Assignment 3

Due date: April 3, 2013

General instructions:

- Submit your solutions by typesetting in LaTeX.
- Write your solutions by furnishing all relevant details (you may assume the results already covered in the class or previous homework problems).
- You are strongly urged to solve the problems by yourself.
- If you discuss with someone else or refer to any material (other than the course notes) then please put a reference in your answer script stating clearly whom or what you have consulted with and how it has benifited you. We would appreciate your honesty.
- If you need any clarification, please ask one of the instructors.

Total: 50 points

In the following problems, $\mathbb{N}$ is the set of natural numbers, $\mathbb{R}$ is the set of real numbers, $\mathbb{Q}$ is the set of rational numbers and $\mathbb{Z}$ is the set of integers.

1. (**4 points**) Let $g_1, \ldots, g_n \in \mathbb{R}^n$ be linearly independent and $\mathcal{L} = \sum_{i=1}^n \mathbb{Z} g_i$ the lattice that they generate. Prove that for each vector $x \in \mathbb{R}^n$ there is a vector $g \in \mathcal{L}$ such that
$$\|x - g\|^2 \leq \frac{1}{4}(\|g_1\|^2 + \ldots + \|g_n\|^2).$$
2. (**5 points**) Give an example of a polynomial $f(x) \in \mathbb{Z}[x]$ that has a root modulo every prime, but still there exists an $n \in \mathbb{N}$ such that f does not have a root modulo n.
3. (**12 points**) A nonsingular matrix $W \in \mathbb{Z}^{n \times n}$, for a positive integer n, is in *Hermite Normal Form* (HNF) [1] if all entries above the diagonal are zero (i.e. W is lower traingular). The following algorithm takes an arbitrary nonsingular matrix $V \in \mathbb{Z}^{n \times n}$ and computes Hermite normal form W of V, such that $W = UV$ for a matrix $U \in \mathbb{Z}^{n \times n}$, which is unimodular (meaning $\det(U) = \pm 1$).

   Algorithm: Hermite Normal Form

   Input: A matrix $V \in \mathbb{Z}^{n \times n}$ with $\det(V) \neq 0$.

   Output: A matrix $W \in \mathbb{Z}^{n \times n}$ in HNF such that $W = UV$ for a unimodular $U \in \mathbb{Z}^{n \times n}$.

[1] Conventionally, HNF is defined by imposing one more condition to ensure uniqueness - we won't need it.

1. $W \leftarrow V$, $m \leftarrow n$.
2. If $m = 1$ then goto step 8.
3. Choose a row index k with $1 \leq k \leq m$ such that $|w_{km}| = \min\{|w_{im}| : 1 \leq i \leq m$ and $w_{im} \neq 0\}$. Exchange rows k and m of W.
4. If $w_{mm}|w_{\ell m}$ for $1 \leq \ell \leq m$ then goto step 7.
5. Choose a column index ℓ with $1 \leq \ell \leq m$ and $w_{mm} \nmid w_{\ell m}$. Compute $q \in \mathbb{Z}$ with $|w_{\ell m} - q w_{mm}| \leq |w_{mm}|/2$ by division with remainder.
6. Subtract q times row m from row ℓ of W. Goto step 3.
7. For $\ell = 1, \ldots m-1$ subtract $w_{\ell m}/w_{mm}$ times row m from row ℓ in W. $m \leftarrow m-1$, goto step 2.
8. Return W.

(a) (**3 points**) Prove that the algorithm works correctly, using the invariant that before each execution of step 2, $W = UV$ for some unimodular matrix U and $w_{ij} = 0$ and $w_{jj} \neq 0$ for $m < j \leq n$ and $1 \leq i < j$. Infer that the minimum in step 3 always exists.

(b) (**3 points**) Show that at most $\log_2 u$ executions of steps 3 through 6 lie between two executions of step 2, where $u = \min\{|w_{im}| : 1 \leq i \leq m$ and $w_{im} \neq 0\}$ at the previous execution of step 2. Conclude that the algorithm terminates.

(c) (**3 points**) Let $a_1, \ldots a_n \in \mathbb{Q}^n$ be linearly independent, $\mathcal{L} = \sum_{1 \leq i \leq n} \mathbb{Z} a_i$ the lattice that they generate, and $b_1, \ldots, b_n \in \mathcal{L}$ be linearly independent as well. Then $\mathcal{M} = \sum_{1 \leq i \leq n} \mathbb{Z} b_i \subseteq \mathcal{L}$ is a sublattice of $\mathcal{L}$. Prove that there exists a basis $c_1, \ldots, c_n$ of $\mathcal{M}$ which has the form.

$$\begin{aligned} c_1 &= w_{11} a_1, \\ c_2 &= w_{21} a_1 + w_{22} a_2, \\ &\vdots \\ c_n &= w_{n1} a_1 + w_{n2} a_2 + \ldots w_{nn} a_n, \end{aligned}$$

with $w_{ij} \in \mathbb{Z}$ and $w_{ii} \neq 0$ for $1 \leq j \leq i \leq n$.

(d) (**3 points**) Suppose that $v_1, \ldots, v_m \in \mathbb{Q}^n$ are not necessarily $\mathbb{Q}$-linearly independent vectors, and $\mathcal{L} = \sum_{1 \leq i \leq m} \mathbb{Z} v_i$. Prove that there exists $\mathbb{Q}$-linearly independent vectors $w_1, \ldots, w_r \in \mathcal{L}$ such that $\mathcal{L} = \sum_{1 \leq j \leq r} \mathbb{Z} w_j$.

4. (**5 points**) Design a deterministic polynomial-time algorithm that given a bivariate polynomial $f(x, y) \in \mathbb{Q}[x, y]$ which is monic with respect to x, determines if it has the property that for all $y \in \mathbb{Q}$, there exists an $x \in \mathbb{Q}$ such that $f(x, y) = 0$.

5. (**4 points**) Let $n = p_1 p_2$, where $p_1, p_2 \in \mathbb{N}$ are distinct odd primes. The n-th cyclotomic polynomial Φ_n is irreducible in $\mathbb{Z}[x]$. Prove that it splits modulo any prime p into at least two factors.

6. (**12 points**) *Background*: Let $f = \sum_{i=0}^{n} a_i x^i$ be a polynomial in $\mathbb{Z}[x]$ and $A = \max_i\{|a_i|\}$. In the class, we have seen how to compute all the integer roots of f in time polynomial in n and $\log(A+1)$. But, suppose that most of the coefficients of f are zero, that is,

barring some k coefficients $a_{i_1}, \ldots, a_{i_k}$ where $k << n$, all the remaining a_i's are zero. It would not be wise then to allow our algorithm to take time polynomial in n which could be potentially much larger than k. The aim of this exercise is to design an algorithm that takes time polynomial in the *actual input size* of the polynomial f.

Definition: Let $f = \sum_{i=0}^{n} a_i x^i$. Suppose, f is given as a list of pairs (a_i, i), where $a_i \neq 0$. The input *size* of f is,

$$\text{size}(f) = \sum_{i: a_i \neq 0} (\log(|a_i| + 1) + \log(i + 1)).$$

We would like to design an algorithm to compute all the integer roots of f in time polynomial in size(f). At the heart of the approach is the following theorem (which we won't prove here). Define *sign* of $f(b)$ for any $b \in \mathbb{Z}$ as follows.

$$f(b) = \begin{cases} -1 & \text{if } f(b) < 0 \\ 0 & \text{if } f(b) = 0 \\ 1 & \text{if } f(b) > 0 \end{cases}$$

Theorem 0.1 *There is an algorithm which given input $b \in \mathbb{Z}$ and $f \in \mathbb{Z}[x]$, computes the sign of $f(b)$ in time polynomial in $\log(|b| + 1)$ and size(f).*

Task: To attain our goal by taking help of the above theorem. Suppose f has only k monomials (i.e only k of the coefficients a_i's are nonzero). We (re)write f as $f = a_1 x^{d_1} + \ldots + a_k x^{d_k}$, where $d_1 > d_2 > \ldots > d_k \geq 0$, and call k the *sparsity* of f.

(a) (**2 points**) Prove that if $f \in \mathbb{R}[x]$ has sparsity k, then it has at most $2k$ real roots.

Definition: Let $f \in \mathbb{Z}[x]$ and $M \in \mathbb{Z}$, $M > 0$. Let $\mathcal{C} = \{[u_i, v_i]\}_{i=1,\ldots,N}$ be a list of closed intervals with integer endpoints satisfying $u_i < u_{i+1}$ and $v_i = u_i$ or $v_i = u_i + 1$ for all i. We say that $\mathcal{C}$ *locates the roots* of f in $[-M, M]$ if for every root r of f in $[-M, M]$ there is an $i \leq N$ such that $r \in [u_i, v_i]$.

Express f as $f = x^{d_k} g$, where $g(0) \neq 0$. Suppose that $\mathcal{C}' = \{[u_i, v_i]\}_{i=1,\ldots,N}$ locates the roots of $\frac{dg}{dx}$ (the derivative of g with respect to x) in $[-M, M]$.

(b) (**5 points**) Show that there is an algorithm which, given input $f, g \in \mathbb{Z}[x]$, M, N and $\mathcal{C}'$ as above, computes a list $\mathcal{C}$ locating all the roots of f in $[-M, M]$. The list $\mathcal{C}$ has at most $N + 2k$ intervals where k is the sparsity of f. The halting time of the algorithm is polynomial in $\log(M+1)$, size(f) and N. [Hint: Use Theorem 0.1]

(c) (**5 points**) Show that there is an algorithm which given input $f \in \mathbb{Z}[x]$ outputs all the integer roots of f in time polynomial in size(f). [Hint: Use (b) and Theorem 0.1. What would be your choice of M?]

7. (**8 points**) Let $\mathcal{L} = \sum_{i=1}^{n} \mathbb{Z}\mathbf{b}_i$ be a lattice generated by $\mathbb{Q}$-linearly independent basis vectors $\mathbf{b}_1, \ldots, \mathbf{b}_n \in \mathbb{Q}^m$, where $m \geq n$. The *dual* of $\mathcal{L}$ is the set $\hat{\mathcal{L}}$ of all $\mathbb{Z}$-linear functions from $\mathcal{L}$ to $\mathbb{Z}$, i.e., the functions $\phi : \mathcal{L} \to \mathbb{Z}$ such that

$$\phi(a\mathbf{x} + b\mathbf{y}) = a\phi(\mathbf{x}) + b\phi(\mathbf{y})$$

for all $a, b \in \mathbb{Z}$ and $\mathbf{x}, \mathbf{y} \in \mathcal{L}$.

(a) (**3 points**) Prove that $\hat{\mathcal{L}}$ is isomorphic to $\mathcal{L}$ as $\mathbb{Z}$-modules.

For any $\mathbf{x} \in \mathbb{Q}^m$, denote by $\phi_{\mathbf{x}}$ the map $\phi_{\mathbf{x}}(\mathbf{y}) = (\mathbf{x}, \mathbf{y})$, where $(\mathbf{x}, \mathbf{y})$ is the inner product of $\mathbf{x}$ and $\mathbf{y}$. Observe that $\phi_{\mathbf{x}} \in \hat{\mathcal{L}}$ if and only if $(\mathbf{x}, \mathbf{y}) \in \mathbb{Z}$ for every $\mathbf{y} \in \mathcal{L}$. We would like to know which $\mathbf{x} \in \mathbb{Q}^m$ has this property. This will give us a nice characterization of the elements of $\hat{\mathcal{L}}$.

(b) (**3 points**) Let B be the $m \times n$ matrix $(\mathbf{b}_1^T\ \mathbf{b}_2^T \ldots \mathbf{b}_n^T)$. Taking into account the correspondence between a vector $\mathbf{x}$ and a map $\phi_{\mathbf{x}}$, show that the row vectors of the $n \times m$ matrix $D = (B^T B)^{-1} B^T$ generate $\hat{\mathcal{L}}$ as a $\mathbb{Z}$-module. Conclude that $\hat{\mathcal{L}}$ is also a lattice, called the *dual lattice* of $\mathcal{L}$, of rank n.

(c) (**2 points**) Prove that the dual of the dual lattice of $\mathcal{L}$ is $\mathcal{L}$ itself. Also, by defining, $\mathrm{vol}(\mathcal{L}) = \sqrt{\det(B^T B)}$, show that $\mathrm{vol}(\hat{\mathcal{L}}) = \mathrm{vol}(\mathcal{L})^{-1}$.

For your information, the notion of dual lattices is used to construct public-key lattice-based cryptographic protocols.