) and (b) use the program `pdflatex` to make a PDF file (viewable with, as available, `xpdf`, or `gpdf`, or *Adobe Reader*$^{\mathrm{TM}}$, or . . .)

2. Write one or more functions for *gp* to facilitate the tasks of two cooperating partners using Diffie-Hellman key exchange with the multiplicative group of $\mathbf{Z}/p\mathbf{Z}$ (the integers modulo p) for a given prime p.

Tue., Feb. 10:

Written Assignment No. 1 Submit this assignment through your University at Albany web site at the (relative) URL `mat587s09/assgt1.html`. (Make sure that it is a valid HTML document.) The HTML *body* should consist of an ordered list (i.e., *ol*) with two items (i.e., two *li*'s) corresponding to the two assigned tasks.

1. Write a function *cfas* for *gp-2.3* (the command line interface to *Pari/gp*, version 2.3) that, given a rational number, returns the alternating sum of the integers in its finite continued fraction expansion. More precisely, if r is the given rational number and

$$r \;=\; a_1 + \cfrac{1}{a_2 + \frac{1}{a_3 + \ldots + \frac{1}{a_n}}}$$

its (finite) continued fraction expansion, the function will return the integer

$$a_1 - a_2 + a_3 - + \ldots + (-1)^{n+1} a_n \quad .$$

Once your code is working correctly, for your submitted response to this task place the listing of your code for *cfas* verbatim in `assgt1.html` using the HTML *pre* element.

2. Using *gp-2.3* and the function you wrote in the previous task determine the alternating sum of the 30th convergent of π[51]

> **Comment on 6 Feb:** I've had several questions about this second task. My intention is that you determine the 30th convergent of π (a rational number) explicitly – see, for example, the fourth task in the assignment for Jan. 29 – and then feed it to *cfas*. Unlike the first task that only asks for a listing of (working) code, your work on this task should be written up as a math problem solution with an explanation of what you did.

Thu., Feb. 5:

Tasks:

- Become familiar with the W3C reference document on HTML 4.01[52], which is classic HTML.

- If you have not already done so, open a web site under your University at Albany user account (the top page may be visibly blank or otherwise publicly useless if you wish).

- Place a translation, whether automatically-generated or "manually written" of the SGML document `tinc.sgml`[53] in your web site at the (relative) URL `mat587s09/tinc.html`.

---

[46]URI: ../refs.html#veryshort

[47]URI: ../refs.html#beginlatex

[48]URI: ../refs.html#notsoshort

[49]URI: http://en.wikipedia.org/wiki/Diffie_Hellman

[50]URI: http://en.wikipedia.org/wiki/ElGamal_encryption

[51]The (rational) value of the initial segment of length 30 in the (infinite) continued fraction expansion of π.

[52]URI: http://www.w3.org/TR/html4/

[53]URI: http://math.albany.edu/pers/hammond/course/uslxh/ctg/tinc-sgml.txt

Make sure that it is a valid HTML document.

Note 1: The document on using the math network[54] (also available as PDF[55] or DVI[56]) in this course have been revised.

Note 2: Because the understanding of markup languages is a topic in this course it is not appropriate at this stage to use a program other than a plain text editor for this task. Moreover, one also should not attempt to use a "word processor" since sometimes, even when creating "plain text", such programs do not generate plain text correctly.

Tue., Feb. 3:

   Reading:

   - Read through the slides on computing basics[57] (also available as PDF[58]).
   - Read through the slides on HTML, SGML, and XML[59] (also available as PDF[60]).
   - Read this document on SGML and XML[61] (also available as PDF[62] or DVI[63]).

   Exercises:

   1. Of documents that can be found on the web claiming to be W3C HTML 4.01, find 3 examples that are valid and also find 3 examples that are not valid. For this task retrieve the underlying HTML files, and use the command "validhtml" found in the unix network.

      A version of "validhtml" suitable for this task can be downloaded to your computer from

      `http://math.albany.edu/~hammond/gellmu/gvalidhtml-0.9.tgz`

      (It will require you to have *OpenSP*, which can be found at the web site of *OpenJade*[64]; you do not need to download OpenJade. Note also that OpenSP is packaged for various systems that have software distributed in packages.)

   2. (*Challenging* at this point) Write a program in whatever language for translating the SGML document type represented by `art.dtd`[65] to HTML 4.01 document type and then use that program to translate the document `tinc.sgml`[66] to an HTML 4.01 document.

Thu., Jan. 29:

   Tasks:

   1. Review my course notes for Math 326 on Continued Fractions[67]. The main points for our purpose here are these:

      (a) Every rational number has a finite continued fraction expansion that may be represented by a finite sequence $[a_1, a_2, \ldots, a_n]$ of integers with $a_i > 0$ for $i > 1$.

      (b) The rational number represented by a given finite sequence is determined by a backward recursion where $a = [a]$ and

      $$[a_m, \ldots, a_n] = a_m + \frac{1}{[a_{m+1}, \ldots, a_n]} \quad \text{when} \quad n > m \quad .$$

---

[54]URI: ../mathnet.html
[55]URI: ../mathnet.pdf
[56]URI: ../mathnet.dvi
[57]URI: mcm090122x.xhtml
[58]URI: mcm090122.pdf
[59]URI: mcm090129x.xhtml
[60]URI: mcm090129.pdf
[61]URI: http://math.albany.edu/pers/hammond/course/uslxh/general.html
[62]URI: http://math.albany.edu/pers/hammond/course/uslxh/general.pdf
[63]URI: http://math.albany.edu/pers/hammond/course/uslxh/general.dvi
[64]URI: http://openjade.sourceforge.net
[65]URI: http://math.albany.edu/pers/hammond/course/uslxh/ctg/art-dtd.txt
[66]URI: http://math.albany.edu/pers/hammond/course/uslxh/ctg/tinc-sgml.txt
[67]URI: ../../cfrac/cfrac.html

2. Become familiar with the computer algebra system Pari/GP[68]. (*Pari* is the name of a library; the user application is *GP*.) Either acquire a personal copy or learn how to use it on the campus math network[69] (also available as PDF[70] or DVI[71]) (where it may be found as `/math/local/solaris/bin/gp-2.3`. Read the first 5 sections of the *Tutorial*, and read § 2.6.1 of the *User's Guide*.

3. Write your own gp function for the Syracuse function.

4. Write your own gp function that when given a finite vector of integers, representing the continued fraction expansion of a rational number, computes the rational number it represents.

Tue., Jan. 27:

> **Tasks:**
>
> 1. Read the Wikipedia page on *Maple*[72], and in a *Maple* session work through the code examples found there. Note that *Maple* is available at many public computing stations on campus and also through remote login to `itsunix.albany.edu`.
>
> 2. 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.
>
> The Syracuse function may be defined in *Maple* with a "one line" procedure definition as follows:
>
> ```
> syr := n -> piecewise(n <= 1, 1, modp(n, 2) = 0, 1/2 n, 3 n + 1);
> ```
>
> Use Maple to find the 5 smallest values of n for which the first $2n+1$ iterations of s applied to n fail to yield 1.

Thu., Jan. 22:

> **First meeting:** No assignment.

UP | TOP | Department

---

[68]URI: http://pari.math.u-bordeaux.fr/
[69]URI: ../mathnet.html
[70]URI: ../mathnet.pdf
[71]URI: ../mathnet.dvi
[72]URI: http://en.wikipedia.org/wiki/Maple_(software)