MTH 505 Homework 4

Roy Howie

April 14, 2017

4.1 Squares Mod 4

(a) Note $0^2 \equiv 0$, $1^2 \equiv 1$, $2^2 \equiv 0$, and $3^2 \equiv 1$ modulo 4. Thus 0 and 1 are the only square elements of $\mathbb{Z}_4$.

(b) First, for $n \in \mathbb{Z}$, note $n \equiv 1 \pmod 2$ implies $n^2 \equiv 1 \pmod 4$. Next, let $x, y, z \in \mathbb{Z}$ such that $x^2 + y^2 = z^2$. Suppose x and y are both odd, then $x^2 \equiv y^2 \equiv 1 \pmod 4$, implying $z^2 \equiv 2 \pmod 4$. A contradiction, as 2 is not a square elements of $\mathbb{Z}_4$. Hence, x and y cannot both be odd. □

4.2 Fermat's Last Theorem

Consider (FLT): $x^4 + y^4 = z^2$ for $x, y, z \in \mathbb{Z}$ with $xyz \neq 0$.

(a) Suppose FLT has a solution $(x_1, y_1, z_1) \in \mathbb{Z}^3$, then there is another solution $(x_n, y_n, z_n) \in \mathbb{Z}^3$ with $\gcd(x_n, y_n) = 1$ and $0 < z_n < |z|$.

Let p be a prime divisor of both x_1 and y_1. If no such number exists, then $\gcd(x_1, y_1) = 1$ and we are done. Otherwise, $(x_1/p, y_1/p, z_1/p^2)$ is another solution, as $(x_1/p)^4 + (y_1/p)^4 = (x_1^4 + y_1^4)/p^4 = z_1^2/p^4$. Recurse.

(b) Suppose (x, y, z) is a solution to FLT with $\gcd(x, y) = 1$.

Note x and y cannot both be odd, as $x^4 + y^4 = (x^2)^2 + (y^2)^2 = z^2$. WLOG, assume x is odd, y is even, and $z = |z|$. There are then coprime $u, v \in \mathbb{Z}$ with $v > 0$ such that $x^2 = v^2 - u^2$, $y = 2uv$, and $z = u^2 + v^2$. As $u^2 + x^2 = v^2$, there are again coprime $r, s \in \mathbb{Z}$ with $s > 0$ such that $x = s^2 - r^2$, $u = 2rs$, and $v = r^2 + s^2$.

Next, consider $y^2 = 2uv$. Since y is even, 4 divides y^2. Note u is even, as x is odd and $u^2 + x^2 = v^2$. Thus, $(y/2)^2 = (u/2)v$. Recall $\gcd(u, v) = 1$ and that if a prime p divides a number t^2, then p^2 does too. Therefore, if p^2 divides $(y/2)^2$, then p^2 divides either $u/2$ or v. Hence, $u/2$ and v are perfect squares each. By similar argument, as $u = 2rs$ and $u/2$ is an even square number, r and s are also perfect squares.

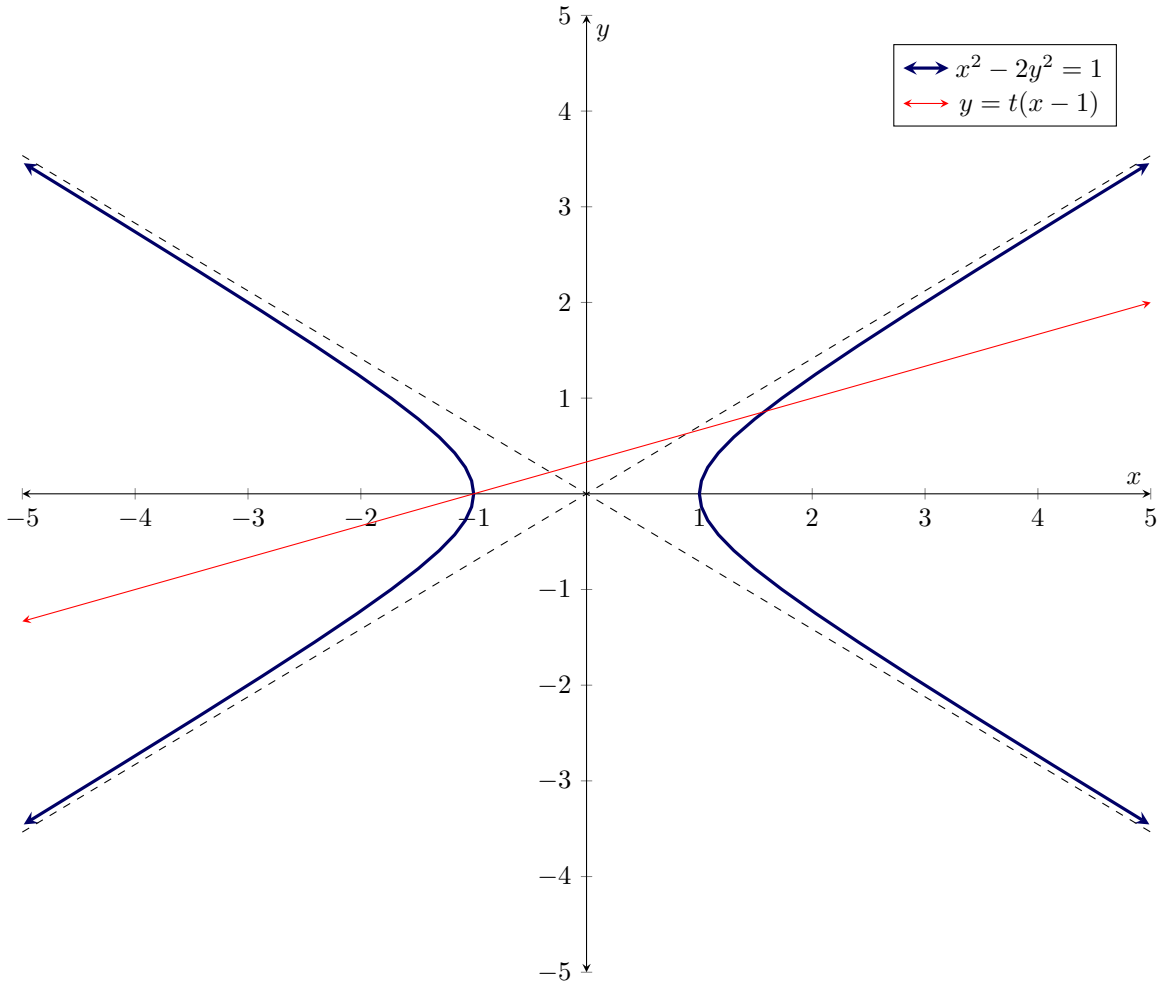
Therefore, there are $(m, n, l) \in \mathbb{Z}^3$ with $s = m^2$, $r = n^2$, and $v = l^2$. Note $v = r^2 + s^2$, so $l^2 = m^4 + n^4$ and (m, n, l) is another solution to FLT. Furthermore, $\gcd(m, n) = 1$, as$r$ and s were coprime; $mnl \neq 0$, as $rsv \neq 0$; and $0 < l < |z|$, as $z = u^2 + v^2$ with v positive and $v = l^2$.

(c) We are back to square one, contradicting the well ordering of the integers, as every solution (a, b, c) to FLT produces another solution (d, e, f) with $0 < f < |c|$. Hence, no solution to FLT exists. □

4.3 Rational Points on a Hyperbola

Consider (Hyp): $4\alpha^2 - 4\alpha\beta - 7\beta^2 - 16\beta - 12 = 0$.

(a) Let $P = \left(\begin{smallmatrix} 1 & 0.5 \\ 0 & 1 \end{smallmatrix}\right)$ and $u = (-0.5, -1)$. Apply the affine transformation $x = Px' + u$, where $x = (\alpha, \beta)$ and $x' = (x, y)$. This yields $\alpha = x + 0.5y - 0.5$ and $\beta = y - 1$.



(b)

(c) Consider the equations $x^2 - 2y^2 = 1$ and $y = t(x+1)$, then

$$\begin{aligned} 0 &= x^2 - 2y^2 - 1 \\ &= x^2 - 2t^2(x+1)^2 - 1 \\ &= x^2 \underbrace{(1-2t^2)}_{a} + x \underbrace{(-4t^2)}_{b} + \underbrace{(-2t^2-1)}_{c} \end{aligned}$$

Using the quadratic formula gives

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

Substituting x into $y = t(x+1)$ yields

$$y = t(x+1) = t\left(\frac{1+2t^2}{1-2t^2} + 1\right) = \frac{2t}{1-2t^2}$$

Thus, $(x_t, y_t) = \left(\frac{1+2t^2}{1-2t^2}, \frac{2t}{1-2t^2}\right)$ for $t \neq \pm 1/\sqrt{2}$.

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

(d) Substituting $t = u/v$ for coprime $u, v \in \mathbb{Z}$ with $v > 0$ into (x_t, y_t) produces

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

$$y_t = \frac{2t}{1-2t^2} = \frac{2\left(\frac{u}{v}\right)^2}{1-2\left(\frac{u}{v}\right)^2} = \frac{2uv}{v^2-2u^2}$$

(e) Inverting the affine transformation presented in **4.4.3a** gives $x' = P^{-1}(x-u)$, or that $x = \alpha - \beta/2$ and $y = \beta + 1$. Thus,

$$\alpha = \frac{2u^2+v^2}{v^2-2u^2} + \frac{uv}{v^2-2u^2} - \frac{1}{2}$$

$$\beta = \frac{2uv}{v^2-2u^2} - 1$$

□

4.4 A Hyperbola with No Rational Points

Consider (Hyp2): $x^2 - 2y^2 = 3$.

(a) Assume there is a solution $(x, y) \in \mathbb{Q}^2$ to Hyp2, then x and y can be written in the form a/c and b/c with $\gcd(a, b, c) = 1$ for some $a, b, c \in \mathbb{Z}$. Hyp2 can then be rewritten as $a^2 - 2b^2 = 3c^2$.

(b) Suppose $\gcd(a, 3) \neq 1$, i.e. $\gcd(a, 3) = 3$, then 3 divides a. Therefore, $a = 3k$ for some $k \in \mathbb{Z}$. Hyp2 can then be rewritten once more as $(3k)^2 - 2b^2 = 3c^2$, implying $2b^2 \equiv 0 \pmod 3$, or that $b \in 3\mathbb{Z}$. Hence, $\gcd(a, b, c) \geq 3$, a contradiction, as $\gcd(a, b, c)$ was said to be 1. Thus, $\gcd(a, 3) = 1$.

(c) Reduce $a^2 - 2y^2 = 3c^2 \bmod 3$ to get $2a^2 \equiv (2y)^2 \pmod 3$. From part **b**, we can reduce this to $2 \equiv (2ya^{-1})^2 \pmod 3$. This is a contradiction, as 2 is not a square modulo 3, for $0^2 \equiv 0$, $1^2 \equiv 1$, and $2^2 \equiv 1$ modulo 3. □