

# Math 117b - Homework 4

**Instructor:** Andrés Eduardo Caicedo

**Due:** February 1, 2007 at 1:00 pm.

This Homework is due either during lecture or in the course box outside 253 Sloan by Thursday February 1<sup>st</sup> at 1:00 pm. Refer to the grading policy for additional requirements.

1. The purpose of this exercise is to give a proof of Lagrange's four square theorem from 1770: Every natural number is the sum of four squares. (Check that 3 squares do not suffice in general.)

I will follow the presentation in Niven, Zuckerman and Montgomery, **An introduction to the theory of numbers**, John Wiley, 5<sup>th</sup> edition (1991), which uses a small amount of machinery from geometry of numbers. More elementary proofs are possible; Matiyasevich's book on the 10<sup>th</sup> problem contains one such proof in its appendix.

- (a) **(Blichfeldt's principle)** Let  $X \subseteq \mathbb{R}^n$  be a set with volume  $\lambda(X) > 1$ . Complete the sketch below to show that there are 2 points  $\vec{s}, \vec{s}'$  in  $X$  such that  $\vec{s} - \vec{s}'$  has integral coordinates:

All the sets discussed below are measurable, i.e., their  $n$ -dimensional volume is defined. You may assume this fact. Use that volume is *countably additive* (i.e., if a (measurable) set  $A$  is union of countably many disjoint sets  $B_i$ , then  $\lambda(A) = \sum_i \lambda(B_i)$ ) to show that it suffices to consider the case when  $X$  is bounded, say  $X$  is contained in the disk  $|\vec{x}| \leq R$  for some  $R$ .

For  $\vec{x} \in \mathbb{R}^n$  let  $C_{\vec{x}}$  be the unit cube with vertex  $\vec{x}$  defined by

$$C_{\vec{x}} = \{\vec{y} : x_i \leq y_i < x_i + 1 \text{ for } i = 1, \dots, n\},$$

where  $\vec{x} = (x_1, \dots, x_n)$ , etc. Let  $X_{\vec{x}} = X \cap C_{\vec{x}}$  and let  $X(\vec{x}) = -\vec{x} + X_{\vec{x}}$  (so  $X(\vec{x})$  is a translate of  $X_{\vec{x}}$  and  $X(\vec{x}) \subseteq C_{\vec{0}}$ ).

Considering points  $\vec{x}$  with integer coordinates, argue that there must be at least 2 of them  $\vec{x}$  and  $\vec{x}'$  such that  $X(\vec{x}) \cap X(\vec{x}') \neq \emptyset$ , and conclude the result.

- (b) **(Minkowski's convex body theorem)** Let  $C \subseteq \mathbb{R}^n$  be convex. This means that if  $\vec{x}, \vec{y} \in C$  then all points in the segment between  $\vec{x}$  and  $\vec{y}$  also lie in  $C$ ; these points all have the form  $s\vec{x} + (1-s)\vec{y}$

for some  $s \in [0, 1]$ . Also assume that  $C$  is symmetric about  $\vec{0}$  (i.e., if  $\vec{x} \in C$ , then  $-\vec{x} \in C$ ) and has volume  $\lambda(C) > 2^n$ . Show that there is a point  $\vec{x} \neq \vec{0}$ ,  $\vec{x} \in C$ , all of whose coordinates are integers.

For this, let  $X = \frac{1}{2}C$  and apply Blichfeldt's principle.

- (c) Here we show a version of Minkowski's theorem for lattices. A *lattice* is a set of the form  $\Lambda = AZ^n$  where  $A$  is an invertible  $n \times n$  matrix with real entries and

$$AZ^n = \{A\vec{x} : \vec{x} \in \mathbb{Z}^n\}.$$

You will need the fact that the absolute value of the determinant of  $A$  is the volume of the parallelepiped determined by the columns  $\vec{a}_1, \dots, \vec{a}_n$  of  $A$ . This is the image of the unit  $n$ -cube under the linear transformation  $A$ , and therefore  $\lambda(A\vec{x}) = \lambda(\vec{x})|\det A|$  for any  $\vec{x}$ . Let  $A$  be such a matrix and  $\Lambda = AZ^n$ . Let  $C \subseteq \mathbb{R}^n$  be convex, symmetric about  $0$ , and of volume  $\lambda(C) > 2^n|\det A|$ . Show that there is  $\vec{x} \in \Lambda$ ,  $\vec{x} \neq \vec{0}$ , such that  $\vec{x} \in C$ .

You will also need that the volume of the disk in  $\mathbb{R}^4$  of radius  $r$ ,

$$\{\vec{x} : x_1^2 + \dots + x_4^2 < r^2\},$$

is  $\frac{1}{2}\pi^2 r^4$ . You can assume this fact.

- (d)  $\mathbb{R}^4$  admits a multiplicative structure that turns it into a division algebra, the *quaternions*. It is given by

$$\begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} \otimes \begin{pmatrix} y_1 \\ y_2 \\ y_3 \\ y_4 \end{pmatrix} = \begin{pmatrix} x_1 y_1 - x_2 y_2 - x_3 y_3 - x_4 y_4 \\ x_1 y_2 + x_2 y_1 + x_3 y_4 + x_4 y_3 \\ x_1 y_3 - x_2 y_4 + x_3 y_1 + x_4 y_2 \\ x_1 y_4 + x_2 y_3 - x_3 y_2 + x_4 y_1 \end{pmatrix}.$$

With  $|\vec{x}| = (x_1^2 + x_2^2 + x_3^2 + x_4^2)^{1/2}$  as usual, verify that this product satisfies

$$|\vec{x} \otimes \vec{y}| = |\vec{x}||\vec{y}|.$$

Conclude that to prove Lagrange's theorem it suffices to show that every odd prime is sum of four squares.

Fix an odd prime  $p$ .

- (e) Show that there are integers  $r, s$  such that  $r^2 + s^2 + 1 \equiv 0 \pmod{p}$ . For this, let  $\mathcal{A} = \{1 + x^2 : x = 0, 1, \dots, (p-1)/2\}$  and  $\mathcal{B} = \{-y^2 : y = 0, 1, \dots, (p-1)/2\}$ , show that the elements of  $\mathcal{A}$  are pairwise non-equivalent mod  $p$ , and the same holds for  $\mathcal{B}$ .

(f) With  $r, s$  as above let

$$A = \begin{bmatrix} p & 0 & r & s \\ 0 & p & s & -r \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}.$$

Show that  $A$  is invertible by computing  $\det(A)$  and let  $\Lambda = AZ^4$ .

Suppose that  $\vec{t} \in \mathbb{Z}^4$  and let  $\vec{x} = A\vec{t}$ . Show that  $|\vec{x}|^2 \equiv 0 \pmod{p}$ .

(g) Let  $C$  be the disk in  $\mathbb{R}^4$  of radius  $\sqrt{2p}$ . Conclude that there is a point  $\vec{x} \in \Lambda \cap C$ ,  $\vec{x} \neq \vec{0}$  and show that  $|\vec{x}|^2 = p$ , proving Lagrange's theorem.

2. Show that there is a recursive enumeration of all polynomials with integer coefficients in finitely many variables. Using this enumeration, we can list all such polynomials as  $p_0, p_1, \dots$ . Let

$$A = \{n : p_n(\vec{x}) = 0 \text{ has a solution in the integers}\}$$

and let

$$B = \{n : p_n(\vec{x}) = 0 \text{ has a solution in the natural numbers}\}.$$

Show that  $A \equiv_T B$  as follows: There is a recursive procedure that to each polynomial  $p$  assigns a polynomial  $p^*$  such that if  $p = p_n$  and  $p^* = p_m$  then  $n \in A$  iff  $m \in B$  (and  $m$  can be recursively computed from  $n$ ). We say the procedure *reduces*  $A$  to  $B$ . Show that there is also such a procedure reducing  $B$  to  $A$ . Conclude that  $A$  and  $B$  have the same degree.

3. Without using that exponentiation is Diophantine, show that if

$$\{(a, b) \in \mathbb{N}^2 : \exists n (a = b^n)\}$$

is Diophantine *then* so is exponentiation:

$$\{(a, b, c) \in \mathbb{N}^3 : a = b^c\}.$$