EXERCISES IN MODULAR FORMS I (MATH 726)

EYAL GOREN, MCGILL UNIVERSITY, FALL 2007

(1) We define a (full) lattice L in $\mathbb{R}^n$ to be a discrete subgroup of $\mathbb{R}^n$ that contains a basis for $\mathbb{R}^n$. Prove that L is a lattice if and only if L is free of rank n as an abelian group and contains a basis of $\mathbb{R}^n$.

(2) Prove that a lattice L is integral if and only if its Gram matrix has integer coefficients.

(3) Prove that the densest lattice packing in $\mathbb{R}^2$ is the hexagonal packing obtained from the lattice $L = \mathbb{Z}[\omega]$, where $\omega = \frac{1+\sqrt{-3}}{2}$ and one uses the usual identification of $\mathbb{R}^2$ with $\mathbb{C}$. Prove that $\Delta(L) = \frac{\pi}{2\sqrt{3}} = 0.9068\ldots$, $\tau(L) = 6$ and $\rho(L) = 1/2$.

(4) Find the laminated lattice Λ_3.

(5) Prove that the Hamming code H_7 is a $[7, 4, 3]$ code and calculate its weight enumerator polynomial. Conclude that the extended Hamming code $H_8 = H_7^e$ is an $[8, 4, 4]$ code with weight enumerator $x^8 + 14x^4y^4 + y^8$.

(6) Discuss self-dual cyclic codes.

(7) For the lattices $\Lambda(C)$ in $\mathbb{R}^n$, obtained from the codes Z, U, P, R, C_{24} (the zero code, the universal code, the parity code, the repetition code and the extended Golay code) calculate the kissing number, packing radius, determinant and theta function. In the case of the theta function, I mean to write it in terms of θ_2, θ_3 but also as $A + Bq^a + Cq^b + h.o.t.$ and to find A, B in each case (here a, b are the first powers that appear, which may be fractional if the lattice is not even integral). Find also C, if you can!

(8) Let Φ be a root system and $r \in \mathbb{R}$ such that there is some root in Φ of length r. Show that $\{\alpha \in \Phi : \|\alpha\| = r\}$ is a root system.

(9) Suppose that Φ is a reducible root system, that is $\Phi = \Phi_1 \cup \Phi_2$, where each $\Phi_i \neq \emptyset$ and Φ_1 is perpendicular to Φ_2. Prove that each Φ_i is a root system.

Conversely, let Φ_i be a root system in the Euclidean space E_i. Prove that $\Phi = \Phi_1 \cup \Phi_2$ in $E_1 \oplus E_2$ is a root system.

(10) Let $M \in \mathrm{GL}_n(\mathbb{Z})$ be a matrix such that both M and M^{-1} have non-negative entries. Prove that M is a permutation matrix (for some $\sigma \in S_n$ we have $Me_i = e_{\sigma(i)}, i = 1, 2 \ldots, n$).

(11) Let Φ be a root system. For $\alpha, \beta \in \Phi$ prove that $\sigma_\alpha \circ \sigma_\beta$ is a rotation by angle 2θ, where θ is the angle between α and β and conclude that $\sigma_\alpha \sigma_\beta$ is of order $2, 3, 4$ or 6, if θ if $\langle \alpha, \beta \rangle \langle \beta, \alpha \rangle$ is $0, 1, 2$ or 3 respectively.

(12) Let A be an admissible set in an Euclidean space E (as in the proof of the classification of Dynkin diagrams). Assume that there is an edge e in Γ_A with end points p, q such that by removing the edge e from Γ (but keeping the vertices p, q) we get a disconnected diagram $\Gamma' = \Gamma_p \coprod \Gamma_q$ with $p \in \Gamma_p, q \in \Gamma_q$. Let Γ'' be the diagram obtained by gluing the diagrams Γ_p and Γ_q by identifying p and q (but identifying no edges or other vertices). Prove that Γ'' is the diagram of some admissible set A'' in some Euclidean space E''.

(13) Let C be the Cartan matrix of a Dynkin diagram of type $A_n (n \geq 1), D_n (n \geq 4)$, E_6, E_7 or E_8. Prove that C is a symmetric positive definite matrix and that there is a matrix M such that ${}^tMM = C$. Conclude that C is the Gram matrix of some lattice C. (Of course, we know that already, because we constructed those C from root systems. The point is that one doesn't really need the root systems once one knows the matrices in order to construct lattices with those matrices as Gram matrices.) Calculate $\det(L)$ directly as $\det(C)$.

The root systems A_n and D_n have nice models.

• **The root system D_n.** Consider the lattice

$$\{(x_1, \ldots, x_n) : x_i \in \mathbb{Z}, \sum x_i \equiv 0 \pmod 2\}.$$

Show that

$$M = \begin{pmatrix} -1 & 0 & \dots & \dots & 0 & 0 \\ 1 & -1 & & & \vdots & \vdots \\ 0 & 1 & & & & \\ \vdots & 0 & & & & \\ & \vdots & & & 0 & 0 \\ & & & & -1 & -1 \\ 0 & 0 & \dots & \dots & 1 & -1 \end{pmatrix}$$

is a generator matrix for the lattice and that the Gram matrix is the one of the root system D_n.

- **The root system A_n.** Consider the lattice

$$\{(x_0, x_1, \dots, x_n) : x_i \in \mathbb{Z}, \sum x_i = 0\}.$$

It is a lattice in the Euclidean space $\{(x_0, x_1, \dots, x_n) : x_i \in \mathbb{R}, \sum x_i = 0\}$ (with inner product obtained by restriction from $\mathbb{R}^{n+1}$). Show that

$$M = \begin{pmatrix} -1 & 0 & \dots & \dots & 0 \\ 1 & -1 & & & \vdots \\ 0 & 1 & & & \\ \vdots & 0 & & & \\ & \vdots & & & 0 \\ & & & & -1 \\ 0 & 0 & \dots & \dots & 1 \end{pmatrix}$$

is a generator matrix for the lattice and that the Gram matrix is the one of the root system A_n.

- Conclude the following table

	det	ρ	τ	δ
A_n	$n+1$	$\frac{1}{\sqrt{2}}$	$n(n+1)$	$2^{-n/2}(n+1)^{-1/2}$
D_n	4	$\frac{1}{\sqrt{2}}$	$2n(n-1)$	$2^{-(n+2)/2}$

(14) Let f be a $C^\infty_{\mathbb{C}}([0,1]^n)$ be a periodic function. I.e, a complex valued function whose mixed partial derivatives of all orders exist and $f(x_1, \dots, \underset{i}{0}, \dots, x_n) = f(x_1, \dots, \underset{i}{1}, \dots, x_n)$ for every i. Prove that f is equal to its Fourier series.

(15) Let $T = \mathrm{SO}_2(\mathbb{R})$ be the unit circle group.

(a) Prove that every continuous homomorphism $\mathbb{R} \to T$ is of the form $x \mapsto e^{2\pi i a x}$ for some fixed $a \in \mathbb{R}$.
(b) Prove that every continuous homomorphism $T \to T$ is of the form $x \mapsto x^n$ for some fixed integer n.

(16) Let Γ be a discrete subgroup of $\mathrm{SL}_2(\mathbb{R})$. Prove that for every $x, y \in \mathfrak{H}$ there exist open sets $x \in U_x, y \in U_y$ such that for every $\gamma \in \Gamma$, if $\gamma(U_x) \cap U_y \neq 0$ then $\gamma x = y$.

(17) An example of a discrete infinite non-abelian subgroup of $\mathrm{SL}_2(\mathbb{R})$ with no cusps.
(a) Prove that the rational quadratic form

$$x^2 + y^2 - 3z^2 - 3w^2$$

does not represent zero. You may use that an integer m is a sum of squares if and only if every prime $p \equiv 3 \pmod 4$ divides n to an even power.
(b) Consider the $\mathbb{Q}$-vector space,

$$B = \mathbb{Q} \oplus \mathbb{Q}i \oplus \mathbb{Q}j \oplus \mathbb{Q}k,$$

with multiplication determined by,

$$i^2 = -1,\ j^2 = 3,\ k^2 = 3,\ ij = k = -ji,$$

and with $\mathbb{Q}$ being in the center. Prove that it can be realized as a subalgebra of $M_2(\mathbb{Q}[\sqrt{3}])$ as follows:

$$a + bj + ci + dk \mapsto \begin{pmatrix} a + b\sqrt{3} & -(c - d\sqrt{3}) \\ c + d\sqrt{3} & a - b\sqrt{3} \end{pmatrix}.$$

Note that this matrix has determinant $a^2 + c^2 - 3b^2 - 3d^2$. We call this determinant the *norm* of $a + bj + ci + dk$.
(c) Prove that B is a division algebra. Prove that $B^* \subset \mathrm{GL}_2(\mathbb{Q}[\sqrt{3}]) \subset \mathrm{GL}_2(\mathbb{R})$ does not contain a parabolic element.
(d) Let $\mathcal{O} = \{a + bj + ci + dk : a, b, c, d \in \mathbb{Z}\}$. Prove that $\mathcal{O}$ is a ring and that the elements of norm 1 in it are a non-commutative infinite discrete subgroup of $\mathrm{SL}_2(\mathbb{R})$.

Remarks: B is an example of a quaternion algebra which is split at infinity. A quaternion algebra over $\mathbb{Q}$ is a $\mathbb{Q}$-algebra of dimension 4 over $\mathbb{Q}$, which is central simple (that is, its center is $\mathbb{Q}$ and it does not split as a direct sum of algebras). Any quaternion algebra over $\mathbb{Q}$ which is not isomorphic to $M_2(\mathbb{Q})$ is in fact a division algebra. (This follows from the Artin-Wedderburn theorem.) A division algebra B is called split at infinity if $B \otimes_{\mathbb{Q}} \mathbb{R}$ is isomorphic to $M_2(\mathbb{R})$. A division algebra B has

a natural norm map to $\mathbb{Q}$, which, if B is split and we embed $B \to B\otimes_{\mathbb{Q}}\mathbb{R} \cong M_2(\mathbb{R})$, is just the determinant.

An order in a quaternion algebra over $\mathbb{Q}$ is a subring which is free of rank 4 as an abelian group. The ring $\mathcal{O}$ above is an example. It is in fact true that given any quaternion division algebra over $\mathbb{Q}$, split at infinity, and any order R in it, the elements of norm 1 in R, R_1, form a discrete infinite subgroup of $\mathrm{SL}_2(\mathbb{R})$ that has no cusps and, moreover, $R_1\backslash\mathcal{H}$ is a compact Riemann surface.

(18) **Horocircles.**

Define the following sets:

$$D_\infty := \{z : \mathrm{Im}(z) \geq 1\} \cup \{\infty\}, \qquad D_\infty^- := \{z : \mathrm{Im}(z) > 1\} \cup \{\infty\}.$$

Also, for every rational number p/q in reduced form:

$$D_{p/q} = \{\tau \in \mathfrak{H} : |\tau - (\frac{p}{q} + i\cdot\frac{1}{2q^2})| \leq \frac{1}{2q^2}\}, \qquad D_{p/q}^- = \{\tau \in \mathfrak{H} : |\tau - (\frac{p}{q} + i\cdot\frac{1}{2q^2})| < \frac{1}{2q^2}\} \cup \{\frac{p}{q}\}.$$

- Prove that if $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ is such that $\gamma\infty = p/q$ then $\gamma D_\infty = D_{p/q}$ and $\gamma D_\infty^- = D_{p/q}^-$. Conclude that $\mathrm{SL}_2(\mathbb{Z})$ acts on the sets $\{D_{p/q}\} \cup \{D_\infty\}$ and $\{D_{p/q}^-\} \cup \{D_\infty^-\}$.
- Prove that if $x \neq y$ are points of $\mathbb{P}^1(\mathbb{Q})$ then $D_x^- \cap D_y^- = \emptyset$ and $D_x \cap D_y$ consists at most of a single point.
- Let $0 \leq x < y \leq 1$ be rational numbers. Prove that $D_x \cap D_y \neq \emptyset$ if and only if x and y are consecutive elements in some Farey series.[1]

(19) Let $\Gamma \subset \mathrm{PSL}_2(\mathbb{Z})$ be a subgroup of finite index and let $d = [\mathrm{PSL}_2(\mathbb{Z}) : \Gamma]$. Let $X(\Gamma) = \Gamma\backslash\mathfrak{H}^*$. Let ϵ_2 be the number of inequivalent elliptic points of Γ of order 2 (resp. 3), that is, the number of points in $\Gamma\backslash\mathfrak{H}$ whose stabilizer in Γ is cyclic of order 2 (resp. 3). Let ϵ_∞ be the number of inequivalent cusps of Γ, i.e., the number of orbits of Γ in $\mathbb{P}^1(\mathbb{Q})$. Prove that the genus of $X(\Gamma)$ is given by

$$1 + \frac{d}{12} - \frac{1}{4}\epsilon_2 - \frac{1}{3}\epsilon_3 - \frac{1}{2}\epsilon_\infty.$$

(20) This exercise deals with the genus formula for the modular curve $X_0(p)$.

(a) Find coset representatives for $\Gamma_0(p)$ in $\mathrm{SL}_2(\mathbb{Z})$ and in particular obtain again that $[\mathrm{PSL}_2(\mathbb{Z}) : \Gamma_0(p)] = p + 1$.

[1]The Farey series of level n consists of the numbers in $\{i/j : 0 \leq i \leq j, 1 \leq j \leq n\}$ with their natural order. For example: the Farey series of level 1 is $0, 1$, of level 2 is $0, 1/2, 1$, of level 3 is $0, 1/3, 1/2, 2/3, 1$, of level 4 is $0, 1/4, 1/3, 1/2, 2/3, 3/4, 1$, of level 5 is $0, 1/5, 1/4, 1/3, 2/5, 1/2, 3/5, 3/4, 4/5, 1$ and so on. It is known, and you can use that, that two fractions $n/k, n'/k'$ (in reduced form and between 0 and 1) are consecutive elements of a Farey series if and only if $|nk' - kn'| = 1$.

(b) Prove that $\Gamma_0(p)$ has two cusps, represented by 0 and ∞.
(c) Calculate the number of elliptic points of order 2 or 3 for $\Gamma_0(p)$. This can be done using the representatives you have found above.
(d) Deduce that the genus of $X_0(p)$ is zero for $p = 2, 3$ and otherwise is given by the formula

$$\frac{p+1}{12} - \frac{1}{4}\left(1 + \left(\tfrac{-1}{p}\right)\right) - \frac{1}{3}\left(1 + \left(\tfrac{-3}{p}\right)\right).$$

(e) Using this, find all p such that $X_0(p)$ has genus 0 or 1.

(21) Let $y^2 = f(x)$, $f(x) = x^{2g+1} + a_{2g}x^{2g} + \cdots + a_0$ be a separable polynomial over $\mathbb{C}$. It defines an affine curve C' in $\mathbb{C}^2$ and the map

$$\pi : C' \to \mathbb{C}, \qquad \pi((x, y)) = x,$$

is a degree 2 holomorphic map. One can prove that C' can be compactified to a Riemann surface C and that the map $\pi : C' \to \mathbb{C}$ extends to a map of Riemann surfaces

$$\pi : C \to \mathbb{P}^1.$$

(One has to go outside $\mathbb{P}^2$ to construct the compactification, which is why I am not giving it explicitly.)
(a) Prove that $C \setminus C'$ consists of a single point that we now denote ∞.
(b) Prove that the map π has $2g + 2$ ramification points and find them.
(c) Prove that C has genus g. It is called a hyperelliptic curve.
(d) Calculate the divisor of the functions x and y on C. Calculate the divisor of the differential dx.
(e) Construct g independent holomorphic differentials on C.
(f) Given any two ramification points P, Q show that there exists a function on C whose divisor is $2[P] - 2[Q]$.

(22) Let $\Gamma \subseteq SL_2(\mathbb{Z})$ be a subgroup of finite index and let $f_1, \ldots, f_n$ be modular forms of weights $w_1 < w_2 < \cdots < w_n$, respectively. Prove that $\{f_1, f_2, \ldots, f_n\}$ are linearly independent as functions on the upper half plane.

The following exercises deal with the ring of modular forms on $X(2)$.

(23) (a) Prove that any modular form for $X(2)$ of negative or odd weight is identically zero.
(b) Calculate the dimension $m(2k)$ of the modular forms of weight $2k$ for $X(2)$, for every $k \geq 0$, and the dimension $s(2k)$ of cusp forms. Prove, in particular, that $m(2) - s(2) = 2$ and $m(2k) - s(2k) = 3$ for $k > 1$.

(c) Let $\Gamma \subseteq \mathrm{SL}_2(\mathbb{Z})$ be of finite index. Prove that two modular forms on $X(\Gamma)$ of the same weight and the same divisor are a scalar multiple of each other.

(d) Prove that the cusps of $X(2)$ are $\infty, 0, 1$. Prove that Δ (the cusp form of weight 12 on $\mathrm{SL}_2(\mathbb{Z})$), considered as a modular form on $X(2)$, vanishes to second order at every cusp of $X(2)$. Prove that there is a unique cusp form δ of weight 6 (up to a scalar) on $X(2)$. Prove that for an appropriate normalization of δ, $\delta^2 = \Delta$.

(e) Denote two linearly independent modular forms of weight 2 for $X(2)$ by F, G. Show we may choose F, G such that they receive the following values at the cusps: $F(\infty) = 1, F(0) = 0, F(1) = -1$, $G(\infty) = 0, G(0) = 1, G(1) = -1$. Prove that this determines F, G uniquely. (Hint: you may want to use the Residue Theorem for Riemann surfaces.)

(f) The Galois group of the cover $X(2) \to X(1)$ is $\mathrm{SL}_2(\mathbb{Z}/2\mathbb{Z}) \cong S_3$. Calculate the representation

$$\mathrm{SL}_2(\mathbb{Z}/2\mathbb{Z}) \to \mathrm{Aut}(M_2),$$

on the space of modular forms of weight 2 obtained by $f \mapsto f|_2\gamma$.

(24) Let F, G be as in the previous exercise.

(a) Write δ as a polynomial in F and G.

(b) Prove that the map of graded rings,

$$\mathbb{C}[F, G] \to \oplus_{k=0}^{\infty} M_{2k}(\Gamma(2)),$$

is surjective.

(c) Prove that the ring of modular forms on $X(2)$ is a free polynomial ring in F, G.

(25) Prove that the modular forms F, G have no common zeroes. Conclude that the map,

$$z \mapsto (F(z) : G(z)),$$

an isomorphism of $X(2)$ with $\mathbb{P}^1$ and therefore any meromorphic function on $X(2)$ is a rational polynomial in $\mu = F/G$.

(26) Find the expression of E_4 and E_6 in terms of F, G and so the map $\mathbb{C}[E_4, E_6] \hookrightarrow \mathbb{C}[F, G]^{S_3}$. Find the action of group $\mathrm{SL}_2(\mathbb{Z}/2\mathbb{Z})$ on μ. Write j as a polynomial in μ.

(27) In this exercise we construct two theta series that shall provide (after some manipulations) generators of the weight 2 modular forms on $X(2)$.

(a) Recall the ring $\mathbb{H}$ of Hamilton quaternions over $\mathbb{Q}$. It is the vector space $\mathbb{Q} \oplus \mathbb{Q}i \oplus \mathbb{Q}j \oplus \mathbb{Q}k$ with the relations $i^2 = j^2 = -1, ij = -ji = k$. If

$z = a + bi + cj + dk$, put $\bar{z} = a - bi - cj - dk$ (this is an anti-involution on $\mathbb{H}$). Put also $\mathrm{Tr}(z) = z\bar{z} = 2a$ and $\mathrm{Norm}(z) = z\bar{z} = a^2 + b^2 + c^2 + d^2$. There is a $\mathbb{Q}$ rational symmetric bilinear form on $\mathbb{H}$ given by

$$\langle x, y\rangle = \mathrm{Tr}(x\bar{y}).$$

The quadratic form associated to it is $2(a^2 + b^2 + c^2 + d^2)$. Consider this bilinear form on the order $\mathbb{Z} \oplus \mathbb{Z}i \oplus \mathbb{Z}j \oplus \mathbb{Z}k$. Show it is given by the matrix $\mathrm{diag}(2, 2, 2, 2)$. Conclude that the associated theta series Θ' is a modular form on $\Gamma_0(4)$ with trivial character.

(b) Show that there is a matrix $\gamma \in \mathrm{SL}_2(\mathbb{R})$ such that $\gamma^{-1}\Gamma_0(4)\gamma = \Gamma(2)$. Prove that $\Theta_1 := \Theta'|_2\gamma$ is a holomorphic modular form of weight 2 on $\Gamma(2)$.

(c) Consider the maximal order in $\mathbb{H}$ given by $\mathbb{Z} \oplus \mathbb{Z}i \oplus \mathbb{Z}j \oplus \mathbb{Z} \cdot \frac{1+i+j+k}{2}$. Show that the bilinear form is given by

$$\begin{pmatrix} 2 & 0 & 0 & 1 \\ 0 & 2 & 0 & 1 \\ 0 & 0 & 2 & 1 \\ 1 & 1 & 1 & 2 \end{pmatrix}.$$

Show that the associated theta series Θ_2 is a holomorphic modular form on level 2 on $X(2)$.

(d) Calculate the leading coefficient in the q-expansion of Θ_1, Θ_2 at each cusp and, using this, express them in terms of F and G. (Hint: it is enough to check 2 cusps. The involution $z \mapsto -1/z$ permutes 0 and ∞).

(28) We write $\theta_{a,b}(\tau)$ for $\Theta\begin{bmatrix} a/2 \\ b/2 \end{bmatrix}(0, \tau)$, which was defined in the lecture. It is known that $\theta_{0,0}^2, \theta_{0,1}^2$ and $\theta_{1,0}^2$ are modular forms of weight 1 for the modular group $\Gamma(4)$. Assuming this, prove *Jacobi's identity*

$$\theta_{0,0}^4 = \theta_{0,1}^4 + \theta_{1,0}^4.$$

(Hint: one way to do that is by computing q-expansions at $i\infty$. One can, in fact, calculate just finitely many terms (though it is easy enough to compute the q-expansions entirely); why's that? and how many terms are needed exactly?)

Prove that the map

$$\psi : \Gamma(4)\backslash\mathfrak{H} \to \mathbb{P}^2, \qquad \tau \mapsto (\theta_{0,0}^2(\tau), \theta_{0,1}^2(\tau), \theta_{1,0}^2(\tau)),$$

is well-defined and has image in the curve C in $\mathbb{P}^2$ given by $x_0^2 = x_1^2 + x_2^2$. The map extends in fact to an isomorphism

$$\psi^* : \Gamma(4)\backslash\mathfrak{H}^* \cong C.$$

Prove this as follows:

(a) Explain why the map extends to a surjective morphism $\psi^* : \Gamma(4)\backslash\mathfrak{H}^* \to C$; [2]
(b) Find 6 points on C that are not in $\psi(\Gamma(4)\backslash\mathfrak{H})$.
(c) Calculate the number of cusps of $\Gamma(4)\backslash\mathfrak{H}^*$.
(d) Argue that the map ψ^* must be injective and hence an isomorphism.

(29) Let $K \subset \mathbb{C}$ be a quadratic imaginary field. Recall that the class group of K, $Cl(K)$, consists of equivalence classes of fractional ideals. Let $\mathscr{E}(K)$ be the set of isomorphism classes of complex tori $\mathbb{C}/\Lambda$ such that $\mathrm{End}(\mathbb{C}/\Lambda) = \mathcal{O}_K$ (this set can also be identified with the set of isomorphism classes of elliptic curves E over $\mathbb{C}$ together with an embedding $\mathcal{O}_K \to \mathrm{End}(E)$ such that the induced action of $\mathcal{O}_K$ on the tangent space to E at the origin is the action of K on $\mathbb{C}$).

Prove that there is a natural bijection

$$Cl(K) \leftrightarrow \mathscr{E}(K).$$

[2]This is a bit tricky – you can either argue that the map is algebraic which is not immediate, I think, or consider it at the cusps using some explicit calculations. At the cusp $i\infty$ it's easy. For the other cusps note that it's really enough to show convergence of the theta functions – the exact value is not important here. This can be done by "brute force".