Bordeaux 1 University
Mathematics

MHT 933 - master 2
2009-2010

Exercises for Chapter 2

Exercise 1 – [Minkowski's Theorem]

1. Explain why, as said in the course, we can suppose that q is $\|\cdot\|^2$ (the Euclidean form) in the proof of the Corollary to Minkowski's Theorem (see course).

2. Find a formula for δ_n the volume of the unit ball of $\mathbb{R}^n$ (for the Lebesgue measure).

3. Let $(\Lambda, \|\cdot\|^2)$ be a lattice of $\mathbb{R}^n$. Show directly (using MT bis) that there exists an $x \in \Lambda \setminus \{0\}$ such that $\max |x_i| \leq \mathrm{d}(\Lambda)^{1/n}$ and deduce that there exists an $x \in \Lambda \setminus \{0\}$ such that

$$\| x \| \leq \sqrt{n}\, \mathrm{d}(\Lambda)^{1/n}.$$

4. Compare with the bound $2\delta_n^{-1/n}\mathrm{d}(\Lambda)^{1/n}$ (Corollary to MT).

Exercise 2 – [Minkowski's Theorem]

Let p be a prime number > 2.

1. Recall why we have

$$p \equiv 1 \bmod 4 \Longleftrightarrow -1 \text{ is a quadratic residue modulo } p.$$

2. Admit from now on that $p \equiv 1 \bmod 4$ so that there exists an integer r such that $p \mid r^2 + 1$. Consider the lattice $(\Lambda, \|\cdot\|^2)$ where $\Lambda \subset \mathbb{R}^2$ is the free $\mathbb{Z}$-module generated by $\begin{pmatrix} r \\ 1 \end{pmatrix}$ and $\begin{pmatrix} p \\ 0 \end{pmatrix}$. Using an appropriate disk and Minkowski's Theorem, prove that p is a sum of two squares.

3. Deduce from this that if p is an odd prime number we have

$$p \equiv 1 \bmod 4 \Longleftrightarrow p \text{ is sum of two squares.}$$

N.B. Proof by Paul Turàn.

Exercise 3 – [More on primes as sums of squares]

Part 1

1. Let $x = a + bi$ and $y = c + di \neq 0$ be two Gaussian integers: $x, y \in \mathbb{Z}[i]$ where i is a square root of -1. Prove that there exists an element $q \in \mathbb{Z}[i]$ such that

$$|x - qy|^2 \leq \frac{1}{2}|y|^2$$

and show how to compute such a q.

2. Deduce from this an algorithm to compute $\gcd(u, v)$[1] where u, v are non zero elements of $\mathbb{Z}[i]$.

3. Show that this algorithm has word complexity in $\widetilde{O}(n^2)$ for operands bounded by 2^n in modulus[2].

4. Let $p \equiv 1 \bmod 4$ be a prime. Let m be the smallest positive quadratic non-residue mod p and let us put $x = m^{(p-1)/4} \bmod p$. Show that the computation of $\gcd(p, x + i)$ in $\mathbb{Z}[i]$ gives a decomposition of p as a sum of two squares.

5. Prove that this decomposition is essentially unique.

6. Write a deterministic algorithm with input p and outpout the decomposition of p as a sum of two squares. Evaluate the complexity of this algorithm[3].

7. We have already seen in the previous exercise that Minkowski's Theorem applied to the free $\mathbb{Z}$-module generated by the columns of

$$\begin{pmatrix} p & r \\ 0 & 1 \end{pmatrix}$$

(where $r^2 \equiv -1 \bmod p$) leads to the existence of such a decomposition. Show how the LLL algorithm gives a solution, write another algorithm for the same problem and compare the new complexity to the previous one.

Part 2

From now on, p is a prime such that $p \equiv 3 \bmod 4$.

8. Let x be a quadratic residue mod p. Find an easy way to obtain a square root of x mod p.

9. Prove that there exist $\alpha, \beta \in \mathbb{Z}$ such that

$$\alpha^2 + \beta^2 \equiv -1 \bmod p.$$

[1] Our gcd is not unique: we can multiply it by ± 1 or $\pm i$. This gives four possibilities. Here, we consider any one of those four possibilities to be "the" gcd.

[2] This naive algorithm can be improved and it is possible to obtain a word complexity in $\widetilde{O}(n)$ (A. Weilert 2000) using a divide and conquer approach.

[3] You can assume GRH and use Bach's bound: $m \leq 2(\log p)^2$.

10. Show how to find such a pair thanks to the smallest positive quadratic non-residue m.

11. Let $\Lambda \subset \mathbb{R}^4$ be the free $\mathbb{Z}$-module generated by the columns of

$$\begin{pmatrix} p & 0 & \alpha & \beta \\ 0 & p & \beta & -\alpha \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

Prove that there exists $(a, b, c, d) \in \Lambda$ such that

$$0 < a^2 + b^2 + c^2 + d^2 < 2p,$$

and deduce from this that p can be written as a sum of four squares. Is this decomposition unique?

12. Explain how this result implies that every non negative integer can be written as a sum of four squares (Lagrange 1770).

13. Show how we can obtain, thanks to LLL-algorithm, a decomposition of p as a sum of four squares.

14. Write a deterministic algorithm with input p and with output a decomposition of p as a sum of four squares.

15. Assuming GRH and Bach's bound, compute the word complexity of this algorithm.

Exercise 4 – [LLL-REDUCTION ALGORITHM]

Let d, $N \in \mathbb{Z}_{>0}$ and $x_1, \ldots, x_d \in \mathbb{Z}/N\mathbb{Z}$. Suppose that $N > 2^{(d+1)/4}$.
Show that there is a polynomial deterministic algorithm which gives $(n_1, \ldots, n_d) \neq (0, \ldots, 0)$ such that

$$|n_i| \leq 2^{d/4} N^{1/(d+1)} \text{ for every } i,$$

and

$$\sum_{i=1}^{d} n_i x_i \bmod N \leq 2^{d/4} N^{1/(d+1)}.$$

Hint : Consider the lattice $(\Lambda, \|\cdot\|^2)$ where $\Lambda \subset \mathbb{R}^{d+1}$ is the free $\mathbb{Z}$-module generated by the columns of

$$B = \begin{pmatrix} N & x_1 & x_2 & \cdots & x_d \\ 0 & 1 & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & \ddots & 0 \\ 0 & \cdots & \cdots & 0 & 1 \end{pmatrix}.$$

N.B. Here $a \bmod b \in [0, b-1]$.

Exercise 5 – [PROOF OF THE THEOREM ON THE LLL-REDUCTION ALGORITHM]

In a first time we want to prove that LLL-algorithm terminates.

1. Let

$$\Lambda_i = \langle b_1, \dots, b_i \rangle_{\mathbb{Z}}$$

denote the lattice in $\Lambda_i \otimes_{\mathbb{Z}} \mathbb{R}$ generated by the first i basis vectors. So $\Lambda_n = \Lambda$. Then define

$$D_i = \operatorname{disc}(\Lambda_i) = \prod_{j \leq i} q(b_j^*),$$

$$D = \prod_{i=1}^{n-1} D_i = q(b_1^*)^{n-1} \dots q(b_{n-1}^*).$$

Show that during each swap D gets replaced by an integer which is less than $\frac{3}{4}D$.

2. Let $A = \max_{i \leq n} q(b_i)$. Show that the number of swaps is $O(n^2 \log A)$ and that the algorithm terminates.

3. Show that the total number of operations is $O(n^4 \log A)$.

Now we want to prove that these operations deal with integers of size $O(n \log A)$.

4. Prove that at any point in the algorithm we have

$$D_{k-1} b_k^* \in \mathbb{Z}^n$$

and

$$D_l \mu_{k,\ell} \in \mathbb{Z}$$

for all $\ell < k \leq n$.

5. Show that at each step

$$D_i \leq A^i$$

and, thanks to this inequality, that the denominators of rational numbers in the algorithm are bounded by $O(n \log A)$.

6. Show that

$$|\mu_{i,j}|^2 \leq D_{j-1} q(b_i).$$

7. Show that $q(b_i) \leq nA$ everywhere except possibly during the reduction step.

8. Let

$$m_i = \max\{|\mu_{i,j};\ 1 \leq j \leq i\}.$$

Show that at the beginning of the reduction step, we have $m_i^2 \leq nA^n$ and that during the reduction step m_i cannot be multiplied by more than 2^{i-1}.

9. Show that during the reduction step we have

$$q(b_i) \leq n^2(4A)^{n+1}$$

and prove that the denominators of the numbers occuring in the algorithm all have length $O(n \log A)$.

Exercise 6 – [HNF–SNF]

Prove the uniqueness of the HNF and more generally that, if A and B are matrices of $M_{m\times n}(\mathbb{Z})$ and $M_{m\times \ell}(\mathbb{Z})$ whose columns generate the same submodule of $\mathbb{Z}^m$, the H-parts of their HNF are equal (see course).

Exercise 7 – [HNF–SNF]

Let $A \in M_n(\mathbb{Z})$ and $(d_1, \ldots, d_n)$ be the diagonal of its SNF. Then

$$\mathbb{Z}^n/\mathrm{Im}(A) \simeq \bigoplus_{i=1}^{n} (\mathbb{Z}/d_i\mathbb{Z})$$

Exercise 8 – [HNF–SNF]

Solve $XA = Y$, where $Y \in M_{\ell\times n}(\mathbb{Z})$, $A \in M_{m\times n}(\mathbb{Z})$, unknown $X \in M_{\ell\times m}(\mathbb{Z})$.
Hint: Write $AU = (0 \mid H)$.

Exercise 9 – [HNF–SNF]

Solve

$$AX = \begin{pmatrix} y_1 \bmod d_1 \\ \vdots \\ y_n \bmod d_n \end{pmatrix}$$

Hint: $AX = Y + DZ$, D diagonal $\Rightarrow (A \mid -D)\begin{pmatrix} X \\ Z \end{pmatrix} = Y$.