Number theory exercises WS 2019, TU Graz

Sheet 3, solutions (on paper) to be handed in on 19th November 2019

3-1. a) Let p be a prime of the form $p = 4k + 1$. Define an involution on $\mathbb{Z}_p^* = \{1, 2, \ldots, p-1\}$ which shows that there is some element $y \in \mathbb{Z}/p\mathbb{Z}$ of order 2, and also prove that there is some $x \in \mathbb{Z}/p\mathbb{Z}$ with $x^2 \equiv -1 \bmod p$.

b) Theorem (Fermat-Girard-Euler): A prime $p \equiv 1 \bmod 4$ is a sum of two squares. Work through the following sketch proof, and draw the corresponding $p \times p$ lattices L_z, on graph paper if possible, e.g. http://www.printfreegraphpaper.com , when $p = 13$ and $p = 17$.

The involution on the finite set $S = \{2 \le a \le \frac{p-1}{2}\}$ defined by

$$a \mapsto \begin{cases} a^{-1} \bmod p & \text{if } 2 \le (a^{-1} \bmod p) \le \frac{p-1}{2}, \\ -a^{-1} \bmod p & \text{otherwise,} \end{cases}$$

has at least one fixed point z, so the fundamental domain of the lattice defined by

$$L_z = \{(x,\ zx \bmod p), 0 \le x < p\}$$

is a square with area p, so that the two squares theorem follows by an application of Pythagoras' theorem. □

3-2. A beautiful example of the power of an involution is here: Don Zagier: A one-sentence proof that every prime $p \equiv 1 \bmod 4$ is a sum of two squares (Amer. Math. Monthly 97 (1990), p. 144).
http://people.mpim-bonn.mpg.de/zagier/files/doi/10.2307/2323918/fulltext.pdf

"The involution on the finite set $S = \{(x, y, z) \in \mathbb{N}^3 : x^2 + 4yz = p\}$ defined by

$$(x, y, z) \mapsto \begin{cases} (x + 2z, z, y - x - z) & \text{if } x < y - z \\ (2y - x, y, x - y + z) & \text{if } y - z < x < 2y \\ (x - 2y, x - y + z, y) & \text{if } x > 2y \end{cases}$$

has exactly one fixed point, so $|S|$ is odd and the involution defined by $(x, y, z) \to (x, z, y)$ also has a fixed point. □"

Work through it and make sure that you understand all(!) details of the proof. In particular verify the implicitly made claims that the maps are well defined and are involutions.

Think about: what are the respective advantages and disadvantages of the two proofs of the two squares theorem?

((Now try the opposite. Where does Zagier's map come from? Let $p \equiv 1 \bmod 4$ be a prime and let $S = \{(x, y, z) \in \mathbb{Z}^3 : x^2 + 4yz = p\}$. Find involutions on S. (Hint: assume these involutions are essentially linear maps. Well, it's tedious but it can be done.))

3-3. Apply Minkowksi's theorem to prove the two squares theorem.

3-4. A proof based on the fact that $\mathbb{Z}[i]$ is a Euclidean ring.
`https://artofproblemsolving.com/wiki/index.php/Fermat's_Two_Squares_Theorem`

3-5. If $m = x_1^2 + x_2^2 + x_3^2 + x_4^2$ and $n = y_1^2 + y_2^2 + y_3^2 + y_4^2$, show that $mn = z_1^2 + z_2^2 + z_3^2 + z_4^2$, where z_i is linear in the variables x_i, y_i, with coefficients ± 1. and the coefficients only need ± 1. (It may help to recall the multiplication of quaternions.) Try to find all (essentially different) sign patterns).

3-6. Give details of the proof of the formula for the volume of the four dimensional spehere of radius r.

3-7. Work through the proof of the four-squares theorem in Hardy-Wright.

3-8. We studied in detail the set of all intgers which are of the form $n = x^2 + y^2$. Now, do the same for $n = x^2 + 2y^2$. Give a classification (with proof) of the primes of this form, and then examine (in terms of the prime factors of n) which integers n are of this form.

Hand in solutions to problems 3.1, 3.2, 3.3., 3.5, 3.6, 3.8

Deadline for crosses are: Tuesday 9.55am.

`https://www.math.tugraz.at/~elsholtz/WWW/lectures/ws19/numbertheory/vorlesung.html`