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 $\mathbb{Z}/4\mathbb{Z}$.]

Proof. (a): Here is a table showing the square of every element of $\mathbb{Z}/4\mathbb{Z}$:

$[a]_4$	$[0]_4$	$[1]_4$	$[2]_4$	$[3]_4$
$[a^2]_4$	$[0]_4$	$[1]_4$	$[0]_4$	$[1]_4$.

We observe from the second row of the table that the only square elements are $[0]_4 = [0^2]_4 = [2^2]_4$ and $[1]_4 = [1^2]_3 = [3^2]_4$.

(b): Suppose we have $x, y, z \in \mathbb{Z}$ with $x^2 + y^2 = z^2$. Reducing this equation mod 4 gives

$$[x^2]_4 + [y^2]_4 = [z^2]_4.$$

If both of x and y are odd, then $[x]_4$ and $[y]_4$ must be in the set $\{[1]_4, [3]_4\}$. But then part (a) implies that $[x^2]_4 = [y^2]_4 = [1]_4$ and hence

$$[z^2]_4 = [x^2]_4 + [y^2]_4 = [1]_4 + [1]_4 = [2]_4.$$

This contradicts the fact that $[2]_4$ is not 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.

Proof. (a): Suppose that we have integers $(x, y, z) \in \mathbb{Z}^3$ such that $x^2 + y^2 = z^2$ and $xyz \neq 0$. If $(x, y) = (0, 0)$ then the equation $z^2 = x^2 + y^2 = 0$ implies that $z = 0$ which contradicts the fact that $xyz \neq 0$, so we may assume that $(x, y) \neq (0, 0)$. Now suppose that p is any common prime divisor of x and y with $x = px'$ and $y = py'$. Then we see that p divides z^2 because

$$\begin{aligned} x^2 + y^2 &= z^2 \\ (px')^2 + (py')^2 &= z^2 \\ p^2((x')^2 + (y')^2) &= z^2, \end{aligned}$$

and from Euclid's Lemma this implies that p divides z, say $z = pz'$. Finally, since $p \neq 0$ we have

$$\begin{aligned} p^2((x')^2 + (y')^2) &= z^2 \\ p^2((x')^2 + (y')^2) &= (pz')^2 \\ p^2((x')^2 + (y')^2) &= p^2(z')^2 \\ (x')^2 + (y')^2 &= (z')^2. \end{aligned}$$

If $\gcd(x', y') = 1$ then we are done. Otherwise, there exists a common prime divisor q of x' and y' with $x' = qx''$ and $y' = qy''$ and we can repeat the process to obtain

$$(x'')^2 + (y'')^2 = (z'')^2$$

for some integer $z'' \in \mathbb{Z}$. I claim that this process must eventually stop. Indeed, since $(x, y) \neq (0, 0)$ we can assume without loss of generality that $x > 0$. If the process never stops then we obtain an infinite decreasing sequence of positive integers

$$x > x' > x'' > \cdots > 0,$$

which contradicts the Well-Ordering Principle.

(b): Assume that there exist integers $(x, y, z) \in \mathbb{Z}^3$ with $x^4 + y^4 = z^2$ such that $xyz \neq 0$ and $\gcd(x, y) = 1$. Since $(x, y) \neq 0$ this implies that $z^2 \neq 0$ so we can assume without loss of generality that $z \geqslant 1$.

To begin, we observe that $z^2 = x^4 + y^4 = (x^2)^2 + (y^2)^2$. From 4.1(b) this tells us that x^2 and y^2 (hence also x and y) cannot both be odd. So let us assume without loss of generality that x is odd and y is even. From the classification of Pythagorean triples (proved in class) we conclude that there exist integers $u, v \in \mathbb{Z}$ with $\gcd(u, v) = 1$ and $v \geqslant 1$ such that

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

Since x is even, the equation $x^2+u^2=v^2$ together with 4.1(b) tells us that u is even. Then the classification of Pythagorean triples (again!) tells us that there exist $r,s\in\mathbb{Z}$ with $\gcd(r,s)=1$ and $s\geqslant 1$ such that

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

Since $\gcd(u,v)=1$ and since u is even we see that $u/2$ is an integer with $\gcd(u/2,v)=1$. Now observe that

$$\left(\frac{u}{2}\right)v=\frac{2uv}{4}=\frac{y^2}{4}=\left(\frac{y}{2}\right)^2\geqslant 1.$$

Since $v\geqslant 1$ this implies that $u\geqslant 1$. Furthermore, since $(u/2)v$ is a perfect square and since $\gcd(u/2,v)=1$ the **unique prime factorization**[1] of $(y/2)^2$ shows us that each of $u/2$ and v is a perfect square. Then since

$$rs=\frac{u}{2}\geqslant 1$$

with $s\geqslant 1$ we see that $r\geqslant 1$, and since $rs=u/2$ is a perfect square with $\gcd(r,s)=1$ we conclude that each of r and s is a perfect square. We have shown that there exist integers $x',y',z'\in\mathbb{Z}$ such that

$$s=(x')^2,\quad r=(y')^2\quad\text{and}\quad v=(z')^2$$

and hence $(x')^4+(y')^4=s^2+r^2=v=(z')^2$. It only remains to show that $x'y'z'\neq 0$, $\gcd(x',y')=1$ and $0<z'<z$. The fact that $x'y'z'\neq 0$ follows from the fact $y\neq 0$ and the equation

$$y^2=2uv=2(2rs)v=4(x'y'z')^2.$$

To see that $\gcd(x',y')=1$, observe that any common divisor of x' and y' is also a common divisor of $s=(x')^2$ and $r=(y')^2$ and hence $1\leqslant\gcd(x',y')\leqslant\gcd(r,s)=1$. Finally, to see that $z'<z$ first observe that the inequalities $1\leqslant z'$ and $1\leqslant v$ imply that $z'\leqslant(z')^2$ and $v\leqslant v^2$. Since $y\neq 0$ and $y^2=2uv$ we must also have $u\neq 0$ and it follows that

$$z'\leqslant(z')^2=v\leqslant v^2<v^2+u^2=z$$

as desired.

(c): Here is the complete proof. **Assume for contradiction that there exist integers $(x,y,z)\in\mathbb{Z}^3$ such that $xyz\neq 0$ and $x^4+y^4=z^4$.** If $z=0$ then this implies that $(x,y)=(0,0)$ which contradicts the fact that $(x,y,z)\neq(0,0,0)$. Furthermore, if $(x,y)=(0,0)$ then we obtain the contradiction $z=0$. So we can assume that $(x,y)\neq(0,0)$ and $z\neq 0$.

Now observe that we have $x^4+y^4=(z')^2$ where $z'=z^2\geqslant 1$. By part (a) this implies that there exist integers $(x',y',z'')\in\mathbb{Z}^3$ with $(x')^4+(y')^4=(z'')^2$ such that $x'y'z''\neq 0$ and $\gcd(x',y')=1$. We can also assume without loss of generality that $z''\geqslant 1$. Then from part (b) we know that there exist integers $(x'',y'',z''')\in\mathbb{Z}^3$ such that $(x'')^4+(y'')^4=(z''')^2$ with $x''y''z'''\neq 0$, $\gcd(x'',y'')=1$ and $1\leqslant z'''<z''$. Finally, we observe that this process can be repeated indefinitely to obtain an infinite decreasing sequence of positive integers

$$z\geqslant z'\geqslant z''>z'''>z''''>\cdots>0,$$

which contradicts the Well-Ordering Principle. □

[Remark: This is by far the easiest case of Fermat's Last Theorem. Euler gave a more involved proof for the exponent 3 which depends on the fact that the commutative ring $\mathbb{Z}[e^{2\pi i/3}]$ has unique prime factorzation. Later it was realized that a similar proof works for exponent n whenever the ring $\mathbb{Z}[e^{2\pi i/n}]$ has unique prime factorization. Unfortunately, Kummer observed that unique

[1]This is a key step. I'll discuss it in the remark after the proof.

factorization fails in general. Eventually Kronecker and Dedekind were able to restore unique factorization by replacing "numbers" with "ideals". Unfortunately too much structure was lost to recover the proof of FLT. The proof had to wait another hundred years for new methods.]

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

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

(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).

Proof. (a): Let's do it from scratch using Hermite reduction. First we consider the quadratic form

$$4\alpha^2 - 4\alpha\beta - 7\beta^2 = \begin{pmatrix}\alpha & \beta\end{pmatrix}\begin{pmatrix}4 & -2\\ -2 & -7\end{pmatrix}\begin{pmatrix}\alpha\\ \beta\end{pmatrix} = \alpha^T A \alpha.$$

We want to find a rational invertible matrix P such that $P^T A P$ is diagonal. To do this we perform a sequence of simultaneous row/column operations on the augmented matrix:

$$\left(\begin{array}{cc|cc} 4 & -2 & 1 & 0\\ -2 & -7 & 0 & 1\\ \hline 1 & 0 & & \\ 0 & 1 & & \end{array}\right) \to \left(\begin{array}{cc|cc} 4 & 0 & 1 & 0\\ 0 & -8 & 1/2 & 1\\ \hline 1 & 1/2 & & \\ 0 & 1 & & \end{array}\right) \to \left(\begin{array}{cc|cc} 1 & 0 & 1/2 & 0\\ 0 & -2 & 1/4 & 1/2\\ \hline 1/2 & 1/4 & & \\ 0 & 1/2 & & \end{array}\right).$$

It follows from this computation that

$$\begin{pmatrix}1/2 & 0\\ 1/4 & 1/2\end{pmatrix}\begin{pmatrix}4 & -2\\ -2 & -7\end{pmatrix}\begin{pmatrix}1/2 & 1/4\\ 0 & 1/2\end{pmatrix} = \begin{pmatrix}1 & 0\\ 0 & -2\end{pmatrix}.$$

Thus we will make a change of variables of the form

$$\begin{pmatrix}\alpha\\ \beta\end{pmatrix} = \begin{pmatrix}1/2 & 1/4\\ 0 & 1/2\end{pmatrix}\begin{pmatrix}x\\ y\end{pmatrix} + \begin{pmatrix}u\\ v\end{pmatrix} = \begin{pmatrix}x/2 + y/4 + u\\ y/2 + v\end{pmatrix}$$

for some rational numbers $u, v \in \mathbb{Q}$. In order to determine u and v, we substitute $\alpha = x/2 + y/4 + u$ and $\beta = y/2 + v$ into (Hyp) to obtain

$$\begin{aligned} 4\alpha^2 - 4\alpha\beta - 7\beta^2 - 16\beta - 9 &= 0\\ 4(x/4 + y/8 + u)^2 - 4(x/4 + y/8 + u)(y/4 + v) - 7(y/4 + v)^2 - 16(y/4 + v) - 9 &= 0\\ x^2 - 2y^2 + (4u - 2v)x - (8 + 8v)y + (4u^2 - 4uv - 7v^2 - 16u - 9) &= 0. \end{aligned}$$

Our goal is to choose u and v so that $(4u - 2v) = 0$ and $(8 + 8v) = 0$. The second equation implies $v = -1$ and then the first equation implies $u = -1/2$. In summary, by making the rational invertible affine change of variables

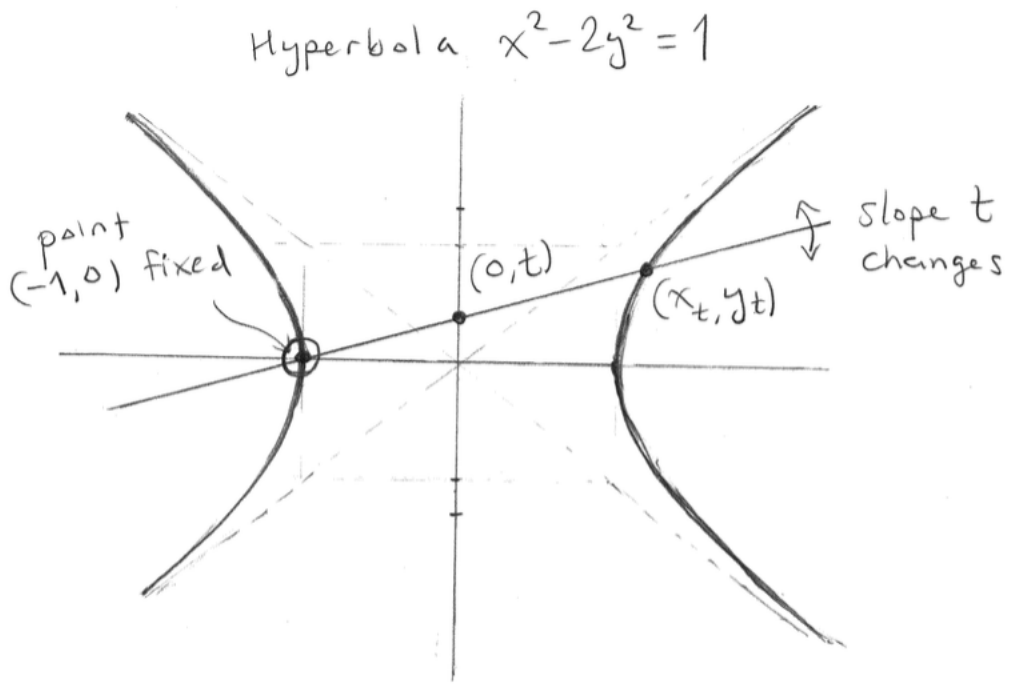
$$\begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} 1/2 & 1/4 \\ 0 & 1/2 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} + \begin{pmatrix} -1/2 \\ -1 \end{pmatrix} = \begin{pmatrix} x/2 + y/4 - 1/2 \\ y/2 - 1 \end{pmatrix}$$

we obtain the equivalent equation

$$\begin{aligned} x^2 - 2y^2 + (4u - 2v)x - (8 + 8v)y + (4u^2 - 4uv - 7v^2 - 16u - 9) &= 0 \\ x^2 - 2y^2 + 0x + 0y + 4(-1/2)^2 - 4(-1/2)(-1) - 7(-1)^2 - 16(-1/2) - 9 &= 0 \\ x^2 - 2y^2 - 1 &= 0 \\ x^2 - 2y^2 &= 1, \end{aligned}$$

as desired.

(b): So let's solve the equation $x^2 - 2y^2 = 1$. Geometrically this is a hyperbola in the real x, y-plane. We consider the line of slope t through the (rational) point $(-1, 0)$ on the hyperbola and we let (x_t, y_t) denote the other point of intersection as in the following beautiful picture:



(c): To compute the coordinates of (x_t, y_t) we substitute the equation of the line $y = t(x + 1)$ into the equation of the hyperbola $x^2 - 2y^2 = 1$ to obtain

$$\begin{aligned} x^2 - 2y^2 &= 1 \\ x^2 - 2t^2(x + 1)^2 &= 1 \\ x^2 - 2t^2(x^2 + 2x + 1) &= 1 \\ (1 - 2t^2)x^2 + (-4t^2)x + (-1 - 2t^2) &= 0. \end{aligned}$$

Then we use the quadratic formula:

$$\begin{aligned} x &= \frac{4t^2 \pm \sqrt{(-4t^2)^2 - 4(1-2t^2)(-1-2t^2)}}{2(1-2t^2)} \\ &= \frac{4t^2 \pm \sqrt{16t^4 + 4 - 16t^4}}{2(1-2t^2)} \\ &= \frac{4t^2 \pm \sqrt{4}}{2(1-2t^2)} \\ &= \frac{4t^2 \pm 2}{2(1-2t^2)} \\ &= \frac{2t^2 \pm 1}{1-2t^2} \\ &= -1 \text{ or } \frac{1+2t^2}{1-2t^2}. \end{aligned}$$

The value $x = -1$ corresponds to the point $(x, y) = (-1, 0)$ so we conclude that $x_t = (1 + 2t^2)/(1 - 2t^2)$. Then we substitute into the equation of the line to obtain

$$y_t = t(x_t + 1) = t\left(\frac{1+2t^2}{1-2t^2} + \frac{1-2t^2}{1-2t^2}\right) = \frac{2t}{1-2t^2}.$$

Finally, it follows from the equation $y_t = t(x_t + 1)$ that

$$(x_t, y_t) \in \mathbb{Q}^2 \quad \Longrightarrow \quad t \in \mathbb{Q}$$

and it follows from the equation

$$(x_t, y_t) = \left(\frac{1+2t^2}{1-2t^2}, \frac{2t}{1-2t^2}\right)$$

that

$$t \in \mathbb{Q} \quad \Longrightarrow \quad (x_t, y_t) \in \mathbb{Q}^2.$$

Indeed, we observe that the denominators never vanish because $t = 1/\sqrt{2}$ is irrational.

(d): From part (c) we see that every rational point on the hyperbola $x^2 - 2y^2 = 1$ has the form (x_t, y_t) for some rational number $t \in \mathbb{Q}$. By writing t in lowest terms we can assume that $t = u/v$ for some unique integers $u, v \in \mathbb{Z}$ with $\gcd(u, v) = 1$ and $v \geqslant 1$. Then we can substitute this into the formula for (x_t, y_t) to obtain

$$\begin{aligned} (x_t, y_t) &= \left(\frac{1+2t^2}{1-2t^2}, \frac{2t}{1-2t^2}\right) \\ &= \left(\frac{1+2(u/v)^2}{1-2(u/v)^2}, \frac{2t}{1-2(u/v)^2}\right) \\ &= \left(\frac{v^2+2u^2}{v^2-2u^2}, \frac{2uv}{v^2-2u^2}\right). \end{aligned}$$

I won't bother to check if these fractions are in lowest terms.

(e): Finally, we invert the affine transformation from part (a) to obtain the complete rational solution to the equation (Hyp). To be specific, for each rational number $t = u/v$ in lowest

terms we obtain the rational point

$$\begin{aligned}(\alpha_t, \beta_t) &= (x_t/2 + y_t/4 - 1/2, y_t/2 - 1) \\ &= \left(\frac{u(4u+v)}{2(v^2-2u^2)}, \frac{2u^2+uv-2v^2}{v^2-2u^2} \right).\end{aligned}$$

Again, I won't check if these fractions are in lowest terms. □

[Remark: Suppose we wanted to find all **integer** solutions $(x, y) \in \mathbb{Z}$ to the equation $x^2 - 2y^2 = 1$. From the answer to part (d), this problem is equivalent to determining all coprime integers $\gcd(u, v)$ with $v \geqslant 1$ such that

$$(v^2 - 2u^2) | (v^2 + 2u^2) \qquad \text{and} \qquad (v^2 - 2u^2) | (2uv).$$

Equivalently, we require that $(v^2 - 2u^2)$ divides the greatest common divisor of $(v^2 + 2u^2)$ and $2uv$. We will need some new ideas to solve this.]

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.

Proof. (a): Suppose that we have $(x, y) \in \mathbb{Q}^2$ such that $x^2 - 2y^2 = 3$. By finding a common denominator we can write $(x, y) = (a/c, b/c)$ for some integers $(a, b, c) \in \mathbb{Z}^3$ with $c \geqslant 1$. Then substituting gives

$$\begin{aligned}(a/c)^2 - 2(b/c)^2 &= 3 \\ a^2 - 2b^2 &= 3c^2.\end{aligned}$$

Finally, let $\lambda = \gcd(a, b, c)$ with $a = \lambda a'$, $b = \lambda b'$ and $c = \lambda c'$. Then we have $\gcd(a', b', c') = 1$ and since $\lambda \neq 0$ we obtain

$$\begin{aligned}a^2 - 2b^2 &= 3c^2 \\ (\lambda a')^2 - 2(\lambda b')^2 &= 3(\lambda c')^2 \\ \lambda^2((a')^2 - 2(b')^2) &= \lambda^2 3(c')^2 \\ (a')^2 - 2(b')^2 &= 3(c')^2\end{aligned}$$

as desired.

(b): I don't want to keep writing the "primes", so let's assume that $a^2 - 2b^2 = 3c^2$ with $\gcd(a, b, c) = 1$. Since 3 is prime we observe that $\gcd(a, 3) \neq 1$ if and only if $3|a$. So let us **assume for contradiction** that $3|a$, say $a = 3a'$. Then the equation

$$\begin{aligned} a^2 - 2b^2 &= 3c^2 \\ (3a')^2 - 2b^2 &= 3c^2 \\ 3(3(a')^2 - c^2) &= 2b^2 \end{aligned}$$

says that $3|2b^2$ and it follows from Euclid's Lemma that $3|b$, say $b = 3b'$. Substituting gives

$$\begin{aligned} a^2 - 2b^2 &= 3c^2 \\ (3a')^2 - 2(3b')^2 &= 3c^2 \\ 9((a')^2 - 2(b')^2) &= 3c^2 \\ 3((a')^2 - 2(b')^2) &= c^2, \end{aligned}$$

which says that $3|c^2$ and hence $3|c$ by Euclid's Lemma. We have shown that 3 is a common divisor of a, b and c, which contradicts the fact that $\gcd(a, b, c) = 1$.

(c): **Assume for contradiction** that there exists a rational point $(x, y) \in \mathbb{Q}^2$ on the hyperbola $x^2 - 2y^2 = 3$. Then part (a) says that there exist coprime integers $\gcd(a, b, c) = 1$ such that $a^2 - 2b^2 = 3c^2$ and part (b) says that $\gcd(a, 3) = 1$. In particular, this says that the element $[a]_3 \in \mathbb{Z}/3\mathbb{Z}$ and hence also the element $[a^2]_3 \in \mathbb{Z}/3\mathbb{Z}$ is **invertible**. By reducing the equation $a^2 - 2b^2 = 3c^2$ mod 3 we obtain

$$\begin{aligned} [a^2 - 2b^2]_3 &= [3c^2]_3 \\ [a^2]_3 - [2b^2]_3 &= [0]_3 \\ [a^2]_3 &= [2b^2]_3 \\ [1]_3 &= [2b^2]_3 \cdot [a^{-2}]_3 \\ [2]_3 \cdot [1]_3 &= [2]_3 \cdot [2b^2]_3 \cdot [a^{-2}]_3 \\ [2]_3 &= [(2b)^2]_3 \cdot [(a^{-1})^2]_3 \\ (*) \qquad [2]_3 &= \left([2b]_3 \cdot [a^{-1}]_3\right)^2. \end{aligned}$$

I don't know what the element $[2b]_3 \cdot [a^{-1}]_3 \in \mathbb{Z}/3\mathbb{Z}$ is, but it certainly exists. Then equation $(*)$ tells us that $[2]_3$ is a square element of $\mathbb{Z}/3\mathbb{Z}$. But this is false because there are only three elements of $\mathbb{Z}/3\mathbb{Z}$ and none of them is a square root of $[2]_3$:

$$[0^2]_3 = [0]_3 \neq [2]_3, \quad [1^2]_3 = [1]_3 \neq [2]_3 \quad \text{and} \quad [2^2]_3 = [1]_3 \neq [2]_3.$$

□

[Remark: A generalization of this argument can be used to show the following. Fix squarefree and pairwise coprime integers $a, b, c \in \mathbb{Z}$ and suppose that we have rational numbers $x, y \in \mathbb{Q}$ such that $ax^2 + by^2 + c = 0$. Then we find that the following elements are **square**:

$$[-ab]_c \in \mathbb{Z}/c\mathbb{Z}, \quad [-ac]_b \in \mathbb{Z}/b\mathbb{Z} \quad \text{and} \quad [-bc]_a \in \mathbb{Z}/a\mathbb{Z}.$$

It is a celebrated theorem of Legendre (1785) that these conditions are also sufficient for the existence of a rational solution. We will prove this in class.]