PuMAC 2009-10 Power Test Solution

A Version

21 Problems; 86 Points

1 Notation

Throughout the solutions we will refer to $\{(1,0,\ldots,0),(0,1,\ldots,0),\ldots,(0,0,\ldots,1)\}$ as the **standard basis** of $\mathbb{Z}^n$. The vector with the ith entry equal to one and the rest zero will be denoted by $\vec{e_i}$.

2 Lattices (4 Problems; 15 Points)

Problem 2.1 (3pts)**.** *What are all the lattices in dimension one (That is, specify their general form in the simplest possible terms).*

Let L be a lattice of dimension 1. If $L \neq \{0\}$, L contains a smallest positive integer d. We claim that $L = d\mathbb{Z}$. Suppose $a \in L$. By the division algorithm, write $a = qd + r$, $0 \leq r < d$. Then $r = a - qd \in L$ and hence $r = 0$ by the minimality of d. Thus $d|a$, which shows $L \subset d\mathbb{Z}$. The opposite containment is obvious. Including $\{0\}$, $L = d\mathbb{Z}$ for nonnegative integers d.

Problem 2.2 (4pts)**.** *Prove that the lattice in dimension n generated by a set S is full if and only if every vector in $\mathbb{Z}^n$ is expressible as a* rational *linear combination of vectors in S, i.e. if every $\vec{a} \in \mathbb{Z}^n$ is expressible in the form $\sum a_i x_i$, where $x_i \in S$ and $a_i \in \mathbb{Q}$.*

Suppose lattice L generated by S is full. Then given $\vec{a} \in \mathbb{Z}^n$, $N\vec{a} \in L$ for some positive integer N, so $N\vec{a}$ can be written as an integral linear combination of vectors in S. Dividing through by N gives $\vec{a}$ as a rational linear combination of vectors in S.

Conversely, given any $\vec{a} \in \mathbb{Z}^n$, write it as a rational linear combination of vectors in S: $\vec{a} = \frac{p_1}{q_1}\vec{s_1} + \cdots + \frac{p_k}{q_k}\vec{s_k}$. Multiplying through by $N = \prod q_i$ gives $N\vec{a}$ as an integral linear combination of s_i, so $N\vec{a} \in L$.

Problem 2.3 (4pts)**.** *Is the lattice generated by $\{(2,1,6),(5,6,8),(1,1,2)\}$ full?*

Since $(2,1,6) + (5,6,8) = 7(1,1,2)$, the lattice generated by $\{(2,1,6),(5,6,8)\}$ is full if and only if the lattice generated by $\{(2,1,6),(5,6,8),(1,1,2)\}$ is full. Now the condition in Problem 2.2 is that

$$\begin{pmatrix} 2 & 5 \\ 1 & 6 \\ 6 & 8 \end{pmatrix} \begin{pmatrix} a_1 \\ a_2 \end{pmatrix} = \begin{pmatrix} x \\ y \\ z \end{pmatrix}$$

has rational solutions a_1, a_2 for any integer triple (x, y, z). Consider $(x, y, z) = (0, 0, 1)$, then $2a_1 + 5a_2 = 1a_1 + 6a_2 = 0$. Solving for two unknowns with two equations yields $a_1 = a_2 = 0$ as the only possible solution. We see that it is impossible to simultaneously also have $6a_1 + 8a_2 = 1$ so the lattice is not full.

Problem 2.4 (4pts)**.** *Is the lattice generated by* $\{(2, 1, 6), (5, 6, 8), (1, 2, 2)\}$ *full?*

We now wish to solve

$$\begin{pmatrix} 2 & 5 & 1 \\ 1 & 6 & 2 \\ 6 & 8 & 2 \end{pmatrix} \begin{pmatrix} a_1 \\ a_2 \\ a_3 \end{pmatrix} = \begin{pmatrix} x \\ y \\ z \end{pmatrix}.$$

The matrix is invertible, having determinant $2(12 - 16) - 5(2 - 12) + 1(8 - 36) = 14 \neq 0$. Multiplying both sides by the inverse on the left, which has rational entries, produces rational a_i for any triple (x, y, z), so this lattice is full. One can use other methods to solve this system of equations as long as it is justified why the solution will be rational.

3 Determinant and Divisor (5 Problems; 17 Points)

Problem 3.1 (2pts)**.** *Show that* $\vec{a} + L = \vec{b} + L$ *if and only if* $\vec{a} - \vec{b} \in L$.

If $\vec{a} + L = \vec{b} + L$, then in particular $\vec{a} + \vec{0} \in \vec{b} + L$, so $\vec{a} = \vec{b} + \vec{l}$ for some $\vec{l} \in L$ and thus $\vec{a} - \vec{b} = \vec{l} \in L$. Conversely, suppose $\vec{a} - \vec{b} \in L$. For any $\vec{l} \in L$, we have $\vec{a} + \vec{l} = \vec{b} + (\vec{a} - \vec{b} + \vec{l})$ with $\vec{a} - \vec{b} + \vec{l} \in L$, so $\vec{a} + \vec{l} \in \vec{b} + L$. This shows $\vec{a} + L \subset \vec{b} + L$. Since $-(\vec{a} - \vec{b}) = \vec{b} - \vec{a}$, exchanging the roles of $\vec{a}$ and $\vec{b}$ in the above argument shows the opposite containment. Hence $\vec{a} + L = \vec{b} + L$.

Problem 3.2 (2pts)**.** *Show that if* $\vec{a} - \vec{b} \notin L$*, then* $(\vec{a} + L) \cap (\vec{b} + L) = \varnothing$.

We check the contrapositive: if $(\vec{a} + L) \cap (\vec{b} + L) \neq \varnothing$, then $\vec{a} + \vec{l_1} = \vec{b} + \vec{l_2}$ for some $\vec{l_i} \in L$, so $\vec{a} - \vec{b} = \vec{l_2} - \vec{l_1} \in L$.

Problem 3.3 (3pts)**.** *Let* L *be the lattice generated by* $\{(1, 2), (2, 1)\}$*. Draw the colattices* $(0, 0) + L$*,* $(0, 1) + L$*, and* $(0, 2) + L$*. If you drew the diagram correctly, it should sort of jump out that these are distinct colattices. If it doesn't jump out, check your diagram! Now prove that these colattices are in fact distinct without using the diagram. Also, prove that* L *has no more colattices. Hence, conclude that* $\det L = 3$.

We show that $(a, b) \in L$ iff $3|a + b$. Any $(a, b) \in L$ has the form $n(1, 2) + m(2, 1) = (n + 2m, 2n + m)$ for integers n and m, so $a + b = 3(n + m)$. Conversely, if $3|a + b$, then

$$(a, b) = \left(b - \frac{a + b}{3}\right)(1, 2) + \left(a - \frac{a + b}{3}\right)(2, 1) \in L.$$

By the above criteria, the difference of any two distinct vectors in $\{(0, i) : i = 0, 1, 2\}$ does not lie in L. Then by Problem 3.1, $(0, i) + L$, $i = 0, 1, 2$, are distinct. For an arbitrary colattice $(a, b) + L$, $3|a + b - i$ for $i = 0, 1$, or 2. Then $(a, b) - (0, i) \in L$, so $(a, b) + L = (0, i) + L$ by Problem 3.1. Hence these are all the colattices, i.e. $\det L = 3$.

Problem 3.4 (5pts)**.** *, Prove that a lattice is full if and only if its determinant is finite.*

Suppose L is full. Then for each $k = 1, \ldots, n$, $N_i\vec{e_i} \in L$ for some positive integer N_i. Given any $\vec{a} = (a_1, \ldots, a_n) \in L$, write $a_i = q_iN_i + r_i$, $0 \leq r_i < N_i$, by the division algorithm on each coordinate. Then

$$\vec{a} - (r_1, \ldots, r_n) = (q_1N_1, \ldots, q_nN_n) = q_1(N_1\vec{e_1}) + \cdots + q_n(N_n\vec{e_n}) \in L.$$

By Problem 3.1, $\vec{a}+L = (r_1, \ldots, r_n)+L$. There are only finitely many colattices $(r_1, \ldots, r_n)+L$ with $0 \leq r_i < N_i$, so $\det L < \infty$.

Now suppose $\det L < \infty$. Then given $\vec{a} \in \mathbb{Z}^n$, the colattices $k\vec{a} + L$, $k \in \mathbb{Z}$, cannot all be distinct, so $k_1\vec{a}+L = k_2\vec{a}+L$ for some $k_1 > k_2$. By Problem 3.1, this implies $(k_1 - k_2)\vec{a} \in L$. Taking $N = k_1 - k_2$ shows that L is full.

Problem 3.5 (5pts)**.** *Prove that if L is a full lattice in dimension n, then its determinant is divisible by* $(\operatorname{div} L)^n$.

Let $\operatorname{div} L$ be denoted by d so that we have the series of inclusions $L \subset d\mathbb{Z}^n \subset \mathbb{Z}^n$. There are d^n colattices of $d\mathbb{Z}^n$ in $\mathbb{Z}^n$ explicitly given as $A_1 = \{(a_1, \ldots, a_n) + d\mathbb{Z}^n | 0 \leq a_i \leq d - 1\}$. Consider the set of colattices of L which we will denote A_2. A function $f : A_2 \to A_1$ can be defined by $f(\vec{a} + L) = \vec{a} + d\mathbb{Z}^n$. Note that it does not matter if we choose a different $\vec{b}$ to represent the same collatice because then $\vec{a} - \vec{b} \in L \subset d\mathbb{Z}^n$ so they define the same collatice of $d\mathbb{Z}^n$. Let $f^{-1}(\vec{a} + d\mathbb{Z}^n)$ denote the subset of A_2 which maps to $\vec{a} + d\mathbb{Z}^n$ by f. This set is non-empty and its size does not vary as we vary the collatice in A_1. Indeed, let c_i be such that $\{c_i + L | 1 \leq i \leq k\} = f^{-1}(d\mathbb{Z}^n)$. For any $\vec{a} + d\mathbb{Z}^n \in A_1$ it is easy to check that $\{\vec{a} + c_i + L | 1 \leq i \leq k\} = f^{-1}(\vec{a} + d\mathbb{Z}^n)$. Now A_1 has been partitioned by the $f^{-1}(\vec{a} + d\mathbb{Z}^n)$ into d^n distinct sets each of size k. We conclude that $kd^n = \det L$ and so $(\operatorname{div} L)^n$ divides the determinant of L.

4 Finite Generation (3 Problems; 13 Points)

Problem 4.1 (3pts)**.** *Prove that if $L_1 \supsetneq L_2$, then* $\det L_1 < \det L_2$ *(or both are ∞).*

Let A_1 and A_2 be the sets of colattices of L_1 and L_2 respectively so that the size of A_i is $\det L_i$. If A_2 is an infinite set, then we are already done. Let A_2 be a finite set. We can define a function $f : A_2 \to A_1$ by sending a colattice $\vec{a} + L_2 \in A_2$ to $\vec{a} + L_1 \in A_1$. Note that if $\vec{a} + L_2 = \vec{b} + L_2$ then $\vec{a} + L_1 = \vec{b} + L_1$ because of Problem 3.1 and $\vec{a} - \vec{b} \in L_2 \subset L_1$. Furthermore, every collatice in A_1 is mapped to by some collatice in A_2 simply by considering $f(\vec{a} + L_2) = \vec{a} + L_1$ for any $\vec{a} \in \mathbb{Z}^n$. Therefore, the number of elements of A_1 is less than or equal to the number of elements of A_2. To prove the strict inequality, we need to exhibit two colattices in A_2 mapping to the same colattice in A_1. Take $\vec{l} \in L_1$ with $\vec{l} \notin L_2$, then $f(\vec{l} + L_2) = f(\vec{0} + L_2) = L_1$ but $\vec{l} + L_2 \neq L_2$.

Problem 4.2 (5pts)**.** *Prove that every full lattice has a full sublattice that is finitely generated.*

Let L denote our full lattice in $\mathbb{Z}^n$ and let $\vec{e_i}$ for $1 \leq i \leq n$ be the standard basis. By the definition of fullness, there exist positive integers N_i for $1 \leq i \leq n$ such that $N_i\vec{e_i} \in L$. The lattice K generated by $\{N_i\vec{e_i}\}$ is a sublattice of L because any integer linear combination of vectors in a lattice is still a vector in the lattice. To see that K is full, take any $\vec{a} \in \mathbb{Z}$ written as $\vec{a} = \sum k_i\vec{e_i}$, then $\prod N_i\vec{a}$ is in K.

Problem 4.3 (5pts)**.** *Prove that every full lattice if finitely generated.*

We combine the last two problems to solve this problem. Consider the set of finitely generated full sublattices of L. These lattices have finite determinant by Problem 3.4 and so by the well ordering principle, there must be a finitely generated full sublattice M with minimal determinant. Assume M does not equal to L so that we can take $\vec{l} \in L$ with $\vec{l} \notin M$. The generators of M together with $\vec{l}$ generate a finitely generated full sublattice of L which we will call M'. Clearly $M' \supsetneqq M$ so by Problem 4.1 $\det M' < \det M$. Therefore M' violates the minimality of M so it must have been that $M = L$ and L is finitely generated.

5 Isomorphism Types of Lattices (7 Problems; 28 Points)

Definition 5.1. Two lattices L_1 and L_2 in $\mathbb{Z}^n$ are said to be *isomorphic* iff there exists a linear bijection $f : \mathbb{Z}^n \to \mathbb{Z}^n$ which is also a bijection from L_1 to L_2. [A map $f : \mathbb{Z}^n \to \mathbb{Z}^m$ is said to be linear iff $f(\vec{0}) = \vec{0}$, and $f(\vec{a} + \vec{b}) = f(\vec{a}) + f(\vec{b})$].

For example, the linear bijection $f : \mathbb{Z}^2 \to \mathbb{Z}^2$ defined by $f(x, y) = (5x + 2y, 2x + y)$ is also a bijection from the lattice L_1 generated by $\{(2, 1), (1, 2)\}$ to the lattice L_2 generated by $\{f(2, 1), f(1, 2)\} = \{(12, 5), (9, 4)\}$; hence L_1 and L_2 are isomorphic. Note that L_2 is also the lattice generated by $\{(3, 0), (0, 1)\}$.

Problem 5.1 (2pts)**.** *Prove that* div *is an isomorphism invariant.*

Let the two lattices L_1 and L_2 be isomorphic by the bijective linear map $f : \mathbb{Z}^n \to \mathbb{Z}^n$. First we show that for any $\vec{a} \in \mathbb{Z}^n$ and any d a positive integer, $f(d\vec{a}) = df(\vec{a})$. This is true for $d = 1$. If it is true for d then it is true for $d + 1$ by

$$f((1 + d)\vec{a}) = f(\vec{a} + d\vec{a}) = f(\vec{a}) + f(d\vec{a}) = f(\vec{a}) + df(\vec{a}) = (1 + d)f(\vec{a}).$$

If the divisors of L_1 and L_2 are denoted d_1 and d_2 respectively then this shows that because every member of L_1 is of the form $d_1\vec{a}$ then so is every member of L_1. Now $d_2 \geq d_1$ by definition. Taking f^{-1} reverses the roles to obtain $d_1 \geq d_2$ and therefore $d_1 = d_2$.

Problem 5.2 (2pts)**.** *Prove that* det *is an isomorphism invariant.*

Let two lattices L_1 and L_2 be isomorphic by the bijective linear map $f : \mathbb{Z}^n \to \mathbb{Z}^n$. Consider a collatice $\vec{a} + L_1$ which maps by f to $f(\vec{a}) + f(L_1) = f(\vec{a}) + L_2$. Therefore f maps collatices to collatices. The inverse map f^{-1} is an inverse to that map on collatices, so the number of collatices of L_1 is equal to the number of collatices of L_2.

Problem 5.3 (3pts)**.** *Are the lattices generated by* $\{(3, 0), (0, 5)\}$ *and* $\{(1, 0), (0, 15)\}$ *isomorphic?*

Yes, the lattices are isomorphic. This follows from Problem 5.6 below, since both lattices have divisor 1 and determinant 15.

Problem 5.4 (3pts). *Are the lattices generated by* $\{(2,0),(0,4)\}$ *and* $\{(1,0),(0,8)\}$ *isomorphic?*

No, the lattices are not isomorphic. This follows from Problem 5.1 above since the divisors are 2 and 1 respectively.

Problem 5.5 (4pts). *For any two integers* $d \geq 1$ *and* $\Delta \geq 1$ *with* Δ *divisible by* d^2*, give an example of a lattice in* $\mathbb{Z}^2$ *with divisor* d *and determinant* Δ*.*

Consider the lattice L generated by $\{(d,0),(0,\Delta/d)\}$. Since d^2 divides Δ, we know that d divides Δ/d. Thus the divisor of L is at least d. By looking at the first generator, we conclude that the divisor of L is at most d. Thus $\operatorname{div} L = d$. Also we certainly have $\det L = d \cdot (\Delta/d) = \Delta$.

Problem 5.6 (7pts). *Prove that if two full lattices in* $\mathbb{Z}^2$ *have the same determinant and same divisor then they are isomorphic. Conclude that all full lattices in* $\mathbb{Z}^2$ *are isomorphic to one of the lattices from problem 5.5 (don't forget the result of problem 3.5).*

By rescaling, it suffices to treat the case that $d = 1$. Suppose we are given a full lattice L in dimension two with $\operatorname{div} L = 1$ and $\det L = \Delta$. We would like to show that L is isomorphic to the lattice generated by $\{(1,0),(0,\Delta)\}$.

Since L is full, we know that $(E,0) \in L$ for some large E. Pick the smallest such E, and let $\vec{a} = (0,E) \in L$. Now again since L is full, the set of y-coordinates of vectors in L contains some elements other than zero. Thus we can find a vector $\vec{b} = (C,D) \in L$ where $C > 0$ is as small as possible. From our choice of vectors, it is clear that $\vec{a}$ and $\vec{b}$ generate L. Thus since $\operatorname{div} L = 1$, we know that $\gcd(C,D,E) = 1$. Thus there exists an integer k such that $\gcd(C, D + kE) = 1$. WLOG, we may assume that $k = 0$. Thus $\gcd(C,D) = 1$, so there exist integers x, y with $Cx + Dy = 1$. Now consider the matrix $M = \left(\begin{smallmatrix} C & D \\ -y & x \end{smallmatrix}\right)$. Since $\det M = Cx + Dy = 1$, M is invertible and M^{-1} has integer entries. Thus we may apply the matrix M^{-1} to the generators of L and get generators of an isomorphic lattice L'. Since $M(1,0) = \vec{b}$, we conclude that $(1,0) \in L'$. Now we are done, since every lattice containing $(1,0)$ is equal to the lattice generated by $\{(1,0),(0,P)\}$ for some integer P. Comparing determinants, we conclude that $P = \Delta$, so the desired isomorphism is demonstrated.

Problem 5.7 (7pts). *Prove that divisor and determinant do not characterize lattices in dimension three. That is, construct two lattices* L_1 *and* L_2 *in* $\mathbb{Z}^3$ *which have the same determinant and the same divisor but which are not isomorphic.*

Let L_1 be the lattice generated by $\{(1,0,0),(0,2,0),(0,0,2)\}$ and let L_2 be the lattice generated by $\{(1,0,0),(0,1,0),(0,0,4)\}$. Both L_1 and L_2 have divisor 1 and determinant 4. By inspection, we see that for any vector $\vec{a} \in \mathbb{Z}^3$, it is true that $2\vec{a} \in L_1$. This property is clearly preserved under isomorphism. However, the vector $\vec{a} = (0,0,1)$ satisfies $2\vec{a} \notin L_2$. Thus L_1 and L_2 are not isomorphic.

6 Canonical Form (2 Problems; 13 Points)

The following theorem is true (proving it is not part of this test).

Theorem 6.1. *Every lattice in dimension n is isomorphic to the lattice generated by*

$$\{d_1\vec{e}_1, \ldots, d_n\vec{e}_n\} \tag{6.1}$$

for some $d_i \in \mathbb{N} \cup \{0\}$ where $d_i | d_{i+1}$. Furthermore, the sequence of integers $(d_1; \ldots; d_n)$ is isomorphism invariant; it is called the signature *of the lattice.*

You may assume it is true for any of your work on problems appearing after this point in the test.

Problem 6.1 (5pts)**.** *Calculate the signature of the lattice generated by:*

$$\{(2, 2, 0), (0, 3, 3)\} \tag{6.2}$$

Since the signature is isomorphism-invariant, we will change the base space slightly, and take the given lattice (call it L) to be the lattice generated by $\{(2, 2, 0), (3, 0, 3)\}$. We can do that by the isomorphism that switches the first two coordinates of an element [so $(2, 2, 0)$ goes to itself, and $(0, 3, 3)$ goes to $(3, 0, 3)$]. So it is enough to find the signature of *this* lattice. But we immediately have $(3, 0, 3) - (2, 2, 0) = (1, -2, 3)$ and $(2, 2, 0) - 2(1, -2, 3) = (0, 6, -6)$, so that our lattice L is in fact generated by $(1, -2, 3)$ and $(0, 6, -6)$. So now, call $(1, -2, 3) = \mathbf{e_1}$ and $(0, 1, -1) = \mathbf{e_2}$. It is easy to show that in $\mathbb{Z}^n$, these basis vectors are exactly equivalent to the usual definitions of $\mathbf{e_1} = (1, 0, 0)$ and $\mathbf{e_2} = (0, 1, 0)$. In particular, the lattice L is generated by $1\mathbf{e_1}$ and $6\mathbf{e_2}$ and $0\mathbf{e_3}$. So, since we have isomorphism invariance, the lattice must also be generated by $\{1(1, 0, 0), 6(0, 1, 0), 0(0, 0, 1)\}$. Hence, the signature of the lattice is $(1; 6; 0)$.

Problem 6.2 (8pts)**.** *Calculate the signature of the lattice generated by:*

$$\{(0, 2, 5, 3), (5, 4, 5, 7), (5, 9, 7, 1), (5, 7, 5, 7)\} \tag{6.3}$$

The signature is $(1; 1; 3; 180)$.

In general, a lattice can be represented by a matrix M with columns generating the lattice. The same lattice is generated if one replaces the *columns* by invertible linear combinations. One can also obtain an isomorphic lattice by taking bijective linear transformations of the underlying $\mathbb{Z}^n$ which amounts to replacing the *rows* by invertible linear combinations. The goal is to compute the signature of the lattice by transforming the matrix M into a diagonal matrix. In this case M is the 4 by 4 matrix

$$\begin{pmatrix} 0 & 5 & 5 & 5 \\ 2 & 4 & 9 & 7 \\ 5 & 5 & 7 & 5 \\ 3 & 7 & 1 & 7 \end{pmatrix}.$$

By using the third column to eliminate the bottom row and one obtains

$$\begin{pmatrix} -15 & -30 & 5 & -30 \\ -25 & -59 & 9 & -56 \\ -16 & -44 & 7 & -44 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

Using the fourth row, one can now elminate the entries in the third column and we are now left with the remaining three by three matrix

$$\begin{pmatrix} 15 & 30 & 30 \\ 25 & 59 & 56 \\ 16 & 44 & 44 \end{pmatrix}.$$

Subtracting the first row from the second and third, then clearing out the first column with the last row yields

$$\begin{pmatrix} 0 & -180 & -180 \\ 0 & -111 & -114 \\ 1 & 14 & 14 \end{pmatrix}.$$

Clearing out the bottom row now leaves us with a two by two matrix which we easily reduce in a few steps:

$$\begin{pmatrix} 180 & 180 \\ 111 & 114 \end{pmatrix} \to \begin{pmatrix} 180 & 0 \\ 111 & 3 \end{pmatrix} \to \begin{pmatrix} 3 & 0 \\ 0 & 180 \end{pmatrix}$$

This solution is very close to a proof of Theorem 6.1. See if you can figure it out.