PUMaC 2009-10 Power Test

B Version

21 Problems; 86 Points

1 Instructions / Rules

These rules supersede any rules appearing elsewhere about the Power Test.

The problems on this test all require you to prove your answer. This means that you should justify your steps in a way that is correct, complete, and succinct. Credit will not be given for an answer without proof.

For the solution of any given problem, you are allowed to use *without proof* the results of all *previous problems* (that is, problems that appear above in the test), even if your team has not solved those problems.

For a YES/NO question, just answsering YES or NO is worth **ZERO** points. You must provide justification to recieve **ANY** credit.

For problems which ask you to perform a calculation, you must show your work as in any other proof. This work should be clearly justified, not just a sheet of unexplained calculations.

It is not necessary to do the problems in order, though it is a good idea to read all the problems, so that you know what is permissible to assume when doing a given problem. However, please collate the solutions in order in your solution packet.

Consulting printed and online references, as well as the use of calculators, computer programs, Mathematica, etc. is allowed. However you must not discuss the problems with anyone outside of your team.

2 Lattices (4 Problems; 15 Points)

We will use the symbol $\mathbb{Z}$ to refer to the set of integers (whole numbers, like 0, 1, 456, and -952); similarly, we will use the slightly more intimidating symbol $\mathbb{Z}^n$ to refer to the set of ordered n-tuples of integers. Each of these n-tuples can be assigned a name and written as a letter with an arrow like a vector on top of it (for instance, $\vec{x}$ can refer to an n-tuple). The individual elements of an n-tuple are called its coordinates. For example, the first, second, and third coordinates of the n-tuple $(3, 9, 0)$ are 3, 9, and 0 respectively. If $\vec{a}, \vec{b} \in \mathbb{Z}^n$ are two elements, then $\vec{a}+\vec{b}$ denotes their coordinatewise sum, in other words the new n-tuple whose coordinates are, in order, the sum of the corresponding coordinates of the added n-tuples $\vec{a}$ and $\vec{b}$.

For example, $(2,4,5) \in \mathbb{Z}^3$, $(54,2,-3432,0) \in \mathbb{Z}^4$, $(3,0,-1) \in \mathbb{Z}^3$, and $(2,4,5) + (3,0,-1) = (2+3, 4+0, 5-1) = (5,4,4)$.

Definition 2.1. A *lattice in dimension n* is an exceptionally complicated term we will throw at you throughout this test. Don't worry, it is not really a very difficult concept to grasp. The formal definition of a lattice in dimension n is a subset L of $\mathbb{Z}^n$ with the following properties:

1. $(0, \ldots, 0) \in L$.
2. If $\vec{a} \in L$ then $-\vec{a} \in L$.
3. If $\vec{a}, \vec{b} \in L$ then $\vec{a} + \vec{b} \in L$.

The best way to understand lattices is to take an example in two dimensions, which is easy to visualize. So, from the definition, a lattice in two dimensions turns out to be a set of ordered pairs of integers which contains $(0,0)$, so that if you choose any two (not necessarily distinct) elements (a,b) and (c,d) from this lattice, *each* of the following elements is also in the lattice: $(a+c, b+d)$, $(-a,-b)$ and $(-c,-d)$. If you think about this in terms of coordinates on a Cartesian map, then remember that the points (a,b), $(a+p, b+q)$, $(a+r, b+s)$ and $(a+p+r, b+q+s)$ form a parallelogram. Then, a lattice looks something like this:

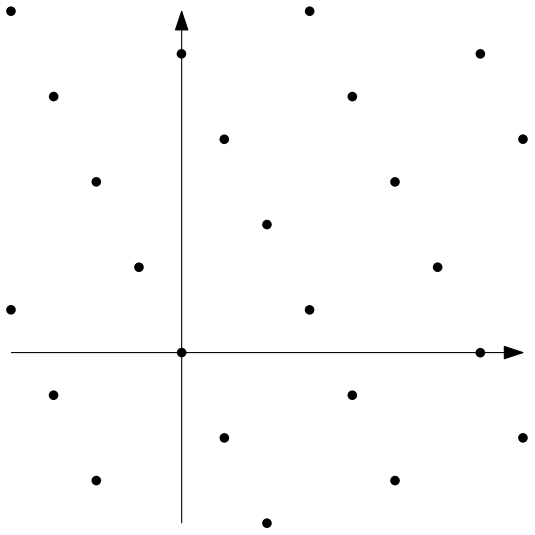

Figure 1: An example of a lattice.

Notice how the lattice looks something like the points representing the corners of the squares on a tilted and skewed chessboard, one of which coincides with the origin, and all of which have integer coordinates.

A lattice in n dimensions is simply a generalization of this 2-dimensional scenario into n dimensions. It would perhaps be slightly unfair to ask you to visualize a lattice as an n-dimensional skewed and tilted chessboard, but that's essentially what it is. If you have never encountered lattices before, don't worry; just read carefully through the formal definition

and the subsequent explanation once more. All in all, it is a simple enough concept; the key lies in understanding that it is just a set of n-tuples of integers that satisfies the 3 properties given in the definition. Please (for your own sake) don't forget that you are dealing with n-tuples of *integers* only.

If we have a set S of n-tuples of integers, we can form a lattice in dimension n by taking the set of all integer linear combinations of the n-tuples in S. This is called the *lattice generated by* S. Notice the fact that this set *does* satisfy all the conditions for lattices described above in the definition, and thus forms a lattice. If you don't get that readily, consider a set S of vectors in $\mathbb{Z}^n$, and let L be the set of all integer linear combinations of the vectors in S, so L is the lattice generated by S. Now, obviously $(0, 0, \ldots, 0) \in L$, because $(0, 0, \ldots, 0)$ is a linear combination of any set of n-tuples. Also, if $\vec{a} \in L$, then $\vec{a} = \sum c_i \vec{s}_i$ for some vectors $\vec{s}_i \in S$ and integers c_i. Then, L also contains $\sum -c_i \vec{s}_i = -\vec{a}$, so the second condition holds. The third condition follows similarly; suppose $\vec{a} \in L$ and $\vec{b} \in L$. Then $\vec{a} = \sum c_i \vec{s}_i$, for vectors $s_i \in S$ and integers c_i, and $\vec{b} = \sum d_i \vec{s}_i$, for $\vec{s}_i \in S$ and integers d_i. Note that here, the s_i run over *all* the vectors in S, so some of the c_i and d_i may be zero. Then, we may write $\vec{a} + \vec{b} = \sum (c_i + d_i)\vec{s}_i$ must also be in L. Thus, the third condition also holds.

An example: the lattice generated by $S = \{(1, 1), (1, -1)\}$ is the set of all integer linear combinations of $(1, 1)$ and $(1, -1)$, that is the subset $\{(a+b, a-b)\}$ of $\mathbb{Z}^2$, where a and b run over the integers. This comes out to be simply the set of all $(x, y) \in \mathbb{Z}^2$ with the property that $x + y$ is even. The diagram below shows the points representing the vectors of this lattice.

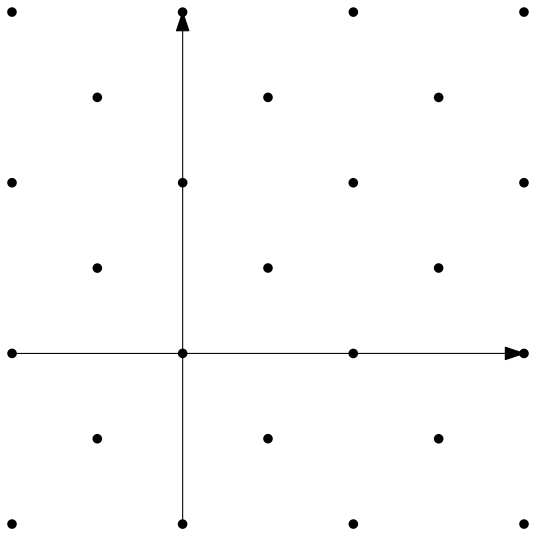

Figure 2: The lattice generated by $\{(1, 1), (1, -1)\}$.

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

Definition 2.2. A lattice L in dimension n is said to be *full* iff for every $\vec{a} \in \mathbb{Z}^n$, there is a positive integer N so that $N\vec{a} \in L$.

In essence, then, a lattice is full if there is a natural number N for every n-tuple of integers, which can be multiplied with this n-tuple to obtain an element in the lattice. This number N may depend on the n-tuple chosen, and can be thought of as a "multiplier" that *carries* the n-tuple into the lattice.

For example, the lattice generated by $\{(1,1),(1,-1)\}$ is full. This is because, if $(a,b) \in \mathbb{Z}^2$, then $2(a,b) = (2a,2b) = ((a+b)+(a-b),(a+b)-(a-b)) = (a+b)(1,1)+(a-b)(1,-1)$. However, the lattice generated by $\{(6,12),(10,20)\}$ is not full. If you draw this then you will see why.

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. iff every n-tuple of integers is expressible in the form $\sum a_i x_i$, for some $x_i \in S$ and $a_i \in \mathbb{Q}$.*

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

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

3 Determinant and Divisor (5 Problems; 17 Points)

Definition 3.1. Let's say we have a lattice L in $\mathbb{Z}^n$ (see the definition we provided earlier if you're anything between mildly confused and scared out of your wits). A *colattice* is another one of the intimidating terms we will throw at you. Formally, a colattice $\vec{a} + L$ for $\vec{a} \in \mathbb{Z}^n$ is the set of vectors $\{\vec{a} + \vec{\ell}\}$ where $\vec{\ell}$ ranges over all the vectors in L. So, a colattice is a set of vectors which has a correspondence with the lattice L; every element $\vec{x}$ in L has the corresponding element $\vec{a} + \vec{x}$ in the colattice $\vec{a} + L$. So a colattice can be thought of as the same lattice "shifted", in a sense. The essential point to keep in mind is that there is a correspondence between a lattice and any one of its colattices: every element of one corresponds to exactly one element of another, with the two elements differing simply by a fixed shift.

For the following problems, keep in mind the notation for colattices.

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

[Note: two sets A and B are said to be *equal* if they have exactly the same elements, that is $A \subseteq B$ and $B \subseteq A$. Also, for this problem, notice the bidirectionality, i.e. proving one direction will only get you half credit. The next problem, however, deals only with *one* direction.]

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

[To clarify, $\varnothing$ denotes the empty set, so the question asks you to prove that if the first condition holds, then the two colattices $(\vec{a} + L)$ and $(\vec{b} + L)$ have no element in common. Note: it *might* help to remember that $A \implies B$ is equivalent to proving $\bar{B} \implies \bar{A}$, where the bars stand for the negations of the corresponding statements.]

Definition 3.2. The *determinant* of a lattice L, denoted by $\Delta = \det L$, is the number of *distinct* colattices of L.

We remark that the determinant may be infinite. If you don't see immediately why, notice, for example, that the lattice L generated by $\{(2,3),(12,18)\}$ has an infinite determinant. This is because the colattices $(0,a)+L$, where a runs over the integers, are all distinct. You can work that out yourself, by noticing that L is simply the set $\{(2k,3k)\}$, where k runs over the integers. Then, for two distinct integers a_1 and a_2, we have, from Problem 3.1, $(0,a_1)+L = (0,a_2)+L$ if and only if $(0,a_1)-(0,a_2) \in L$, that is if $(0,a_1-a_2) \in L$. But that means for some integer k, we must have $2k = 0$ and $3k = a_1 - a_2$, leading to $a_1 = a_2$. So, the colattices are distinct for distinct integers, and since the number of integers is infinite, the number of distinct colattices is infinite as well. Thus, the determinant is infinite.

Problem 3.3 (3pts)**.** *Suppose we denote by L the lattice generated by $\{(1,2),(2,1)\}$. Draw the colattices $(0,0)+L$, $(0,1)+L$, and $(0,2)+L$ based on what you've learned so far. If you drew the diagram correctly, it should sort of jump out immediately that these are distinct colattices. If it doesn't jump out, something is very wrong somewhere. Check your diagram! Now prove that these colattices are in fact distinct without using the diagram. (Sorry, we realize that the diagram makes the fact pretty obvious. And yet we must insist that you stick to the rigors of formal, diagram-less, more complicated looking proofs. We think they are cooler). Also, prove (again, formally) that L has no more colattices. Hence, conclude that* $\det L = 3$.

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

[Again, notice the bidirectionality. This is, we admit, a fairly hard problem—a leap from what you've done so far. You have been warned.]

Definition 3.3. The *divisor* of a lattice L is defined formally as the greatest positive integer $d = \operatorname{div} L$ with the property that for every $\vec{a} \in L$, $\vec{a}/d \in \mathbb{Z}^n$. In much simpler terms, the divisor of a lattice is the greatest positive integer by which you can divide all the elements of the lattice, such that the integer goes perfectly into the dividend without leaving a remainder, i.e. the quotient is still an n-tuple of integers. Consider, for instance, the lattice generated by $\{(2,4),(4,6)\}$. A little calculation will show you that this is simply the set of all ordered pairs of *even* integers (you can do the calculation by yourself now—you've learned enough about lattices). The divisor of this lattice is 2, because you can divide any element of the lattice by 2 and still get an ordered pair of integers, and also because 2 is the highest such positive integer (1 is the only other positive integer which can divide all the elements and still yield an integer ordered pair).

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

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 ∞). The notation $L_1 \supsetneq L_2$ simply means that there are two lattices L_1 and L_2, and that every element of L_2 is also in L_1,* and *there is at least one element of L_1 that is* not *in L_2.*

[Note the strict inequality, and don't ignore the possibility that they both can have an infinite determinant. We want formalism in everything. This is serious math right here.]

Definition 4.1. A lattice is said to be *finitely generated* iff it is equal to the lattice generated by a finite set S. For instance, the lattice generated by $\{(1,2,3),(4,5,6),(7,8,9)\}$ is finitely generated, as are all of the examples presented throughout this test.

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

[Read through all definitions again if you don't understand any term. Then *use* these definitions.]

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

[This is a generalization of the last problem, and draws upon one or more of the results derived earlier in the test. Once again, remember the rule that for solving this question, you can cite any result preceding this question *without* proof.]

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

This section (along with the last one) is going to be one of the two hardest sections on the test. It will be useful if you have seen some of this kind of mathematics before, but you can still solve the problems even if you never have, based on what you've learned so far in the test. It is always useful to keep going back and reading through all the definitions and whatever you have solved so far. The most important tool you have is an understanding of the basic fundamentals of the concepts; NOT your previous experience. If you have really understood what lattices are and how they work, this section is just another section in the test. But yes, the ideas here are much harder, and intuition might not work that well. But we think it's a good idea to give you a flavor of advanced mathematical ideas like isomorphisms at this stage, so that you know what you're up for should you choose to study math (and we hope you will!). We hope you understand the concept without getting intimidated from the start, and that you take something back with you from the PUMaC Power Round. Good luck!

Definition 5.1. One of our most ridiculous, insane-sounding definitions: isomorphism. As always, the formal version first. 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 $f(\vec{a}+\vec{b}) = f(\vec{a})+f(\vec{b})$]. [A map $f : X \to Y$ is a *bijection* if it gives a one-to-one correspondence between elements of X and elements of Y].

So essentially, if you want to check whether two lattices (both in, say, $\mathbb{Z}^n$) are isomorphic, you have to look for a bijective function f that takes ordered n-tuples to ordered n-tuples, and which *also* takes elements from L_1 to elements in L_2 bijectively. This function has to

be linear, i.e. it must deal with linear combinations of the elements of each n-tuple and not take their higher powers. It must, in other words, be of the form:

$$f(x_1, x_2, \ldots, x_n) = (a_{11}x_1 + a_{12}x_2 + \ldots + a_{1n}x_n, \ldots, a_{n1}x_1 + a_{n2}x_2 + \ldots + a_{nn}x_n) \quad (5.1)$$

The function f also has to be bijective, i.e. one-to-one as well as onto, BOTH from $\mathbb{Z}^n$ to $\mathbb{Z}^n$, AND from L_1 to L_2. Recall that a function $g : X \to Y$ is *one-to-one* when g does not ever take two distinct elements of X to the same element of Y, and is *onto* when every element in Y has at least one preimage in X. Mathematically, one-to-one means $g(a) = g(b) \implies a = b$, and onto means $\forall d \in Y$, $\exists c \in X$ such that $g(c) = d$. If it helps, remember that a bijective function always has an inverse function (which is also bijective).

If a bijective function f (a "bijection") exists between $\mathbb{Z}^n$ and $\mathbb{Z}^n$, so that f is also a bijection between L_1 and L_2, then we say that the lattices L_1 and L_2 are isomorphic. The bijection is then called an *isomorphism* from L_1 to L_2.

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 $\{(3, 0), (0, 1)\}$. If in doubt, feel free to work out the results just stated—they aren't too hard to work out.

Now, the problems.

Problem 5.1 (2pts)**.** *Prove that if two lattices are isomorphic then they have the same divisor.*

Problem 5.2 (2pts)**.** *Prove that if two lattices are isomorphic then they have the same determinant.*

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

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

Problem 5.5 (4pts)**.** *For any two integers* $d \geq 1$ *and* $D \geq 1$ *with* D *divisible by* d^2*, give an example of a lattice in* $\mathbb{Z}^2$ *with divisor* d *and determinant* D*. This is a "construction" problem; you have to construct a lattice that has the two properties we require.*

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).*

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.*

[The last two problems were pretty hard, so don't worry if you didn't get the solutions. If you did get the solutions, that's amazing, of course.]

6 Canonical Form (2 Problems; 13 Points)

The following theorem is true. The good news is, 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 integers $d_i \geq 0$ where d_i divides d_{i+1}. Furthermore, the sequence of integers $(d_1; \ldots; d_n)$ is isomorphism invariant; it is called the signature *of the lattice.*

Here $\vec{e}_i$ is the vector $(0, \ldots, 0, 1, 0, \ldots, 0)$ where the 1 appears in the ith entry.

What the theorem says is the following. Let's say you have a lattice L in dimension n. Now, you can always find n nonnegative (and not necessarily distinct) integers $d_1, d_2, \ldots, d_n$ such that d_i divides d_{i+1} for all i, with the property that the lattice L is isomorphic to the lattice generated by $\{d_i\vec{e}_i\}$, where the i runs from 1 to n. Here, note that $\vec{e}_i$ stands for the n-tuple which has 1 at the ith place and 0's everywhere else. So $\vec{e}_1, \vec{e}_2, \ldots, \vec{e}_n$ forms a basis for $\mathbb{Z}^n$. Since $\vec{e}_1 = (1, 0, 0, \ldots, 0)$, $\vec{e}_2 = (0, 1, 0, \ldots, 0)$, and so on, it is obvious that any n-tuple $(a_1, a_2, \ldots, a_n)$ of integers can be represented in terms of the basis elements as $a_1\vec{e}_1 + a_2\vec{e}_2 + \ldots + a_n\vec{e}_n = \sum a_i\vec{e}_i$.

Now, with the integers d_i, you can make the n-element long sequence $(d_1; d_2; \ldots; d_n)$, which is called the signature of the lattice L. The theorem just asserts that every lattice has a unique signature. It is easy to see that the signature is an isomorphism invariant, i.e. if L_1 and L_2 are isomorphic, then their signatures are the same.

An example should clarify things. Consider the bijection that takes an ordered pair (a, b) of integers to the ordered pair $(a, a + b)$. That this is a bijection isn't hard to prove at all, and you should be able to do it very easily. Now consider the lattice L generated by the set $\{(1, 1), (1, -1)\}$. This is isomorphic to the lattice generated by the bijection applied to the two elements of the generating set, i.e. the lattice L_2 generated by $\{(1, 2), (1, 0)\}$. This lattice L_2 can be shown in one step to be the same as the lattice generated by $\{(1, 0), (0, 2)\} = \{1(1, 0), 2(0, 1)\}$. So here, we have immediately obtained $d_1 = 1$ and $d_2 = 2$, and these satisfy all the requirements in the definition above. So, the signature of L (and L_2) is $(1; 2)$.

You may assume that the theorem above is true for any of your work on problems appearing after this point in the test. You're welcome.

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

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

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

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

7 Thanks

We hope you enjoyed taking the test as much as we did making it. If you're at this point, go out and buy yourself a sandwich. You've earned it.