MATH 3320, HOMEWORK #13

DUE WEDNESDAY, NOVEMBER 28

To ensure that you get full credit, be sure to *show your work* in the problems that require calculations. Very little credit is given for answers without justification. Please write in complete sentences to help us understand what you are doing.

You may collaborate with classmates in solving the problems, including the extra credit problems. If you do so, please list their names on your assignment. However, you should not consult *any* other people (except the instructors or TAs), or use online resources. (Seriously, it's very obvious to us when this occurs, and there are drastic consequences, so don't do it!) If you use results that were not proved in class, please provide your own proof.

For some problems here, you may need to use a computer to do them in a reasonable amount of time.

1. Lagrange proved that if $p = 4k+1$ is a prime, then we have the continued fraction expansion $\sqrt{p} = \langle a_0, \overline{a_1, \dots, a_m, a_m \dots a_1, 2a_0}\rangle$. He showed that if you write $\alpha_{m+1} = \frac{R_{m+1}+\sqrt{p}}{S_{m+1}}$, then $R_{m+1}^2 + S_{m+1}^2 = p$.

(a) (5 points) Use this method to find a solution to $x^2 + y^2 = 73$.

(b) (10 points) The numbers $(2177, 528)$ satisfy $2177^2 - 17 \cdot 528^2 = 1$. Use Lagrange's method to find a solution to $x^2 - 17 \cdot y^2 = -1$.

Lagrange's Method: Write $2177 = 2t+1$ and $528 = 2r = 2 \cdot 264 = 2 \cdot (8 \cdot 3 \cdot 11)$. Factor $t = 17 \cdot 64 = 17 \cdot 8^2$ and compare with $t+1 = 11^2 \cdot 3^2$. A solution $a^2 - 17b^2 = \pm 1$ with smaller values than $(2177, 528)$ can be extracted from this. If you get -1 you have found a solution. If not, repeat the process with the smaller (a, b).

(c) (5 points) Is $(2177, 528)$ the *smallest* solution to $x^2 - 17y^2 = 1$? Use continued fractions. How would you use the answer (and method) from part (b) to find smaller solutions to $x^2 - 17y^2 = \pm 1$?

2. Jacobsthal found the following method to give a solution to $x^2 + y^2 = p$. Let $S_+ = \sum \left(\frac{y^3 - y}{p}\right)$, and $S_- = \sum \left(\frac{y^3 - \epsilon y}{p}\right)$, where ϵ is any residue which is not a square (and $(\ )$ is the Legendre symbol). Both numbers are even. He then showed that $(\frac{1}{2}|S_+|)^2 + (\frac{1}{2}|S_-|)^2 = p$.

(a) (5 points) Use this method to find a solution to $x^2 + y^2 = 73$. (Compute the sums directly using a computer.)

(b) (5 points) Show that $S_\pm$ must be even.

(c) (10 points) Show that the absolute values $\left|S(a) = \sum \left(\frac{y^3 - ay}{p}\right)\right|$ only depend on whether $a \pmod p$ is a square $\pmod p$ or not.

3. A quadratic form $ax^2 + bxy + cy^2$ is said to be *reduced*, if either $-a < b \le a < c$ or $0 \le b \le a = c$. The discriminant $\Delta = b^2 - 4ac$.

(a) (5 points) Let $d \in \mathbf{Z}$. Show that $d \equiv 0, 1 \pmod 4$ if and only if we can write $d = b^2 - 4ac$ for some $a, b, c \in \mathbf{Z}$.

(b) (5 points) Show that if $\Delta = -4$, then there is only one reduced form.

(c) (5 points) Show that if $\Delta = -8$ then there is again only one reduced form.

(d) (5 points) Find two distinct reduced forms of discriminant -24.

4.

(a) (10 points) Show that an integer n is properly represented by some binary quadratic form $ax^2 + bxy + cy^2$ of discriminant Δ, if and only if Δ is a square modulo $4n$. Precisely, show that there are integers p, q satisfying $gcd(x, y) = 1$ and $ap^2 + bpq + cq^2 = n$, if and only if $\Delta = b^2 - 4ac$ is a square modulo $4n$. (Hint: Use congruences to show that the condition is necessary. For the sufficient condition, choose b using the congruence condition, and then a c such that the form $nx^2 + bxy + c$ has the given discriminant.)

(b) (10 points) Use part (a) to show that a prime p can be represented as $p = x^2 + y^2$ if and only if $p \equiv 1 \pmod 4$. (Hint: Use the fact that there is only one equivalence class of positive definite quadratic forms with discriminant -4.)

5. (10 points) How many solutions does $x^2 + y^2 = 154468 = 4 \cdot 73 \cdot 23^2$ have? Give the number and a description how to obtain them without listing all.

6. (Extra Credit) The following short proof was given by Zagier (1990) in his note "A one-sentence proof that every prime $p \equiv 1 \pmod 4$ is a sum of two squares,"[1]

> The involution on the finite set $S = \{(x, y, z) \in \mathbf{N}^3 : x^2 + 4yz = p\}$ defined by
>
> $$x \mapsto \begin{cases} (x + 2z, z, y - x - z), & \text{if } x < y - z \\ (2y - x, y, x - y + z), & \text{if } y - z < x < 2y \\ (x - 2y, x - y + z, y), & \text{if } x > 2y \end{cases}$$
>
> has exactly one fixed point, so $|S|$ is odd and the involution defined by $(x, y, z) \mapsto (x, z, y)$ also has a fixed point.

For (10 points), supply all the missing details of the proof. In particular, address (a) why the map $f : S \to S$ given above is well-defined and is an *involution* (i.e. a function that is its own inverse), (b) why the number of fixed points of an involution $S \to S$ has the same parity as $|S|$, and (c) how the assumption that $p \equiv 1 \pmod 4$ is used.

[1] `https://people.mpim-bonn.mpg.de/zagier/files/doi/10.2307/2323918/fulltext.pdf`