MTH 505: Number Theory **Spring 2017**
Homework 4 **Drew Armstrong**

4.1. (Squares Mod 4). We say that an element $[a]_n \in \mathbb{Z}/n\mathbb{Z}$ is *square* if there exists an element $[x]_n \in \mathbb{Z}/n\mathbb{Z}$ such that $[a]_n = ([x]_n)^2 = [x^2]_n$.

(a) Prove that $[0]_4$ and $[1]_4$ are the only square elements of $\mathbb{Z}/4\mathbb{Z}$.

(b) Suppose that we have integers $x, y, z \in \mathbb{Z}$ with the property

$$x^2 + y^2 = z^2.$$

In this case use part (a) to show that x and y cannot both be odd. [Hint: The elements $[x^2]_4$ and $[y^2]_4$ are square elements of $\mathbb{Z}/4\mathbb{Z}$. If x and y are both odd, show that the sum $[x^2]_4 + [y^2]_4$ cannot be a square element of $\mathbb{Z}/4\mathbb{Z}$.]

4.2. (Fermat's Last Theorem). In this exercise you will prove the easiest case of Fermat's Last Theorem, which is the only case that Fermat proved himself. That is, you will prove that there **do not exist integers** $(x, y, z) \in \mathbb{Z}^3$ such that $xyz \neq 0$ and

$$x^4 + y^4 = z^4.$$

In fact, you will prove the stronger statement that the equation

(FLT) $$x^4 + y^4 = z^2.$$

has no integer solution $(x, y, z) \in \mathbb{Z}^3$ with $xyz \neq 0$.

(a) Suppose that (FLT) has a solution $(x, y, z) \in \mathbb{Z}^3$ with $xyz \neq 0$. In this case prove that (FLT) has a solution $(x', y', z') \in \mathbb{Z}^3$ with $x'y'z' \neq 0$ and $\gcd(x', y') = 1$. [Hint: If p is a common prime divisor of x and y show that $(x/p, y/p, z/p^2) \in \mathbb{Z}^3$ is another solution. Repeat until x and y have no common prime divisor.]

(b) *(Fermat's Method of Infinite Descent)* Suppose that (FLT) has a solution $(x, y, z) \in \mathbb{Z}^3$ with $xyz \neq 0$ and $\gcd(x, y) = 1$. In this case, prove that there exists a solution (x', y', z') with $x'y'z' \neq 0$, $\gcd(x', y') = 1$ and $0 < z' < |z|$. [Hint: Since $x^4 + y^4 = (x^2)^2 + (y^2)^2 = z^2$, Problem 4.1(b) says that x and y cannot both be odd, so assume WLOG that x is odd and y is even. By replacing z with $|z|$ we can also assume that $z > 0$. Then from the classification of Pythagorean triples (proved in class) there exist integers $u, v \in \mathbb{Z}$ with $\gcd(u, v) = 1$ and $v > 0$ such that

$$x^2 = v^2 - u^2, \quad y^2 = 2uv \quad \text{and} \quad z = v^2 + u^2.$$

Use 4.1(b) and the classification of Pythagorean triples (again!) to show that there exist integers $r, s \in \mathbb{Z}$ with $\gcd(r, s) = 1$ and $s > 0$ such that

$$x = s^2 - r^2, \quad u = 2rs \quad \text{and} \quad v = s^2 + r^2.$$

Use the fact $(u/2)v = (y/2)^2$ to show that $u/2$ and v are perfect squares, then use the fact $rs = u/2$ to show that r and s are perfect squares. Finaly, show that we have $s = (x')^2$, $r = (y')^2$ and $v = (z')^2$ for some integers $(x', y', z') \in \mathbb{Z}^3$ with $x'y'z' \neq 0$, $\gcd(x', y') = 1$ and $0 < z' < |z|$.]

(c) Combine the results of (a) and (b) to finish the proof.

4.3. (Rational Points on a Hyperbola). In this problem you will find the complete rational solution $(\alpha, \beta) \in \mathbb{Q}^2$ to the equation

(Hyp) $$4\alpha^2 - 4\alpha\beta - 7\beta^2 - 16\beta - 9 = 0.$$

(a) Find an invertible affine transformation with rational coefficients to rewrite (Hyp) in the equivalent form
$$x^2 - 2y^2 = 1.$$

(b) Draw a picture of the hyperbola $x^2 - 2y^2 = 1$ with a line of slope t going through the point $(-1, 0)$. Let (x_t, y_t) be the coordinates of the other point of intersection.

(c) Compute formulas for the coordinates of (x_t, y_t) in terms of t. Use your formulas to show that
$$t \in \mathbb{Q} \quad \Longleftrightarrow \quad (x_t, y_t) \in \mathbb{Q}^2.$$

(d) Substitute $t = u/v$ for coprime integers $u, v \in \mathbb{Z}$ with $v > 0$ to find the general formula for rational points on the hyperbola $x^2 - 2y^2 = 1$.

(e) Invert your affine transformation from part (a) to find the general formula for rational points on the original hyperbola (Hyp).

4.4 (A Hyperbola With No Rational Points). If we could find just one rational point on the hyperbola $x^2 - 2y^2 = 3$ then we would obtain infinitely many rational points as in Problem 4.3. However, we will see that there **are no rational points**.

(a) Assume that there exist rational numbers $(x, y) \in \mathbb{Q}^2$ such that $x^2 - 2y^2 = 3$. In this case prove that there exist integers $(a, b, c) \in \mathbb{Z}^3$ with **no common factor** such that
$$a^2 - 2b^2 = 3c^2.$$

(b) With $a, b, c \in \mathbb{Z}$ as in part (a), prove that $\gcd(a, 3) = 1$.

(c) Reduce the equation $a^2 - 2b^2 = 3c^2 \bmod 3$ to get
$$\begin{aligned} [a^2]_3 &= [2b^2]_3 \\ [2]_3 \cdot [a^2]_3 &= [2]_3 \cdot [2b^2]_3 \\ [2]_3 \cdot [a^2]_3 &= [(2b)^2]_3. \end{aligned}$$
Now part (b) implies that we can divide both sides by $[a^2]_3$ to get
$$[2]_3 = [(2b)^2]_3 \cdot [a^{-2}]_3 = \left([2b]_3 \cdot [a^{-1}]_3\right)^2.$$
Use this to find a contradiction.