# MATH 4400
# HOMEWORK 6
# COMMENTS AND SOLUTIONS

**Problem 1:** This exercise outlines a proof of Pick's theorem.

(a) Suppose $A$ and $B$ are two lattice polygons which share a side. Let $C$ be the lattice polygon obtained by "gluing" $A$ and $B$ together (so that the side they share vanishes). Show that if Pick's theorem holds for $A$ and $B$, it holds for $C$. Also show that if Pick's theorem holds for $A$ and $C$, it holds for $B$.

(b) Assuming, then, that every lattice polygon can be partitioned into lattice triangles (which is true and not hard to see), it suffices to prove the theorem for triangles. By drawing a rectangle around an arbitrary triangle, explain why it suffices to prove the theorem for right triangles whose legs are parallel to the coordinate axes, and rectangles whose sides are parallel to the coordinate axes.

(c) Complete the proof of the theorem.

**Solution:** (a) Let $b_A, b_B, b_C$ be the number of boundary points on $A, B, C$ respectively. Let $i_A, i_B, i_C$ be the number of interior points. Finally, let $s$ be the number of points on the side shared by $A$ and $B$. Then $b_C = (b_A - s) + (b_B - s) + 2$ and $i_C = i_A + i_B + (s - 2)$. The statement about boundary points is perhaps the more difficult one; we have thrown out the $s$ boundary points of $A$ and of $B$, but then we have to throw in the endpoints of the shared side, which continue to be boundary points of $C$–hence the 2 at the end.

So we get

$$\begin{aligned} i_C + b_C/2 - 1 &= i_A + i_B + (s-2) + \frac{b_A + b_B + 2 - 2s}{2} - 1 \\ &= i_A + i_B + \frac{b_A + b_B}{2} - 2 \\ &= \text{area}(A) + \text{area}(B) = \text{area}(C) \end{aligned}$$

by Pick's theorem applied to $A$ and $B$. Similar arithmetic shows that if Pick's theorem holds for $A$ and $C$, then it holds for $B$.

(b) I can't easily give you the picture in LaTeX, but suffice it to say that we draw a rectangle around a triangle. Then the rectangle is partitioned into several right triangles whose legs are parallel to the coordinate axes, plus the triangle in question. By part (a), then, it suffices to prove the theorem for the rectangle and the right triangles.

(c) Suppose the rectangle has length $a$ and width $b$. Then it has $2a + 2b$ boundary points and $(a-1)(b-1)$ interior points. Then Pick's theorem gives $(a-1)(b-1) + a + b - 1 = ab$ for the area, which is correct. As for the right triangle, it makes up half of a rectangle. The other half of the rectangle is another copy of the same right triangle. So if Pick's theorem is off by some number $c$ for the right triangle, it will be off by the same $c$ for the other copy, which will mean (by computations as in part (a)) that it will be off by $2c$ for the rectangle. So $c = 0$. (I trust you can fill in the details of my hand-waving here!) □

**Problem 2:** Prove the most general generalization of Minkowski's theorem: let $\mathbf{v}_1, \ldots, \mathbf{v}_n$ be linearly independent vectors in $\mathbb{R}^n$, and $L$ be the lattice consisting of all integer linear combinations of the $\mathbf{v}_i$, and $\Delta$ be the area of the fundamental parallelopiped of $L$. Then suppose $R$ is a convex centrally symmetric body of volume $> 2^n\Delta$. Then $R \cap L$ contains at least one point other than the origin.

**Solution:** This is just like the proof we gave in class. Consider the effect of translating a point in $R$, written say as $a_1\mathbf{v}_1 + \cdots + a_n\mathbf{v}_n$, with the $a_i$ real numbers, into the central parallelopiped given by

$$C = \{b_1\mathbf{v}_1 + \cdots + b_n\mathbf{v}_n \colon -1 < b_i \leq 1\}.$$

Of course $C$ has volume $2^n\Delta$. The translation is of course given by adding a point in $2L$ to our point; for every $p$ there is a unique point $q \in L$ such that $p - 2q \in C$. (Use the modified division algorithm and divide each $a_i$ by 2.)

Now, since the volume of $R$ is greater than that of the central parallelopiped, we must have two distinct points that get sent to the same point in $C$. So $p_0$ and $p_0 + 2q$ are both in $R$, for some $p_0 \in C$ and nonzero $q \in L$. Then $-p_0 \in R$ by symmetry, and then $q \in R$ by convexity applied to $-p_0$ and $p_0 + 2q$. $\square$

**Problem 3:** Let $\alpha$ be an irrational number. We say that $p/q$ is a *good rational approximation* to $\alpha$ if $\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^2}$. This exercise outlines a proof that every $\alpha$ has infinitely many good rational approximations.

(a) Show that for any real number $m > 1$ which is not an integer, there are integers $p, q$ not both 0 such that

$$|q\alpha - p| < \frac{1}{m}, \quad |q| < m.$$

(Hint: Use Minkowski's theorem! Maybe drawing a picture would help. Make sure you use the assumption that $m$ is not an integer.)

(b) Show that $p/q$ is a good rational approximation to $\alpha$. Explain why this implies that $\alpha$ has infinitely many good rational approximations.

**Solution:** (a) Consider the region given by the inequalities $|y\alpha - x| < \frac{1}{m}$, $|y| < m$. This region is a parallelogram whose area is $\frac{2}{m}(2m) = 4$. Since $m$ is not an integer, we can change the second inequality to $|y| < m_1$, where $m_1$ is, say, the average of $m$ and $\lceil m \rceil$. This gives us another parallelogram whose area is strictly greater than 4, but the new parallelogram and the old parallelogram contain the same lattice points (we can't have introduced any new ones because the $y$-coordinate is supposed to be an integer). The new parallelogram satisfies the hypotheses of (the original, non-generalized) Minkowski's theorem; hence it (and also the old parallelogram) contain a non-origin lattice point, which is exactly what we wanted.

By the way, notice that $q$ cannot be 0 unless $p$ is, which is impossible. We'll want this for part (b).

(b) Well,

$$\left|\frac{p}{q} - \alpha\right| = \frac{|p - q\alpha|}{|q|} < \frac{1}{m|q|} < \frac{1}{q^2}.$$

Why does this imply that $\alpha$ has infinitely many good rational approximations? Suppose it did not; then, by finiteness, there would be some (sufficiently large) integer $m$ such that

$\left|\frac{p}{q} - \alpha\right| \geq \frac{1}{m}$ for all good rational approximations $p/q$ (since $\alpha$ is irrational, so we can't get it exactly). But for this $m$, there is a nontrivial point in the region given in part (a), and hence another good rational approximation satisfying $\left|\frac{p}{q} - \alpha\right| < \frac{1}{m}$, which would be a contradiction. □

**Problem 4:** (taken from an old Putnam exam) Show that any convex lattice pentagon has area $\geq 5/2$. Also, show that this bound is sharp. (Hint for the first part: Pick's theorem!)

**Solution:** This is a cute application of the Pigeonhole Principle. Notice that there are four possibilities for the coordinates of any lattice point mod 2: $(0,0)$, $(0,1)$, $(1,0)$, and $(1,1)$. Since there are five vertices, there must be two that reduce to the same thing mod 2. Call these points $P, Q$. But then the midpoint $M$ of the line between them is also a lattice point! By convexity it is either an interior point or a boundary point.

Case 1: $M$ is an interior point. Then we are done by Pick's theorem, because $I \geq 1$ and $B \geq 5$.

Case 2: $M$ is a boundary point (the two vertices were adjacent). Well, in this case, we are done unless $P, Q$ was the only pair of vertices that agreed mod 2 (otherwise we can make one more boundary point out of another pair, and then $B \geq 7$ and we are done). This means that the other three vertices all have to be different mod 2, so there is one of each other type. Ah, but then consider $M$. If it reduces to the same thing as $P$ and $Q$ mod 2, then there are two more boundary points (the midpoints of $\overline{MP}$ and $\overline{MQ}$), so $B \geq 8$ and we are done instantly. If it doesn't, then it agrees with one of the other vertices mod 2, and the midpoint of the line from $M$ to that vertex must be an interior point, because it can't lie on the boundary. So then $I \geq 1$ and we are done.

Finally, note that the pentagon with vertices at $(0,0)$, $(0,1)$, $(1,2)$, $(2,1)$, and $(1,0)$ is convex and has area exactly $5/2$, so the bound is sharp. (By the way, it is in fact not difficult to show that there is always at least one interior point no matter what; we did not need this for our argument.) □

**Problem 5:** Define $s(k)$ to be the smallest positive integer such that $k$ can be written in the form

$$k = x_1^2 \pm \cdots \pm x_{s(k)}^2$$

for some positive integers $x_i$. (The $\pm$ signs are independent of each other.)

(a) Show that $s(k) \leq 2$ if $k$ is odd and $s(k) \leq 3$ if $k$ is even.

(b) Show that there are infinitely many $k$ such that $s(k) = 3$.

**Solution:** (a) We have that $2n+1 = (n+1)^2 - n^2$, and $2n = (n+1)^2 - n^2 - 1^2$.

(b) Suppose $k \equiv 6 \bmod 8$; then $k$ cannot be written as the sum or difference of two squares (because the squares mod 8 are $0, 1, 4$). Don't say I never give you short problems! □

**Problem 6:** (a) The *Three Squares Theorem* states that a positive integer $n$ can be written as the sum of three squares if and only if $n \neq 4^k(8a+7)$ for nonnegative integers $a, k$. Show the "only if" part of this theorem. (The "if" part is much harder.)

(b) Show that the Three Squares Theorem implies Lagrange's Four Squares Theorem (the one we proved in class).

**Solution:** (a) First note that $8a + 7$ cannot be the sum of three squares, by a mod-8 analysis. Now as for the rest, we'll argue by induction on $k$. So suppose that no integer of the form $4^k(8a + 7)$ can be written as a sum of three squares; the base case $k = 0$ was the first sentence of our solution. Then suppose that, for some $a$, $4^{k+1}(8a+7)$ can be written as $x^2 + y^2 + z^2$, for some $x, y, z$. Since $4^{k+1}(8a + 7)$ is 0 mod 4, it is immediate that $x, y, z$ are all even, by looking mod 4. But then we get

$$4^k(8a + 7) = (x/2)^2 + (y/2)^2 + (z/2)^2,$$

a representation of $4^k(8a + 7)$ as a sum of three integer squares. This is a contradiction. Hence the statement is true for $k + 1$, and then by induction the statement is true for all $k$.

(b) Let $n$ be a positive integer. The only troublesome case is when $n = 4^k(8a + 7)$, as otherwise it can be written as a sum of three squares (just add $0^2$ to get a sum of four squares). But then $n = 4^k(8a + 7) = 2^{2k} + 4^k(8a + 6)$, and $4^k(8a + 6)$ must be able to be written as a sum of three squares (in particular, it has an odd power of 2 in its prime factorization, and all the numbers that are not sums of three squares have even powers of two in their prime factorizations). So that does it. □

**Problem 7:** Here we will examine the problem of which integers can be written as sums of five positive squares.

Suppose $n$ cannot be written as a sum of five positive squares. Notice that

$$169 = 13^2 = 12^2 + 5^2 = 12^2 + 4^2 + 3^2 = 11^2 + 4^2 + 4^2 + 4^2 = 12^2 + 4^2 + 2^2 + 2^2 + 1^2.$$

Show that if $n$ cannot be written as the sum of five positive squares, then $n < 169$. (Hint: suppose not; then apply the Four Squares Theorem to $n - 169$.) Computer exercise: check all the numbers less than 169 to find the complete list of positive integers which cannot be written as a sum of five positive squares.

**Solution:** Certainly $n - 169$ can be written as a sum of either 0, 1, 2, 3, or 4 positive squares, because it can be written as a sum of four squares, some of which may be 0. But then we get a representation of $n$ as a sum of exactly five positive squares by adding the appropriate representation of 169 to $n - 169$. Let me illustrate with an example: if $n = 174$, then $n - 169 = 2^2 + 1^2$, a sum of two positive squares, so $n = 2^2 + 1^2 + (12^2 + 4^2 + 3^2)$. See what I mean?

All right, so the computer exercise. The laziest way to generate this list might simply be to generate the set

$$\{a_1^2 + \cdots + a_5^2 \colon 1 \le a_i \le 12\}$$

and see which integers less than 169 don't make it in. The list I get is

$$1, 2, 3, 4, 6, 7, 9, 10, 12, 15, 18, 33. \ \square$$

**Problem 8:** Now we move on to four positive squares. In what follows we will need to assume the Three Squares Theorem (see problem 6).

(a) First show that, for any positive integer $k$, we have that $8k$ is a sum of four positive squares if and only if $2k$ is.

(b) Show that if $n \equiv 2$, 3, 4, or 6 mod 8, and $n \ge 169$, then $n$ is a sum of four positive squares. (Hint: $n - 169$.)

(c) Suppose that $n \equiv 1$ or 5 mod 8. Show that if $n \geq 676$, then $n$ is a sum of four positive squares. (Hint: $n - 676$.)

(d) Suppose that $n \equiv 7$ mod 8. Show that $n$ is a sum of four positive squares. (Hint: if you apply the correct theorems, this should be no work at all.)

(e) Put it all together to obtain the following result: every positive integer is a sum of four positive squares except for $n = 1, 3, 5, 9, 11, 17, 29, 41$, and all integers of the form $2 \cdot 4^m$, $6 \cdot 4^m$, and $14 \cdot 4^m$ ($m \in \mathbb{Z}$, $m \geq 0$). (Of course this will require a bit of computer searching, much like Problem 7.)

**Solution:** (a) Clearly, if $2k$ is a sum of four positive squares, then so is $8k$; just multiply each of the four numbers by 2. On the other hand, if $8k$ is a sum of four positive squares, then the usual mod-8 analysis shows that each of these squares must be 0 or 4 mod 8; that is, they are even. So we can divide each of the four numbers by 2 to get a representation of $2k$.

(b) We have that $n - 169$ is congruent to 1, 2, 3, or 5 mod 8. So by the Three Squares Theorem, $n - 169$ is a sum of three squares, hence a sum of 0, 1, 2, or 3 positive squares. Using the same trick as in the previous problem, we add the appropriate representation of 169 to get $n$ as a sum of exactly four positive squares.

(c) We have that $n - 676$ is congruent to 1 or 5 mod 8. So by the Three Squares Theorem, $n - 676$ is a sum of three squares, hence a sum of 0, 1, 2, or 3 positive squares. Using the same trick as in the previous problem, we add the appropriate representation of 676 to get $n$ as a sum of exactly four positive squares. (Of course $676 = 4 \cdot 169$, so we can generate these appropriate representations by multiplying all the squared numbers by 2.)

(d) This should be clear: $n$ is a sum of four squares by the Four Squares Theorem, but by a mod-8 analysis, none of these squares can even be 0 mod 8 (indeed, the only possibility is $4 + 1 + 1 + 1$). So they're all positive squares.

(e) We restrict to classes mod 8. Parts (b), (c), and (d) imply that there are only finitely many integers not congruent to 0 mod 8 which cannot be written as a sum of four positive squares. In fact, we only have to search up to 676 to find them all. A similar computer search to the one we did before turns up the following exceptions:

$$1, 2, 3, 5, 6, 9, 11, 14, 17, 29.$$

(Remember, we were only looking for integers that were not divisible by 8.)

Now we finish by looking for exceptions that are divisible by 8. Well, part (a) implies that if we have an exception that is divisible by 8, we can divide it by 4 over and over again until we get an exception not divisible by 8 (which will, of course, be even). So any exception that is divisible by 8 will, upon repeated division by 4, end up being on the list above. But the only even integers in the above list are 2, 6, and 14. Part (a) also implies that *any* integer obtained from multiplying 2, 6, or 14 by 4 some number of times will be an exception. So the exceptions that are divisible by 8 are exactly the numbers of the form $2 \cdot 4^k$, $6 \cdot 4^k$, and $14 \cdot 4^k$ ($k \geq 1$). So the complete list is

$$1, 3, 5, 9, 11, 17, 29, 2 \cdot 4^k, 6 \cdot 4^k, 14 \cdot 4^k (k \geq 0). \ \square$$

**Problem 9:** For $k \geq 6$, show that the only positive integers that cannot be written as a sum of $k$ positive squares are

$$1, \ldots, k-1, k+1, k+2, k+4, k+5, k+7, k+10, k+13.$$

**Solution:** I apologize for the typo on the original problem set: the list there contained $k+3$, which is of course a sum of $k$ positive squares. Anyway, this is another good example of an induction proof where the base case is the hard part. Let's put the case $k = 6$ off until later.

First we show that none of the integers on the above list can be written as the sum of $k$ positive squares. Consider the smallest positive integers we *can* get in this way. The smallest is clearly $1^2 + \cdots + 1^2 = k$. How can we change this to get something else? We can change some of the 1's to bigger numbers. But realize that once we introduce a $4^2$, we're at least at $k+15$. Once we introduce two $3^2$'s, we're at least at $k+16$. Once we introduce five $2^2$'s, we're at least at $k+15$. So to get something less than $k+15$, we must have at most one $3^2$, and at most four $2^2$'s. There aren't too many possibilities left for numbers smaller than $k+15$: just

(1) no 2's, no 3's: $k$
(2) one 2, no 3's: $k+3$
(3) two 2's, no 3's: $k+6$
(4) three 2's, no 3's: $k+9$
(5) four 2's, no 3's: $k+12$
(6) no 2's, one 3: $k+8$
(7) one 2, one 3: $k+11$
(8) two 2's, one 3: $k+14$

So these are the only integers less than $k+15$ that we can get. The remaining integers are precisely the ones on the above list. Of course, we aren't done yet: we have to show that the list is complete and that there's not some integer bigger than $k+15$ that is an exception. We do this by induction. Again, the base case is left for last.

Now suppose we have proved the result for $k$. To see the result for $k+1$, what do we do? Well, suppose we have some positive integer $n$ which is not the sum of $k+1$ positive squares. Then certainly $n-1$ cannot be written as the sum of $k$ positive squares, because if it could then we could add $1^2$ to this representation. So then $n-1=0$ or $n-1$ is on the list

$$1, \ldots, k-1, k+1, k+2, k+4, k+5, k+7, k+10, k+13.$$

So $n$ is on the list

$$1, \ldots, (k+1)-1, (k+1)+1, (k+1)+2, (k+1)+4, (k+1)+5, (k+1)+7, (k+1)+10, (k+1)+13.$$

And we showed above that everything on this list cannot be written as a sum of $k+1$ positive squares, so this concludes the inductive step.

Finally, the base case: we want to show that the only integers that are not a sum of six positive squares are

$$1, 2, 3, 4, 5, 7, 8, 10, 11, 13, 16, 19.$$

(Of course we have already shown that every integer on this list is an exception, so we just need to show that these are the only ones.) Well, looking at $n-1$ and using the same argument as in the inductive step, we see that if $n$ is not a sum of six positive squares, then

$n-1=0$ or $n-1$ has to be in the list of exceptions to five positive squares that we generated in Problem 7. So $n$ is one of

$$1, 2, 3, 4, 5, 7, 8, 10, 11, 13, 16, 19, 34.$$

(See the solution to Problem 7!) But, thankfully, $34 = 2^2 + 2^2 + 2^2 + 2^2 + 3^2 + 3^2$.

I guess the way to think about this result is that weird things happen for $k \leq 5$, but after $k = 6$, the behavior stabilizes, and the only way for something not to be a sum of six positive squares is that it's just too small and most of the squares have to be 1. $\square$