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.

One needs to derive the formulas. To do this one uses parametric equations. For instance, to find where the point $(x_0, y_0, z_0) \in S^2\backslash\{(0,0,1)\}$ maps one uses that the line connecting $(0,0,1)$ and (x_0,y_0,z_0) is given by $x = x_0 t, y = y_0 t, z = (z_0 - 1)t$. The projected point is when $z = 0$, and so it is given by $(x, y) = \left(\frac{x_0}{1-z_0}, \frac{y_0}{1-z_0}\right)$. Thus, the equation for the projection is

$$f(x_0, y_0, z_0) = \left(\frac{x_0}{1-z_0}, \frac{y_0}{1-z_0}\right).$$

The same type of argument with a line between (x_0, y_0) and $(0,0,1)$ gives the inverse map

$$g(x_0, y_0) = \left(\frac{2x_0}{1+x_0^2+y_0^2}, \frac{2y_0}{1+x_0^2+y_0^2}, \frac{-1+x_0^2+y_0^2}{1+x_0^2+y_0^2}\right).$$

It is not just a matter of checking that $g \circ f(x_0, y_0, z_0) = (x_0, y_0, z_0)$, which is an easy (if messy) calculation.

(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.

A line in the plane is given by the set of points $\{(x, mx + b)\}$ for some fixed $m, b \in \mathbb{R}$. These points map to the set

$$\left\{\left(\frac{2x}{1+x^2+(mx+b)^2}, \frac{2(mx+b)}{1+x^2+(mx+b)^2}, \frac{-1+x^2+(mx+b)^2}{1+x^2+(mx+b)^2} : x \in \mathbb{R}\right)\right\}.$$

Now we want to see what happens to these points as $x \to \pm\infty$.. It is clear that the x and y coordinates go to zero as the bottom term is a polynomial of degree 2 and the top has degree 1. The z-coordinate goes to 1 as the numerator and denominator are each polynomials of degree two with leading coefficient $(m^2 + 1)$.

(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.

When considered on the unit sphere, they both must pass through $(0, 0, 1)$ as was shown in part (b), thus they intersect.

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 $x^2 \equiv a (\bmod\, pq)$? If so, find an example. If not, prove it can never happen.

Proof: What this problem is asking is to determine if there exists y so that $y^2 \equiv a(\bmod\, pq)$ if we know that there are no solutions to the equations $x^2 \equiv a(\bmod\, p)$ and $x^2 \equiv a(\bmod\, q)$. Suppose there is such a y. Then we have that $pq \mid (y^2 - a)$. In particular, $p \mid (y^2 - a)$ and so $y^2 \equiv a(\bmod\, p)$. But we already know that a is not a quadratic residue modulo p, so this is a contradiction. ■

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!)

Proof: Recall that if 2 is a quadratic residue modulo p then 2 cannot be a primitive root. Thus, we show that $\left(\frac{2}{p}\right) = 1$ for primes p of the form $3 \cdot 2^n + 1$ unless $p = 13$, i.e., unless $n = 2$. Recall that $\left(\frac{2}{p}\right) = 1$ if $p \equiv \pm 1(\bmod\, 8)$. If $n = 1$, then $p = 7 \equiv -1(\bmod\, 8)$, so in this case $\left(\frac{2}{p}\right) = 1$. If $n \geq 3$, then $p \equiv 1(\bmod\, 8)$ so that $\left(\frac{2}{p}\right) = 1$ as well. For $p = 13$, we have $p \equiv 5(\bmod\, 8)$ and so $\left(\frac{2}{13}\right) = -1$. ■

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.

Proof: Recall that there are precisely $(p-1)/2$ quadratic residues and that $1^2, 2^2, \ldots, ((p-1)/2)^2$ are all quadratic residues. Thus, to show these are all the quadratic residues modulo p we need to show that these are all distinct elements. Suppose $i^2 \equiv j^2(\bmod\, p)$. This implies that $p \mid (i^2 - j^2) = (i-j)(i+$

$j)$, i.e., $p \mid (i-j)$ or $p \mid (i+j)$. However, we know that $1 \le i, j \le (p-1)/2$, so in particular we have that if $p \mid (i \pm j)$, then $i = j$. Thus, these elements are all distinct and so are all the quadratic residues modulo p.
The sum of all the quadratic residues is given by

$$\begin{aligned} 1^2 + 2^2 + \cdots + ((p-1)/2)^2 &= \sum_{k=1}^{(p-1)/2} k^2 \\ &= \frac{\left(\frac{p-1}{2}\right)\left(\frac{p-1}{2}+1\right)\left(2\frac{p-1}{2}+1\right)}{6} \\ &= p\frac{\left(\frac{p-1}{2}\right)\left(\frac{p-1}{2}+1\right)}{6}. \end{aligned}$$

Thus, it is clear that p divides this as the 6 cannot cancel the p (we assumed $p > 3$ here!) $\blacksquare$

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

Proof: One uses the criterion we proved for $\left(\frac{2}{p}\right)$ and $\left(\frac{3}{p}\right)$ and then the Chinese remainder theorem. $\blacksquare$

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

Note that 12703 is prime and $3658 = 2 \cdot 31 \cdot 59$. Thus, $\left(\frac{3658}{12703}\right) = \left(\frac{2}{12703}\right)\left(\frac{31}{12703}\right)\left(\frac{59}{12703}\right)$. Since $12703 \equiv -1 \pmod 8$, we know that $\left(\frac{2}{12703}\right) = 1$. We use quadratic reciprocity to calculate the other two. quadratic reciprocity gives

$$\begin{aligned} \left(\frac{31}{12703}\right)\left(\frac{12703}{31}\right) &= (-1)^{((12703-1)/2)\cdot((31-1)/2)} = -1 \\ \left(\frac{59}{12703}\right)\left(\frac{12703}{59}\right) &= (-1)^{((59-1)/2)\cdot((12703-1)/2)} = -1. \end{aligned}$$

Thus, we need to calculate $\left(\frac{12703}{31}\right) = \left(\frac{24}{31}\right)$ and $\left(\frac{12703}{59}\right) = \left(\frac{18}{59}\right)$. We show the first and omit the second.

$$\begin{aligned} \left(\frac{24}{31}\right) &= \left(\frac{4}{31}\right)\left(\frac{2}{31}\right)\left(\frac{3}{31}\right) \\ &= \left(\frac{2}{31}\right)\left(\frac{3}{31}\right). \end{aligned}$$

Since $31 \equiv -1 (\bmod 8)$, we have $\left(\frac{2}{31}\right) = 1$. We use quadratic reciprocity again to calculate $\left(\frac{3}{31}\right)$. This gives

$$\left(\frac{3}{31}\right)\left(\frac{31}{3}\right) = -1$$

and $31 \equiv 1 (\bmod 3)$ and so $\left(\frac{31}{3}\right) = \left(\frac{1}{3}\right) = 1$. Thus, $\left(\frac{3}{31}\right) = -1$. Using this and the calculation omitted one obtains $\left(\frac{3658}{12703}\right) = 1$.

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 $\left(\frac{-a}{p}\right) = 1$.

Proof: Suppose that the equation $x^2 + py + a = 0$ has an integral solution. Reducing this equation modulo p gives $x^2 \equiv -a (\bmod p)$, and so $\left(\frac{-a}{p}\right) = 1$. Now suppose $\left(\frac{-a}{p}\right) = 1$. This implies there exists $z \in \mathbb{Z}$ so that $z^2 \equiv -a (\bmod p)$, i.e., there exists $t \in \mathbb{Z}$ so that $z^2 + a = pt$. Thus, the equation has an integer solution, namely $x = z$ and $y = -t$. ■

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

Recall a point (x_0, y_0) on the curve $f(x, y) = 0$ is a singular point if $\frac{\partial f}{\partial y}(x_0, y_0) = \frac{\partial f}{\partial x}(x_0, y_0) = 0$. We have

$$\frac{\partial f}{\partial y} = x(x^2 - 3) = 0$$

if and only if $x = 0$ or $x = \pm\sqrt{3}$ and

$$\frac{\partial f}{\partial x} = 3y(x^2 - 1) = 0$$

if and only if $y = 0$ or $x = \pm 1$. Clearly if $x = \pm 1$, then $\frac{\partial f}{\partial y} \neq 0$, so we must have $y = 0$ from the second equation. Thus, the possible singular points are $(0, 0), (\pm\sqrt{3}, 0)$. It is clear these points are all on the curve, so we have these three singular points.

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.

This proceeds essentially as before, only now we take a tangent line instead of a line between two distinct points P and Q. Let $y = m(x - x_0) + y_0$ be the tangent line to the elliptic curve E_N at the point P. We saw before that this intersects the elliptic curve at another point $R = (x_1, y_1)$. As in class, if we set $f(x) = x^3 - N^2x - (m(x - x_0) + y_0)^2$, then the sum of the roots is equal to the negative of x^2 coefficient, i.e, equal to m^2. The sum of the roots this time is $x_0 + x_0 + x_1$. Thus, we have $x_1 = -2x_0 + m^2$. To calculate m we implicitly differentiate the equation for the elliptic curve and solve for $\frac{dy}{dx}$ to obtain

$$m = \frac{3x_0^2 - N^2}{2y_0}.$$

We can plug this value for x_1 back into the equation of the line to get the value of y_1, i.e., $y_1 = m(x_1 - x_0) + y_0$. We know that the x-coordinate of $2P$ is exactly x_1 and the y-coordinate is $-y_1$. Thus, we have equations to calculate $2P$. (These will be needed in the next homework assignment!!!) ■

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 $\gcd(x, y, z) = 1$.

Proof: Let $X = \frac{a}{b}$ and $Y = \frac{c}{d}$ in lowest terms. We begin by observing that we can assume $\gcd(a, c) = 1$ for if not, we can divide X, Y, and Z by $\gcd(a, c)$. Let $x = \operatorname{lcm}(b, d)X = \frac{ad}{\gcd(b,d)}$, $y = \operatorname{lcm}(b, d)Y = \frac{cb}{\gcd(b,d)}$, and $z = \operatorname{lcm}(b, d)Z$. Let p be a prime so that $p \mid x$ and $p \mid y$. Since $\gcd(b, d) \mid b$ and $\gcd(a, b) = 1$ (since the fraction is in lowest terms) we have $\gcd(a, \gcd(b, d)) = 1$. Thus, we have $p \mid a$ or $p \mid \frac{d}{\gcd(b,d)}$. If $p \mid a$, then we know that $p \nmid c$ since $\gcd(a, c) = 1$, so $p \mid \frac{d}{\gcd(b,d)}$. However, this is a contradiction as $\gcd\left(\frac{b}{\gcd(b,d)}, \frac{d}{\gcd(b,d)}\right) = 1$. Now suppose $p \mid \frac{d}{\gcd(b,d)}$. Then necessarily we have $p \mid c$ arguing as above. But this contradicts the fact that $\gcd(c, d) = 1$. Thus, it must be that no prime divides x and y so they are relatively prime. ■

(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.

Proof: We showed in class that if (x, y, z) is a Pythagorean triple with $\gcd(x, y, z) = 1$, then either x is even or y is even, but not both. (If they both were, 2 would divide z as well and we wouldn't have a gcd of 1!) Assume without loss of generality that x is even. Then z^2 is congruent to 1 modulo 4, so 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.

Proof: Suppose that 1 is a congruent number and let (X, Y, Z) be a Pythagorean triple having area 1 as in part (a). It is clear that there cannot be an integer sided triangle with area 1. (Just check the cases!) As in class, using $N = 1$ here, we obtain the equation

$$\left(\frac{X^2 - Y^2}{4}\right)^2 = \left(\frac{Z}{2}\right)^4 - 1.$$

Multiplying through by 16 we obtain

$$(X^2 - Y^2)^2 = (Z)^4 - 2^4.$$

This gives the solution $w = X^2 - Y^2$, $v = 2$, and $u = Z$ to the equation. This is not an integer solution though. We must clear denominators. Again we multiply by $\frac{bd}{\gcd(b,d)}$ (keeping the same notation as part(a)). Thus, defining x, y, and z as above we have the integer solution $w = x^2 - y^2$, $u = z$, and $v = \frac{2bd}{\gcd(b,d)}$. Since x is even and y is odd, $x^2 - y^2$ is necessarily odd, as desired. ■

(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!)

Proof: Suppose there is a nontrivial triple (a, b, c) with $a^4 + b^4 = c^4$, i.e., $c^4 - a^4 = b^4$. Setting $u = c$, $a = v$ and $b^2 = w$ gives an integer solution to $u^4 - v^4 = w^2$. Thus, if there are no solutions to the equation $u^4 - v^4 = w^2$ then there can be no nontrivial integer solution to Fermat's equation of exponent 4. ■