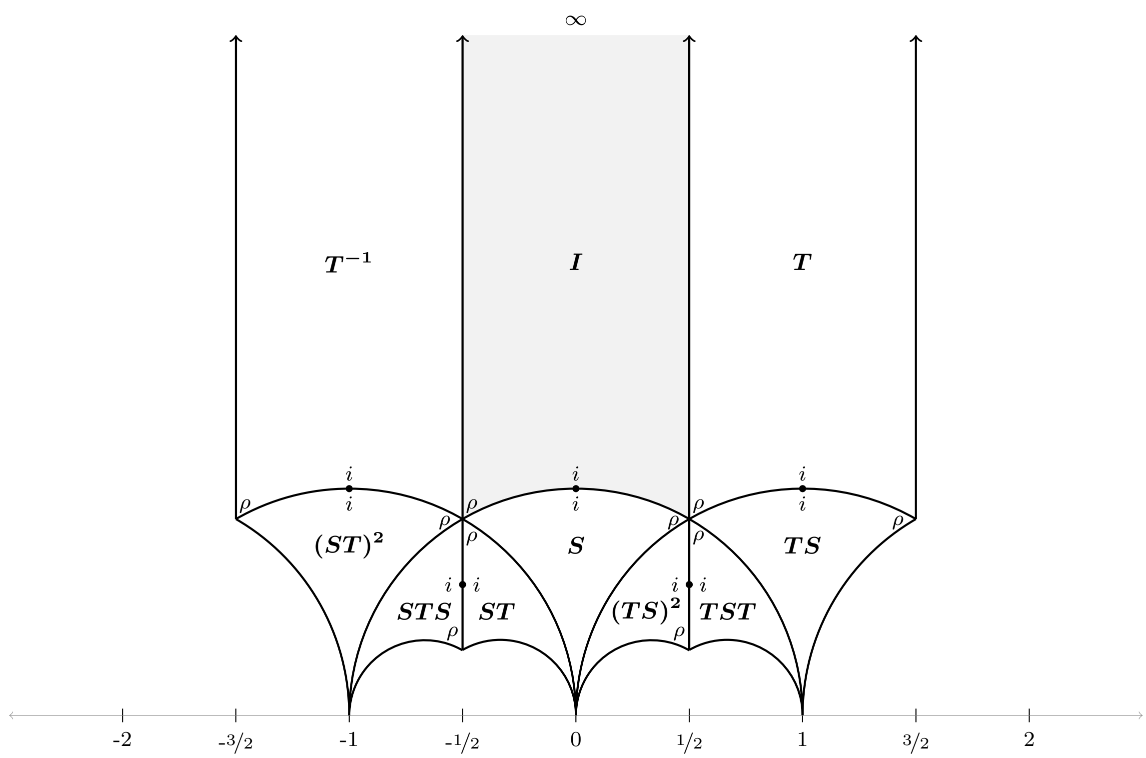
## Description

These problems are related to the material covered in Lectures 18-21. As usual, the first person to spot each non-trivial typo/error will receive a point of extra credit.

**Instructions**: Solve Problems 1-3 and then complete Problem 4, which is a survey.

## Problem 1. Congruence subgroups (30 points)

The diagram below depicts 9 translates of the fundamental region $\mathcal{F}$ for $\mathbb{H}^*/\Gamma(1)$ in $\mathbb{H}^*$. Each translate $\gamma F$ is labelled in bold by $\gamma$, where $\gamma$ is expressed in terms of $S = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ and $T = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ The labels $\rho$ and $i$ within the region labeled by $\gamma$ indicate the points $\gamma\rho$ and $\gamma i$, respectively.




**1.** Determine the index of $\Gamma(2)$ in $\Gamma(1)$, determine the number of $\Gamma(2)$ cusp orbits. Then specify a connected fundamental region for $\mathbb{H}^*/\Gamma(2)$ by listing a subset of the translates of $\mathcal{F}$ in the diagram above and identify the cusps that lie in your region. Compute the genus of $X(2)$ by triangulating your fundamental region and applying Euler's formula $V - E + F = 2 - 2g$. Be careful to count vertices and edges correctly — initially specify vertices and edges as $\mathbb{H}^*$-points in the diagram (e.g. $ST\rho$), then determine which vertices and edges are $\Gamma(2)$-equivalent (note that in the quotient $X(2) = \mathbb{H}^*/\Gamma(2)$ there may be more than one edge between the same pair of vertices).

**2.** For each of the following congruence subgroups, determine its index in $\Gamma(1)$, the number of cusp orbits, and a set of representative cusps: $\Gamma_0(2)$, $\Gamma_0(3)$, $\Gamma_1(3)$, $\Gamma(3)$.

**3.** Derive formulas for the index in $\Gamma(1)$ and the number of cusps for the congruence subgroups $\Gamma_0(p)$, $\Gamma_1(p)$, $\Gamma(p)$, where $p$ is any odd prime.

## Problem 2. Polycyclic presentations (35 points)

Let $\vec{\alpha} = (\alpha_1, \ldots, \alpha_k)$ be a sequence of generators for a finite abelian group $G$, and let $G_i = \langle \alpha_1, \ldots, \alpha_i \rangle$ be the subgroup generated by $\alpha_1, \ldots, \alpha_i$. The series

$$1 = G_0 \vartriangleleft G_1 \vartriangleleft \cdots \vartriangleleft G_{k-1} \vartriangleleft G_k = G,$$

is a *polycyclic series*: each $G_{i-1}$ is a normal subgroup of $G_i$ and each of the quotients $G_i/G_{i-1} = \langle \alpha_i G_{i-1} \rangle$ is a cyclic group. Every finite solvable group admits a polycyclic series, but we restrict ourselves here to abelian groups (written multiplicatively).

When $G$ is the internal direct product of the cyclic groups $\langle \alpha_i \rangle$, we have $G_i/G_{i-1} \cong \langle \alpha_i \rangle$ and call $\vec{\alpha}$ a *basis* for $G$, but this is a special case. For abelian groups, $G_i/G_{i-1}$ is isomorphic to a subgroup of $\langle \alpha_i \rangle$, but it may be a proper subgroup, even when $G$ is cyclic.

The sequence $r(\vec{\alpha}) = (r_1, \ldots, r_k)$ of *relative orders* for $\vec{\alpha}$ is defined by

$$r_i = |G_i : G_{i-1}|,$$

and satisfies $r_i = \min\{r : \alpha_i^r \in G_{i-1}\}$. We necessarily have $r_i \le |\alpha_i|$, but equality typically does not hold ($\vec{\alpha}$ is a basis precisely when $r_i = |\alpha_i|$ for all $i$). In any case, we always have $\prod_i r_i = |G|$, thus computing the $r_i$ determines the order of $G$.

**1.** Let $\vec{\alpha} = (\alpha_1, \ldots, \alpha_k)$ be a sequence of generators for a finite abelian group $G$, with relative orders $r(\vec{\alpha}) = (r_1, \ldots, r_k)$. Prove that every $\beta \in G$ can be uniquely represented in the form

$$\beta = \vec{x} \cdot \vec{\alpha} = \alpha_1^{x_1} \cdots \alpha_k^{x_k},$$

where the integers $x_i$ satisfy $0 \le x_i < r_i$. Show that if $\beta = \alpha_i^{r_i}$, then $x_j = 0$ for $j \ge i$.

By analogy with the case $r = 1$, we call $\vec{x}$ the *discrete logarithm* of $\beta$ with respect to $\vec{\alpha}$ (but note that the discrete logarithm of the identity element is now the zero vector). The vector $\vec{x}$ can be conveniently encoded as an integer $x$ in the interval $[0, |G| - 1]$ via

$$x = \sum_{1 \le i \le k} x_i N_i, \qquad N_i = \prod_{1 \le j < i} r_j,$$

and we may simply write $x = \log_{\vec{\alpha}} \beta$ to indicate that $x$ is the integer encoding the vector $\vec{x} = \log_{\vec{\alpha}} \beta$. Note that $x_i = \lfloor x/N_i \rfloor \bmod r_i$, so it is easy to recover $\vec{x}$ from its encoding $x$.

**2.** Design a generic group algorithm that, given a sequence of generators $\vec{\alpha} = (\alpha_1, \ldots, \alpha_k)$ for a finite abelian group $G$, constructs a table $T$ with entries $T[0], ..., T[|G| - 1]$ with the property that if $T[n] = \beta$, then $n = \log_\alpha \beta$. Your algorithm should also output the relative orders $r_i$, and the integers $s_i$ for which $T[s_i] = \alpha_i^{r_i}$.

This allows us to compute a *polycyclic presentation* for $G$, which consists of the sequence $\vec{\alpha}$, the relative orders $r(\vec{\alpha}) = (r_!, \ldots, r_k)$, and the vector of integers $s(\vec{\alpha}) = (s_1, \ldots, s_k)$. With this presentation in hand, we can effectively simulate any computation in $G$ without actually performing any group operations (i.e. calls to the black box). This can be very useful when the group operation is expensive.

3. Let $\alpha$, $r(\alpha)$, and $s(\alpha)$ be a polycyclic presentation for a finite abelian group $G$. Given integers $x = \log_{\vec{\alpha}} \beta$ and $y = \log_{\vec{\alpha}} \gamma$, explain how to compute the integer $z = \log_{\vec{\alpha}} \beta\gamma$ using $r(\alpha)$ and $s(\alpha)$, without performing any group operations. Also explain how to compute the integer $w = \log_{\vec{\alpha}} \beta^{-1}$.

As a side benefit, the algorithm you designed in part 2 gives a more efficient way to enumerate the class group $\text{cl}(D)$ than we used in Problem Set 9, since the class number $h(D)$ is asymptotically on the order of $\sqrt{|D|}$ (this is a theorem of Siegel).

But first we need to figure out how to construct a set of generators for $G$. We will do this using *prime forms*. These are forms $f = (a, b, c)$ for which $a$ is prime and $-a < b \le a$ (but we do not require $a \le c$, so prime forms need not be reduced). Prime forms correspond to prime ideals whose norm is prime (degree-1 primes). Recall that imaginary quadratic orders $\mathcal{O}$ are determined by their discriminant $D$, which can always be written in the form $D = u^2 D_K$, where $D_K$ is the discriminant of the maximal order $\mathcal{O}_K$ and $u = [\mathcal{O}_K : \mathcal{O}]$ is the conductor of $\mathcal{O}$.

4. Let $a$ be a prime. Prove that if $a$ divides the conductor then there are no prime forms of norm $a$, and that otherwise there are exactly $1 + (\frac{D}{a})$ prime forms of norm $a$, where $(\frac{D}{a})$ is the Kronecker symbol.[1] Write a program that either outputs a prime form $(a, b, c)$ with $b \ge 0$ or determines that none exists.

When $D$ is fundamental, we can generate $\text{cl}(D)$ using prime forms of norm at most $\sqrt{|D|/3}$; this follows from the bound proved in Problem Set 9 and the fact that the maximal order $\mathcal{O}_K$ is a Dedekind domain (so ideals can be uniquely factored into prime ideals). We can still generate $\text{cl}(D)$ with prime forms when $D$ is non-fundamental, but bounding the primes involved is slightly more complicated, so we will restrict ourselves to fundamental discriminants for now.

5. Implement the algorithm you designed in part 2, using the program from part 4 to enumerate the prime forms of norm $a \le \sqrt{|D|/3}$ in increasing order by $a$. Use the prime forms as generators, but use a table lookup to discard prime forms that are already present in your table so that your $\alpha_i$ all have relative orders $r_i > 1$ (**warning**: prime forms need not be reduced: be sure to reduce them before making any comparisons). For the group operation, you can create binary quadratic forms in Sage using `BinaryQF([a,b,c])`, and then compose forms $f$ and $g$ using `h=f*g`. Use `h.reduced_form()` to get the reduced form. You will only be using this code on small examples, so don't worry about efficiency; you will only be graded on your answers to part 6 (which you can probably solve mostly by hand, with a little help from Sage).

6. Run your algorithm on $D = -5291$, and then run it on the first fundamental discriminant $D < -N$, where $N$ is the first five digits of your student ID. Don't list all the elements of $\text{cl}(D)$, just give the reduced forms for the elements of $\vec{\alpha}$ and the integer vectors $r(\vec{\alpha})$ and $s(\vec{\alpha})$. Sanity check your results by verifying that you at least get the right class number for $D$ (you can check this in Sage using `NumberField(x**2-D,'t').class_number()`).

[1] Thus $(\frac{D}{2})$ is 0 if $D$ is even, 1 if $D \equiv 1 \bmod 8$, and $-1$ otherwise. Note that we refer to $a$ as the "norm" of the form $(a, b, c)$, since the corresponding ideal has norm $a$.

## Problem 3. Mapping the CM torsor (35 points)

Let $\mathcal{O}$ be an imaginary quadratic order of discriminant $D$, and let $p > 3$ be a prime that splits completely in the ring class field of $\mathcal{O}$, equivalently, a prime of the form $4p = t^2 - v^2 D$. As explained in lecture, the set

$$\mathrm{Ell}_{\mathcal{O}}(\mathbb{F}_p) = \{j(E/\mathbb{F}_p) : \mathrm{End}(E) \simeq \mathcal{O}\}$$

is a $\mathrm{cl}(\mathcal{O})$-torsor. This means that for any pair $j_1, j_2 \in \mathrm{Ell}_{\mathcal{O}}(\mathbb{F}_p)$, there is a unique $\alpha \in \mathrm{cl}(\mathcal{O})$ for which $\alpha j_1 = j_2$. This has many implications, two of which we explore in this problem.

First and foremost, the $\mathrm{cl}(\mathcal{O})$-action can be used to enumerate the set $\mathrm{Ell}_{\mathcal{O}}(\mathbb{F}_p)$, all we need is a starting point $j_0 \in \mathrm{Ell}_{\mathcal{O}}(\mathbb{F}_p)$. In this problem we will "cheat" and use the Hilbert class polynomial $H_D(X)$ to do this (in Problem Set 11 we will find a starting point ourselves). The polynomial $H_D(X)$ splits completely in $\mathbb{F}_p[X]$, and its roots are precisely the elements of $\mathrm{Ell}_{\mathcal{O}}(\mathbb{F}_p)$. We could enumerate $\mathrm{Ell}_{\mathcal{O}}(\mathbb{F}_p)$ by factoring $H_D(X)$ completely, but that would not let us "map the torsor". We want to construct an explicit bijection from $\mathrm{cl}(\mathcal{O})$ to $\mathrm{Ell}_{\mathcal{O}}(\mathbb{F}_p)$ that is compatible with the group action.

Let us start with a simple example, using $D = -1091$. In this case the class number $h(D) = 17$ is prime, so $\mathrm{cl}(D)$ is cyclic and every non-trivial element is a generator. For our generator, let $\alpha$ be the class of the prime form $(3, 1, 91)$, which acts on $\mathrm{Ell}_{\mathcal{O}}(\mathbb{F}_p)$ via cyclic isogenies of degree 3: each $j \in \mathrm{Ell}_{\mathcal{O}}(\mathbb{F}_p)$ is 3-isogenous[2] to the $j$-invariant $\alpha j$. This means that $\Phi_3(j, \alpha j) = 0$ for all $j \in \mathrm{Ell}_{\mathcal{O}}(\mathbb{F}_p)$, where $\Phi_3(X, Y) = 0$ is the modular equation for $X_0(3)$.

To enumerate $\mathrm{Ell}_{\mathcal{O}}(\mathbb{F}_p)$ as $j_0, j_1, j_2, \ldots$, with $j_k = \alpha^k j_0$, we start by identifying $j_1$ is a root of the univariate polynomial $\Phi_3(j_0, Y)$. Now $\left(\frac{D}{3}\right) = 1$ in this case, so by part 4 of problem 2 there are two ideals of norm 3 in $\mathrm{cl}(D)$, both of which act via 3-isogenies; the other one corresponds to the form $(3, -1, 91)$, the inverse of $\alpha$ in $\mathrm{cl}(\mathcal{O})$. Thus there are at least two roots of $\Phi_3(j_0, Y)$ in $\mathbb{F}_p$, but provided that we pick the prime $p$ so that 3 does not divide $v$, there will be only two $\mathbb{F}_p$-rational roots.

There are methods to determine which of of these two roots "really" corresponds to the action of $\alpha$, but for now we disregard the distinction between $\alpha$ and $\alpha^{-1}$; this ultimately depends on how we embed $\mathbb{Q}(\sqrt{-1091})$ into $\mathbb{C}$ in any case. Let us arbitrarily designate one of the $\mathbb{F}_p$-rational roots of $\Phi_3(j_0, Y)$ as $j_1$. To determine $j_2$, we now consider the $\mathbb{F}_p$-rational roots of $\Phi_3(j_1, Y)$. Again there are exactly two, but we already know one of them: $j_0$ must be a root, since $\Phi_3(X, Y) = \Phi_3(Y, X)$. So we can unambiguously identify $j_2$ as the *other* $\mathbb{F}_p$-rational root of $\Phi_3(j_1, Y)$, equivalently, the unique $\mathbb{F}_p$-rational root of $\Phi_3(j_1, Y)/(Y - j_0)$.

**1.** Let $D = -1091$, and let $t$ be the least odd integer greater than $1000N$ for which $p = (t^2 - D)/4$ is prime, where $N$ is the last three digits of you student ID. Use the Sage function `hilbert_class_polynomial` to compute $H_D(X)$, then pick a root $j_0$ of $H_D(X)$ in $\mathbb{F}_p$ (you will need to coerce $H_D$ into the polynomial ring $\mathbb{F}_p[X]$ to do this). Using the function `isogeny_nbrs` implemented in the Sage worksheet 18.783 Problem Set 10 Problem 3.sws, enumerate the set $\mathrm{Ell}_{\mathcal{O}}(\mathbb{F}_p)$ as $j_0, j_1, j_2, \ldots$ by walking a cycle of 3-isogenies starting from $j_0$, as described above, so that $j_k = \alpha^k j_0$ (assuming that your arbitrary choice of $j_1$ was in fact $j_1 = \alpha j_0$). You should find that the length of this cycle is 17, because $\alpha$ has order 17 in $\mathrm{cl}(D)$. Finally, verify that the you have in fact enumerated all the roots of $H_D(X)$.

[2] When we say that $j_1$ and $j_2$ are 3-isogenous, we are referring to isomorphism classes of elliptic curves over $\overline{\mathbb{F}}_p$. There are 3-isogenous curves $E_1/\mathbb{F}_p$ and $E_2/\mathbb{F}_p$ with $j_1 = j(E_1)$ and $j_2(E_2)$, but one must be careful to choose the correct twists.

**2.** Let $D$, $p$, and $j_0$ be as in part 1, and let $\beta \in \mathrm{cl}(D)$ be the class of the prime form $(7, 1, 39)$. Compute $k = \log_\alpha \beta$. Enumerate $\mathrm{Ell}_\mathcal{O}(\mathbb{F}_p)$ again as $j'_0, j'_1, j'_2, \ldots$, starting from the same $j'_0 = j_0$ but this time use the action of $\beta$, by walking a cycle of 7-isogenies. Rather than choosing $j'_1$ arbitrarily, choose $j'_1$ in a way that is consistent with the assumption $j_1 = \alpha j_0$ in part 1: i.e., choose $j'_1$ so that $j'_1 = \beta j_0 = \alpha^k j_0 = j_k$. Then verify that for all $m = 1, 2, 3, \ldots, 16$ we have $j'_m = \beta^m j_0 = \alpha^{km} j_0 = j_{km}$, where the subscript $km$ is reduced modulo $|\alpha| = 17$.

You should find the results of parts 1 and 2 remarkable (astonishing even). *A priori*, there is no reason to think that there should be a relationship between a cycle of 3-isogenies and a cycle of 7-isogenies. The fact that we can use the modular polynomials $\Phi_\ell$ to enumerate the roots of $H_D$ is extremely useful. One can enumerate the roots of polynomial whose degree is, say, 10 million, simply by finding roots of polynomials of very small degree (typically one can use $\Phi_\ell$ with $\ell < 20$). We can also use the CM torsor to find zeros of $\Phi_\ell$, even when $\ell$ is ridiculously large.

**3.** Let $\ell$ be the least prime greater than $10^{100}N$ for which $\left(\frac{D}{\ell}\right) = 1$, where $N$ is the last three digits of your student ID. Determine the $\mathbb{F}_p$-rational roots of $\Phi_\ell(j_0, Y)$.

For reference, the total size of the polynomial $\Phi_\ell \in \mathbb{Z}[X, Y]$ is roughly $6\ell^3 \log \ell$ bits, which is on the order of $10^{1000000}$ bits in the problem you just solved. Even reduced modulo $p$, it would take more than $10^{10000}$ bits to write down the coefficients of this polynomial (for comparison, there are fewer than $10^{100}$ atoms in the universe). This example might seem fanciful, but an isogeny of degree $10^{100}$ is well within the range that might be of interest in cryptographic applications.

Now for a slightly more complicated example, where the class group is not a cyclic group of prime order. Let $D = -5291$. In this case $h(D) = 36$ and the class group $\mathrm{cl}(D)$ is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/18\mathbb{Z}$. In problem 3 you computed a polycyclic presentation $\vec{\alpha}$, $r(\vec{\alpha})$, $s(\vec{\alpha})$ for $\mathrm{cl}(D)$, which should involve generators $\vec{\alpha} = (\alpha_1, \alpha_2, \alpha_3)$, of norms 3, 5, and 7.

**4.** Let $D = -5291$, and let $t$ be the least odd integer greater than $1000N$ for which $p = (t^2 - D)/4$ is prime, where $N$ is the last three digits of you student ID. Using the polycyclic presentation for $\mathrm{cl}(D)$ that you computed in problem 3, enumerate $\mathrm{Ell}_\mathcal{O}(D)$ starting from a $j$-invariant $j_0$ obtained as a root of $H_D$. Your enumeration $j_0, j_1, j_2, \ldots, j_{35}$ should have the property that the element $\beta \in \mathrm{cl}(\mathcal{O})$ whose action sends $j_0$ to $j_k$ satisfies $k = \log_\alpha \beta$ (in terms of the table $T$ in part 2 of problem 3, $j_k = T[k]j_0$), subject to the assumption that $j_1 = \alpha_1 j_0$.

Here are a few tips on part 4. You will compute $j_0, \ldots, j_{r_1-1}$ using 3-isogenies, but to compute $j_{r_1}$ you will need to compute a 5-isogeny from $j_0$. When choosing $j_{r_1}$ as a root of $\Phi_5(j_0, Y)$, make this choice consistent with the assumption $j_1 = \alpha_1 j_0$ by using the fact that $s_2 = \log_{\vec{\alpha}} \alpha_2^{r_2}$ (assuming $s_2 \neq 0$, which is true in this case). When you go to compute $j_{r_1+1}$, you will need to choose a root of $\Phi_3(j_{r_1}, Y)$. Here you can make the choice consistent with the fact that $\mathrm{cl}(\mathcal{O})$ is abelian, so the action of $\alpha_1\alpha_2$ should be the same as the action of $\alpha_2\alpha_1$. Similar comments apply throughout; any time you start a new isogeny cycle, you have a choice to make, but you can make all of them consistent with your choice of $j_1$.

I don't recommend trying to write a program to make all these choices (this can be done but it is a bit involved), it will be easier and more instructive to work it out by hand, using Sage to enumerate paths of $\ell$-isogenies as required (you can use the function `isogeny_path` in the Sage worksheet 18.783 Problem Set 10 Problem 3.sws.

## Problem 4. Survey

Complete the following survey by rating each of the problems you attempted on a scale of 1 to 10 according to how interesting you found the problem (1 = “mind-numbing,” 10 = “mind-blowing”), and how difficult you found the problem (1 = “trivial,” 10 = “brutal”). Also estimate the amount of time you spent on each problem to the nearest half hour.

| | Interest | Difficulty | Time Spent |
|---|---|---|---|
| Problem 1 | | | |
| Problem 2 | | | |
| Problem 3 | | | |

Also, please rate each of the following lectures that you attended, according to the quality of the material (1=“useless”, 10=“fascinating”), the quality of the presentation (1=“epic fail”, 10=“perfection”), the pace (1=“way too slow”, 10=“way too fast”, 5=“just right”) and the novelty of the material (1=“old hat”, 10=“all new”).

| Date | Lecture Topic | Material | Presentation | Pace | Novelty |
|---|---|---|---|---|---|
| 4/25 | Riemann surfaces and X(1) | | | | |
| 4/30 | The modular equation | | | | |

Please feel free to record any additional comments you have on the problem sets or lectures, in particular, ways in which they might be improved.

18.783 Elliptic Curves
Spring 2013