Math 573 Problem Set 6

1. Consider the projection from the unit sphere $S^2\backslash\{(0,0,1)\}$ to the xy-plane discussed in class.

(a) Establish that the projection is a bijection between $S^2\backslash\{(0,0,1)\}$ and the xy-plane by explicitly writing down the formulas that give the projection and it's inverse and checking they are inverse maps.

(b) Given a line ℓ_1 in the plane, determine the equation under mapping to the sphere. Show that the limit as x goes to $\pm\infty$ in the xy-plane maps to the north pole on the unit sphere for the line.

(c) Let ℓ_1 and ℓ_2 be two parallel lines in the xy-plane. Conclude that two parallel lines intersect when mapped to the unit sphere.

2. Let p and q be odd primes. Is it possible that a is a quadratic nonresidue modulo p and q but there is a solution to the equation $x^2 \equiv a(\operatorname{mod} pq)$? If so, find an example. If not, prove it can never happen.

3. Prove that 2 is not a primitive root of any prime of the form $p = 3\cdot 2^n + 1$ unless $p = 13$. (Hint: Think quadratic residues here!)

4. Prove that the quadratic residues modulo p ($p =$ odd prime) are congruent to $1^2, 2^2, 3^2, \ldots, ((p-1)/2)^2$. Prove that is $p > 3$ then the sum of the quadratic residues is divisible by p.

5. Prove that $\left(\frac{6}{p}\right) = 1$ if and only if $p \equiv 1, 5, 19, 23(\operatorname{mod} 24)$.

6. Compute $\left(\frac{3658}{12703}\right)$ by hand.

7. Let p be an odd prime. Show that the equation

$$x^2 + py + a = 0$$

with $\gcd(a,p) = 1$ has an integral solution if and only if $\left(\frac{-a}{p}\right) = 1$.

8. Determine all singular points of the curve $f(x,y) = 0$ where $f(x,y) = y(x^3 - 3x)$.

9. Let $P = (x_0, y_0)$ be a point on the elliptic curve E_N. Derive a formula for $P \oplus P$ in terms of x_0 and y_0.

10. (a) Let $X, Y, Z \in \mathbb{Q}$ be such that $X^2 + Y^2 = Z^2$, i.e., (X, Y, Z) is a Pythagorean triple. Prove that one obtains from this a Pythagorean triple $(x, y, z) \in \mathbb{Z}^3$ so that $\gcd(x, y, z) = 1$.

(b) Prove that if $(x, y, z) \in \mathbb{Z}^3$ is a Pythagorean triple with $\gcd(x, y, z) = 1$, then z must be odd.

(c) Prove that if 1 is a congruent number then the equation $u^4 - v^4 = w^2$ would have an integer solution with w odd.

(d) Prove that if there is no nontrivial integer solution to the equation in part (c), then there is no nontrivial integer solution to the equation $a^4 + b^4 = c^4$, Fermat's last theorem for exponent 4. (This should convince you it is hard to show 1 is not a congruent number. In fact 1 is not a congruent number, but showing that the equation in part (c) does not have a solution requires proof by descent, which would require some more work. A paper about Fermat's theory of proof by descent may be a good idea though!)