Research Methods in Mathematics
Extended assignment 1

T. PERUTZ

Due: at the beginning of class, October 5.

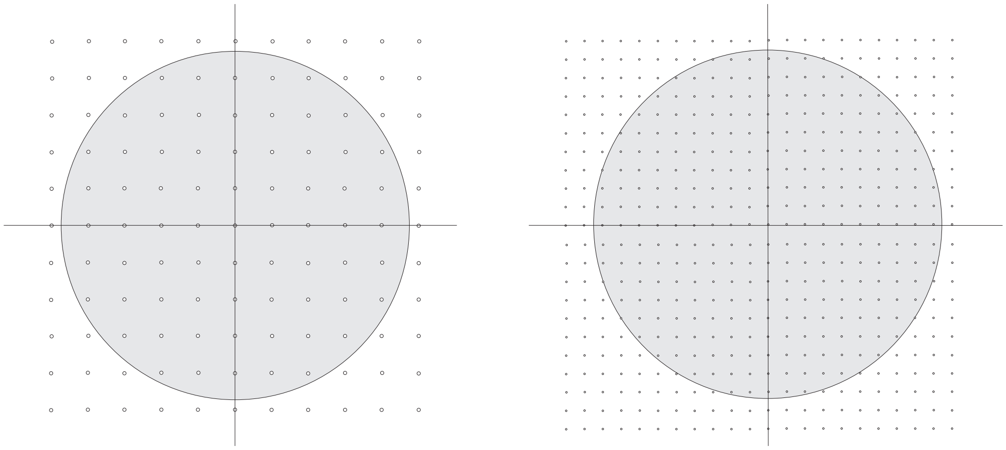
Choose one of the following assignments:

(1) The circle problem
(2) Complete ordered fields

1 The circle problem

The circle problem is this: how many lattice points are there inside or on a circle of radius R centered at the origin?

(A *lattice point* is a point (m,n) in the plane whose coordinates m and n are integers.)



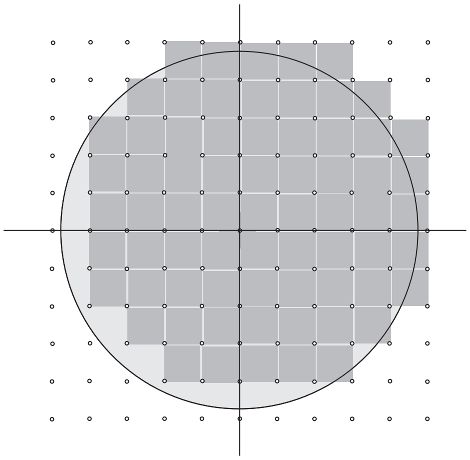
Formally, we define $N(R)$ to be the number of ordered pairs (m,n) where m and n are integers and $m^2+n^2 \leq r^2$.

(1) *Exact formula.* Prove that

$$N(R) = 1 + 4\lfloor R \rfloor + 4 \sum_{j=1}^{\lfloor R \rfloor} \lfloor \sqrt{R^2 - j^2} \rfloor.$$

Here $\lfloor x \rfloor$ denotes the greatest integer less than or equal to x (for instance, $\lfloor 3.9 \rfloor = 3$).
[*Hint.* Start by counting the points on the axes.]
Comment: Using the exact formula, we can ask a computer to calculate $N(R)$ for any R that isn't too huge. However, this isn't very satisfying. The formula is too messy to give a sense of the pattern *that $N(R)$ follows. It doesn't give us* qualitative *information about $N(R)$. For this, a tidy but approximate formula would be more useful. In the next steps we'll develop such a formula.*

(2) For each lattice point $P=(m,n)$, let S_P be the unit square with P as its bottom-left corner. The union of all the S_P, where P runs over all lattice points (m,n) with $m^2+n^2 \leq R^2$, is a shape we'll call $S(R)$. In the picture below, $S(R)$ is shaded dark gray.
Explain why $N(R)$ is equal to the area of $S(R)$.



(3) I claim that an approximation to $N(R)$, for R large, is given by

$$N(R) \approx \pi R^2.$$

Explain why this is so. Explain two reasons why this formula is not exactly correct.

(4) By drawing circles entirely containing $S(R)$ and entirely contained in $S(R)$, prove that

$$\pi(R - \sqrt{2})^2 < N(R) < \pi(R + \sqrt{2})^2$$

for all $R \geq \sqrt{2}$.

(5) Show that

$$\lim_{R\to\infty} \frac{N(R)}{\pi R^2} = 1.$$

(6) We can get a slightly sharper upper bound for $N(R)$ by observing that $S(R)$ is contained in the union of four 45° pie-slices, one in each quadrant, of different radii. Use this method to prove that

$$N(R) < \pi \left[R^2 + (1 + \frac{1}{\sqrt{2}})R + \frac{3}{2} \right].$$

Find a similar lower bound for $N(R)$.

Comment: the bounds we have obtained were discovered by Gauss around 1800. Much sharper bounds have since been discovered. It is conjectured that for any $\epsilon > 0$ there is a constant $C > 0$ such that $|N(R) - \pi R^2| \leq CR^{\frac{1}{2}+\epsilon}$ for large enough R. It's a theorem of Hardy and Landau (1915) that there does not *exist a constant C such that $|N(R) - \pi R^2| \leq CR^{\frac{1}{2}}$ for large enough R.*

(7) *Extra credit.* Let $r(n)$ denote the number of pairs (x,y) where x and y are integers such that $x^2+y^2=n$. For instance, $r(5)=8$, the eight possible pairs (x,y) being $(\pm 1,\pm 2)$ (four possibilities) and $(\pm 2,\pm 1)$ (four more). Prove that

$$N(R)=\sum_{n=0}^{\lfloor R^2\rfloor} r(n).$$

Now let $A(m)$ denote the average value of $r(n)$ as n runs from 0 to m, that is, $A(m)=\frac{1}{m+1}\sum_{n=0} mr(n)$. Deduce that $A(m)\to\pi$ as $m\to\infty$. (In words: the average number of ways a number in which can be represented as a sum of two squares is π.)

2 Complete ordered fields

There are several ways to give a rigorous definition of the system of real numbers. The most familiar is to define a real as a possibly-infinite decimal string, but there are other methods (notably, via Dedekind cuts or via Cauchy sequences).

One might wonder whether these different methods give equivalent results. The answer is that they do. It turns out that the only important thing is that the real numbers form a *complete ordered field.* In this assignment, we will see that complete ordered fields have familiar properties. At the end, we will find that there is essentially only one complete ordered field.

Reference for this assignment: Spivak, Chapter 30.

A: Fields

Definition 2.1 A *field* F is a system of numbers in which one can add and multiply, and in which these operations satisfy certain axioms. The axioms are as follows:

- $(x+y)+z = x+(y+z)$ for all x, y, z in F.
- $x+y = y+x$ for all x, y in F.
- There is an element 0 so that $x+0 = x$ for all x.
- For any x there is an element $-x$ so that $x+(-x) = 0$.
- $x(yz) = x(yz)$ for all x, y, z.
- $xy = yx$ for all x, y.
- There is an element 1 so that $1x = x$ for all x.
- For any $x \neq 0$ there is an element x^{-1} so that $xx^{-1} = 1$.
- $x(y+z) = xy+xz$ for all x, y, z.

(1) Explain why the rationals $\mathbb{Q}$ form a field.

B. Ordered fields.

Definition 2.2 An *ordered field* is a field in which one has a notion of positivity: There is a given subset P of elements x in the field which are considered positive. We write $x > 0$ if x lies in P. The subset P must have the following properties:

- For any x, one and only one of the following three things holds: $x > 0$; $x = 0$; $-x > 0$.
- If $x > 0$ and $y > 0$ then $x+y > 0$.

- If $x > 0$ and $y > 0$ then $xy > 0$.

(1) Referring to your class notes, explain why the rationals $\mathbb{Q}$ are an ordered field.

(2) Show that in an ordered field, there can be no number i such that $i^2 = -1$. [*Hint.* Consider the possibilities: $i > 0$, $i = 0$, $i < 0$.]

(3) Show that in an ordered field, if x is an element of the field and n a natural number such that

$$\overbrace{x + x + \cdots + x}^{n} = 0$$

then $x = 0$.

(4) Let F be an ordered field. Find a mapping (that is, a function) $i \colon \mathbb{Q} \to F$ such that $i(x+y) = i(x) + i(y)$ and $i(xy) = i(x)i(y)$ for all x, y in $\mathbb{Q}$. Show that there is only one such mapping. [*Hint.* Start by defining $i(1)$. Then consider $i(2)$...]

(5) In an ordered field, one can speak of upper bounds and least upper bounds. Referring to your notes, define an *upper bound* for a subset S of an ordered field F. Also define a *least upper bound* for S and explain why S has at most one least upper bound.

C. Complete ordered fields.

Definition 2.3 An ordered field F is called *complete* if it has the following property: If S is any non-empty subset of F that that has an upper bound, then S has a (necessarily unique) *least* upper bound, denoted $\sup S$.

Let F be a complete ordered field.

(1) Show for any positive element x in F, there is some natural number n such that $i(n) - x > 0$. (So there are no 'infinite' elements in F.)
[*Hint*: if not, consider a least upper bound for $\{i(n)\}$ as n ranges over the natural numbers.]

(2) Deduce from the previous part that for any positive element y in F, there is some natural number n such that $y - i(\frac{1}{n}) > 0$. (So there are no 'infinitesimal' elements in F.)

(3) Show that one has

$$0 = \sup\{i(y) : \ y \in \mathbb{Q}, \ -i(y) > 0\}.$$

Show that more generally, for any x in F, one has $x = \sup S_x$, where

$$S_x = \{i(y) : \ y \in \mathbb{Q}, \ x - i(y) > 0\}.$$

(4) Suppose that F_1 and F_2 are complete ordered fields. Show that there is a mapping $I\colon F_1 \to F_2$ such that (a) $I(x+y) = I(x) + I(y)$ for all x, y in F_1; (b) $I(xy) = I(x)I(y)$ for all x, y in F_1; and (c) if $x > 0$ in F_1 then $I(x) > 0$ in F_2. [*Hint*: begin by defining $F(i(x))$ for x rational. Then think what F ought to do to least upper bounds.]

(5) *Extra credit.* Show that there is only one mapping I as in the last part. Show that I is one-to-one and onto. (That is, every x' in F_2 can be expressed as $I(x)$ for a unique x in F_1.)
Comment: We conclude from the last two parts that any two complete ordered fields are essentially the same.