The Quaternion Algebra Unit Circle

Andrew W. Herring

Department of Mathematics and Statistics
University of New Mexico

April 23, 2013

1 $\mathbb{Q}$-Rationality

Let K be a field. The quaternion algebra $\left(\dfrac{a,b}{K}\right)$ is the four dimensional K-algebra with K-basis $\{1, \mathbf{i}, \mathbf{j}, \mathbf{k}\}$ subject to the multiplication

$$\mathbf{i}^2 = a \ , \ \mathbf{j}^2 = b \ , \ \mathbf{ij} = \mathbf{k} = -\mathbf{ji}$$

where $a, b \in K^{\times}$, and multiplication is extended to sums by distribution. From the above three multiplication rules, we can arrive at the additional relations

$$\mathbf{ik} = a\mathbf{j} = -\mathbf{ki} \ , \ \mathbf{kj} = b\mathbf{i} = -\mathbf{jk}$$

In this section, we consider the equation $x^2 + y^2 = 1$ for $x, y \in \left(\dfrac{a,b}{\mathbb{Q}}\right)$, and eventually show that the variety $X = Z(x^2 + y^2 - 1)$ has infinitely many rational points over $\left(\dfrac{a,b}{\mathbb{Q}}\right)$, of unbounded height. More specifically, we show that X is $\mathbb{Q}$-rational.

Definition. *Let V be a variety which is given by polynomials in $\mathbb{Q}[x_1, \dots, x_n]$ for some n. We say that V is $\mathbb{Q}$-rational if there exists a birational map $f : V \dashrightarrow \mathbb{P}^n$ such that f is given by rational functions with $\mathbb{Q}$ coefficients.*

Toward this goal, let $x, y \in \left(\dfrac{a,b}{\mathbb{Q}}\right)$ be given by

$$x = p + q\mathbf{i} + r\mathbf{j} + s\mathbf{k} \ , \ y = \alpha + \beta\mathbf{i} + \gamma\mathbf{j} + \delta\mathbf{k}$$

We calculate first, the formula for x^2. Based on the above rules of multiplication

$$x^2 = p^2 + aq^2 + br^2 - abs^2 + 2p(q\mathbf{i} + r\mathbf{j} + s\mathbf{k})$$

Similarly for y^2,

$$y^2 = \alpha^2 + a\beta^2 + b\gamma^2 - ab\delta^2 + 2\alpha(\beta\mathbf{i} + \gamma\mathbf{j} + \delta\mathbf{k})$$

Then $x^2 + y^2 = 1$ if and only if

$$\begin{cases} p^2 + aq^2 + br^2 - abs^2 + \alpha^2 + a\beta^2 + b\gamma^2 - ab\delta^2 = 1 \\ 2(pq + \alpha\beta) = 0 \\ 2(pr + \alpha\gamma) = 0 \\ 2(ps + \alpha\delta) = 0 \end{cases} \tag{1}$$

From the last three equations of the above system, we notice that

$$\frac{p}{\alpha} = \frac{-\beta}{q} = \frac{-\gamma}{r} = \frac{-\delta}{s}$$

Denote by λ this common ratio, and observe that

$$p = \lambda\alpha \ , \ q = \frac{-\beta}{\lambda} \ , \ r = \frac{-\gamma}{\lambda} \ , \ s = \frac{-\delta}{\lambda}$$

If we then substitute this back in to the first equation of the system, we obtain

$$(\lambda\alpha)^2 + a\left(\frac{-\beta}{\lambda}\right)^2 + b\left(\frac{-\gamma}{\lambda}\right)^2 - ab\left(\frac{-\delta}{\lambda}\right)^2 + \alpha^2 + a\beta^2 + b\gamma^2 - ab\delta^2 = 1$$

After some algebraic manipulation, we see that this expression is equivalent to the following:

$$(\lambda\alpha)^2 + a\beta^2 + b\gamma^2 - ab\delta^2 = \frac{\lambda^2}{\lambda^2+1} \tag{2}$$

Toward proving that the variety X given by this expression is $\mathbb{Q}$-rational, we first show that there exists a single solution with $\mathbb{Q}$ coefficients. This follows from a corollary of the Hasse-Minkowski Theorem. The corollary (actually a Theorem), which can be attributed to Meyer, states the following

Theorem. *Let f be a quadratic form over $\mathbb{Q}$ of rank n for $n \geq 5$. Then $f = 0$ has a rational solution if and only if f is indefinite.*

At first glance, it does not appear that we are in the position to employ Meyer's Theorem; recalling that λ is considered as a constant, the system (2) is an indefinite quadratic form of rank 4, not 5. However, here we reproduce the argument which shows that by homogenizing the expression, we can use Meyer's Theorem.

Lemma. *Let $f(x,y,z,t)$ be an indefinite quadratic form of rank 4 over $\mathbb{Q}$. Then for $\mu \in \mathbb{Q}^\times$, $f(x,y,z,t) = \mu$ has a solution $(x_0,y_0,z_0,t_0) \in \mathbb{Q}^4$.*

Proof. We achieve a solution by homogenizing the expression

$$f(x,y,z,t) = \mu \tag{3}$$

Let u be a new variable, and consider the expression

$$f(x,y,z,t) = \mu u^2 \tag{4}$$

By Meyer's Theorem, $f(x,y,z,t) - \mu u^2 = 0$ has a rational solution (x_0,y_0,z_0,t_0,u_0). There are two possible cases which we consider separately. The first is the case when $u_0 \neq 0$. In this case, set

$$x_1 = \frac{x_0}{u_0} \ , \ y_1 = \frac{y_0}{u_0} \ , \ z_1 = \frac{z_0}{u_0} \ , \ t_1 = \frac{t_0}{u_0}$$

and we have that (x_1,y_1,z_1,t_1) is a rational solution to (3).
In the case when $u_0 = 0$, we let X be the quadric in $\mathbb{P}^4$ given by $f(x,y,z,t) - \mu u^2 = 0$, and let $Y = X \cap Z(u)$. Let $\mathcal{O}$ be a point of Y. Consider the projection map π from $\mathcal{O}$ to $\mathbb{P}^3$, and let $s \in \mathbb{P}^3(\mathbb{Q})$. If we take $T \in \pi^{-1}(s) \setminus Y$, then $T = (x_T, y_T, z_T, t_T, w)$ for some $w \in \mathbb{Q}^\times$, is a point of X. Then we have a new value for u, $u_0' = w$ which is non-zero and we are reduced to the previous case. □

This modification of Meyer's Theorem guarantees that (2) has a rational point. In fact, given a single $\mathbb{Q}$ point we can show (becuase X is a quadric) that it is $\mathbb{Q}$-rational.

Theorem. *Let $V \subset \mathbb{P}^n$ be a variety which is defined by a quadratic polynomial with $\mathbb{Q}$-coefficients. If $P \in V$ is a point with rational coefficients and L_{PA} denotes the line connecting P and some other point $A \in V$, then the map*

$$\varphi : V \dashrightarrow \mathbb{P}^{n-1}$$

defined by

$$\varphi(A) = (L_{PA} \cap \mathbb{P}^{n-1}) \setminus \{P\}$$

is a birational isomorphism defined by rational functions with coefficients in $\mathbb{Q}$, i.e., V is $\mathbb{Q}$-rational.

Proof. Suppose the above hypotheses are satisfied. Let $P = (p_1, \ldots, p_n)$ and $A = (a_1, \ldots, a_n)$. The line L_{PA} connecting P and A is written parametrically as

$$x_i = (a_i - p_i)t + p_i$$

for $i = 0, \ldots, n$. To proceed we will make the following identification

$$\mathbb{P}^{n-1} = \{(z_0 : \ldots : z_n) \in \mathbb{P}^n | z_0 = 0\}$$

Indeed, we are identifying $\mathbb{P}^{n-1}$ as the image of the hyperplane in $\mathbb{P}^n$ with $z_0 = 0$ under the birational isomorphism which sends

$$(0 : z_1 : \ldots : z_n) \mapsto (z_1 : \ldots : z_n)$$

Now, the image $\varphi(A)$ of $A \in V$ under φ is defined to be the intersection of the line L_{PA} with $\mathbb{P}^{n-1}$. By our identification, this happens precisely where $x_0 = 0$;

$$x_0 = (a_0 - p_0)t + p_0 = 0$$

Solving for t,

$$t = \frac{p_0}{p_0 - a_0}$$

Then we have the following expression for the image of A under φ:

$$\varphi(A) = \frac{p_0}{p_0 - a_0}(0 : (a_1 - p_1) : \ldots : (a_n - p_n)) + (0 : p_1 : \ldots : p_n) \tag{5}$$

So therefore we see that the coordinates of $\varphi(A)$ are rational functions with coefficients in $\mathbb{Q}$ (as P was assumed to be a $\mathbb{Q}$ point of V), of the coordinates of A.

We show that φ has rational inverse ψ. With φ defined as above, we will define ψ to be the map

$$\psi : \mathbb{P}^{n-1} \dashrightarrow V$$

which sends a point $B \in \mathbb{P}^{n-1}$ to the second point of intersection of L_{PB} with V. Procedurally, we first form the line L_{PB} joining P and B. Since V is a quadric, L_{PB} can intersect V in only one other point aside from P, so that ψ is well defined. We define $\psi(B)$ to be this second point of intersection. Certainly φ and ψ are inverse to one another. Since φ has the well defined inverse ψ, it is a bijection.

We must show that ψ is in fact a rational function. We give the proof for the case when the variety V is defined by a quadratic polynomial in two variables. The same argument is valid upon moving to an arbitrary number of variables, but the calculations become sufficiently unpleasant in just two variables so as to warrant this shortcut.

Let f be the quadratic polynomial in $\mathbb{Q}[x, y]$ defined by

$$f(x, y) = \alpha x^2 + \beta xy + \gamma y^2 + \delta x + \varepsilon y + \mu$$

and let $V = Z(f)$. Suppose as before, that $P = (p_1 : p_2)$ is a point of V having $\mathbb{Q}$-coefficients, and let $B = (b_1 : b_2)$ be an arbitrary point of $\mathbb{P}^1$. The equation for the line L_{PB} passing through P and B is given by

$$y = \frac{p_2 - b_2}{p_1 - b_1}(x - b_1) + b_2 \tag{6}$$

Let λ denote the slope,

$$\lambda = \frac{p_2 - b_2}{p_1 - b_1}$$

Now, L_{PB} intersects V precisely where

$$f(x, \lambda(x - b_1) + b_2) = \alpha x^2 + \beta x(\lambda(x - b_1) + b_2) + \gamma(\lambda(x - b_1) + b_2)^2 + \delta x + \varepsilon(\lambda(x - b_1) + b_2) + \mu = 0$$

After simplifying this is equivalent to

$$x^2(\alpha + \beta\lambda + \gamma\lambda^2) + x(\beta b_2 - \beta\lambda b_1 - 2\gamma\lambda(\lambda b_1 - b_2) + \delta + \varepsilon\lambda) + (\gamma(\lambda b_1 - b_2)^2 - \varepsilon\lambda b_1 + \varepsilon b_2 + \mu) = 0$$

Now, divide by the coefficient of x^2:

$$x^2 + x\left(\frac{\beta b_2 - \beta\lambda b_1 - 2\gamma\lambda(\lambda b_1 - b_2) + \delta + \varepsilon\lambda}{\alpha + \beta\lambda + \gamma\lambda^2}\right) + \left(\frac{\gamma(\lambda b_1 - b_2)^2 - \varepsilon\lambda b_1 + \varepsilon b_2 + \mu}{\alpha + \beta\lambda + \gamma\lambda^2}\right) = 0 \qquad (7)$$

By our definition, λ was a rational function with $\mathbb{Q}$ coefficients of the coordinates of B. In the coefficient of x above (let's call it η), we have a ratio of $\mathbb{Q}$-linear combinations of powers of λ. Therefore η is also a rational function with $\mathbb{Q}$ coefficients of the coordinates of B. If we let x_1 and x_2 be the two solutions to (7), then we must have that

$$-\eta = x_1 + x_2$$

To see this, we write the above polynomial as a product of the linear factors

$$\begin{aligned} x^2 + x\left(\frac{\beta b_2 - \beta\lambda b_1 - 2\gamma\lambda(\lambda b_1 - b_2) + \delta + \varepsilon\lambda}{\alpha + \beta\lambda + \gamma\lambda^2}\right) + \left(\frac{\gamma(\lambda b_1 - b_2)^2 - \varepsilon\lambda b_1 + \varepsilon b_2 + \mu}{\alpha + \beta\lambda + \gamma\lambda^2}\right) &= (x - x_1)(x - x_2) \\ &= x^2 - x(x_1 + x_2) + x_1 x_2 \end{aligned}$$

But we already know what one of the solutions to the above is! By construction, $x_1 = p_1$. Therefore

$$x_2 = -(p_1 + \eta)$$

But by assumption p_1 is an element of $\mathbb{Q}$. So the expression for x_2 is a rational function of the coordinates of B with $\mathbb{Q}$ coefficients. By construction, x_2 gives the x-coordinate of the image of B under our map ψ. To find an expression for the y-coordinate we simply plug $x = x_2$ into (6) and solve for y. Then the expression giving the y-coordinate of $\psi(B)$ is also a rational function of the coordinates of B with $\mathbb{Q}$ coefficients. Therefore, ψ is also seen to be a $\mathbb{Q}$-rational map. We may finally conclude that

$$\varphi : V \dashrightarrow \mathbb{P}^{n-1}$$

is a $\mathbb{Q}$-rational map. □

It is very nice to be able to say that a particular variety which is studied from a Diophantine perspective is $\mathbb{Q}$-rational. By the existence of a $\mathbb{Q}$-rational map between a variety V and $\mathbb{P}^n$, V has as many $\mathbb{Q}$ points as $\mathbb{P}^n$ does. We would love to be able to combine the theoretical result with a working parameterization which could give most of the $\mathbb{Q}$ points of X over any quaternion algebra over $\mathbb{Q}$, but at the present time we are stuck. More specifically, we do not see how to find a single rational point of X while continuing to leave a and b arbitrary. However, when we specify a and b so that we obtain the most familiar of quaternion algebras, we arrive at a parameterization.

2 Hamiltonian Unit Circle

If we let $a = b = -1$, the quaternion algebra $\left(\frac{-1,-1}{\mathbb{Q}}\right)$ we obtain is none other than the rational Hamiltonians (many refer to the Hamiltonians simply as "quaternions," or even "Hamiltonian quaternions"). The specialized multiplication rule is

$$\mathbf{i}^2 = -1\ ,\ \mathbf{j}^2 = -1\ ,\ \mathbf{ij} = \mathbf{k} = -\mathbf{ji}$$

As before we let $x = p + q\mathbf{i} + r\mathbf{j} + s\mathbf{k}$ and $y = \alpha + \beta\mathbf{i} + \gamma\mathbf{j} + \delta\mathbf{k}$. We aim to parameterize the equation $x^2 + y^2 = 1$. We once more let

$$\lambda = \frac{p}{\alpha} = \frac{-\beta}{q} = \frac{-\gamma}{r} = \frac{-\delta}{s}$$

Then $x^2 + y^2 = 1$ for $x, y \in \left(\frac{-1,-1}{\mathbb{Q}}\right)$ whenever

$$(\lambda\alpha)^2 - \beta^2 - \gamma^2 - \delta^2 - \frac{\lambda^2}{\lambda^2+1} = 0 \tag{8}$$

Note that given a solution $(p, q, r, s, \alpha, \beta, \gamma, \delta)$ of (2) and $\alpha, q, r, s \neq 0$, if λ is defined as above, then $(\lambda, \alpha, \beta, \gamma, \delta)$ solves (8). Vice versa, if $(\lambda, \alpha, \beta, \gamma, \delta)$ is a solution of (8) and $\lambda \neq 0$, then upon letting p, q, r, s be given by

$$p = \lambda\alpha\ ,\ q = \frac{-\beta}{\lambda}\ ,\ r = \frac{-\gamma}{\lambda}\ ,\ s = \frac{-\delta}{\lambda} \tag{9}$$

we get that $(p, q, r, s, \alpha, \beta, \gamma, \delta)$ ia solution of (1) with $a = b = -1$.
To make things simple, and because we only need to produce a single solution to (8), set $\gamma = \delta = 0$. Then we have that

$$(\lambda\alpha)^2 - \beta^2 = \frac{\lambda^2}{\lambda^2+1}$$

which implies that

$$(\lambda\alpha + \beta)(\lambda\alpha - \beta) = 1 \cdot \frac{\lambda^2}{\lambda^2+1}$$

We may choose that $\lambda\alpha + \beta = 1$ and $\lambda\alpha - \beta = \frac{\lambda^2}{\lambda^2+1}$. Therefore $\alpha = \frac{\frac{\lambda^2}{\lambda^2+1}+1}{2\lambda}$ and $\beta = \frac{\frac{\lambda^2}{\lambda^2+1}-1}{2}$. So we have produced a single point P_λ (written as a vector of the form $(\alpha, \beta, \gamma, \delta)$) which solves equation (8):

$$P_\lambda = \left(\frac{\frac{\lambda^2}{\lambda^2+1}+1}{2\lambda}, \frac{1-\frac{\lambda^2}{\lambda^2+1}}{2}, 0, 0\right)$$

Now that we have a formula for finding a single point P_λ, we shall trace lines through P_λ having any rational slope we like, and then shall find the second point of intersection (should it exist) with this line and the hypersurface. But first, it is important to motivate why this is possible. We recall a very basic lemma from algebraic geometry, (see [3]).

Lemma. *Let $f(x_1, x_2, \ldots, x_n) \in k[x_1, x_2, \ldots x_n]$ be of the form $f = f_d + f_{d+1}$ where f_d is a homogeneous polynomial of degree d and f_{d+1} is homogeneous of degree $d+1$, and let $X = Z(f) \subset \mathbb{A}^n$ be the zero locus of f. Let $x_i = v_i t$ define a line $L \subset \mathbb{A}^n$. Then either $L \subset X$, or $L \cap X = \{0, P\}$ for some $P \in \mathbb{A}^n \setminus \{0\}$, or $L \cap X = \{0\}$. Furthermore, if all the coefficients of f and each v_i is rational, then P is rational as well.*

Proof. To find the intersection of L with X, we plug $v_i t$ in for x_i in f and set to zero.

$$0 = f(v_1 t, \ldots, v_n t)$$

Recalling that f has a very particular form, we observe that

$$\begin{aligned}0 &= f_d(v_1t,\dots,v_nt)+f_{d+1}(v_1t,\dots,v_nt)\\ &= t^d f_d(v_1,\dots,v_n)+t^{d+1}f_{d+1}(v_1,\dots,v_n)\\ &= f_d(v_1,\dots,v_n)+tf_{d+1}(v_1,\dots,v_n)\end{aligned}$$

Note that both f_d and f_{d+1} assume constant values when evaluated at $(v_1,\dots,v_n)\in\mathbb{A}^n$, denote these constants by m and n respectively. Then the intersection of L with X is defined by the equation

$$0 = m + tn$$

which as a linear function of t can have infinitely many solutions (case where $L\subset X$), one non-zero solution ($X\cap L=\{0,P\}$), or no non-zero solutions ($X\cap L=\{0\}$). The second assertion in the lemma is a consequence of the fact that the rationals are a field. □

Remark. *It is important to realize that this result remains valid upon shifting the initial point on X away from 0. This modified version of the lemma is in fact the one that we shall directly employ. Essentially we translate 0 to some other initial point Q and then proceed in the same fashion. This translated version of the lemma however, is much less elegantly stated, although the proof remains essentially the same.*

Now with these results at our disposal, we are justified in claiming that every solution to (6) shall be of the form $(\alpha,\beta,\gamma,\delta)$ where

$$\alpha=\frac{\frac{\lambda^2}{\lambda^2+1}+1}{2\lambda}+sz_1\ ,\ \beta=\frac{1-\frac{\lambda^2}{\lambda^2+1}}{2}+sz_2\ ,\ \gamma=sz_3\ ,\ \delta=sz_4 \qquad (10)$$

Here s is the parameter which extends the line $L=P_\lambda+s(z_1,z_2,z_3,z_4)$ away from from the point P in the direction of (z_1,z_2,z_3,z_4). We would like to have an expression of s in terms of z_1,z_2,z_3,z_4, and λ Let us then substitute $\alpha,\beta,\gamma,\delta$ from (10) into our original expression (8). We obtain

$$\left(\frac{\frac{\lambda^2}{\lambda^2+1}+1}{2}+s\lambda z_1\right)^2-\left(\frac{1-\frac{\lambda^2}{\lambda^2+1}}{2}+sz_2\right)^2-(sz_3)^2-(sz_4)^2=\frac{\lambda^2}{\lambda^2+1}$$

which when simplified yields

$$s\left[s\left((\lambda z_1)^2-z_2^2-z_3^2-z_4^2\right)+\lambda z_1\left(\frac{\lambda^2}{\lambda^2+1}+1\right)+z_2\left(\frac{\lambda^2}{\lambda^2+1}-1\right)\right]=0$$

We already know the solution when $s=0$, namely, P_λ. Therefore we are left to conclude that in terms of the parameters z_1,z_2,z_3,z_4, and λ

$$s=\frac{z_2(1-\frac{\lambda^2}{\lambda^2+1})-\lambda z_1(\frac{\lambda^2}{\lambda^2+1}+1)}{(\lambda z_1)^2-z_2^2-z_3^2-z_4^2}$$

For consistency, we rename the parameter λ by z_0, and then state the main result in a theorem.

Theorem. *Let $z_0,z_1,z_2,z_3,z_4\in\mathbb{Q}$, and let $\alpha,\beta,\gamma,\delta\in\mathbb{Q}$ be given by*

$$\begin{aligned}\alpha&=\frac{\frac{z_0^2}{z_0^2+1}+1}{2z_0}+\frac{z_2(1-\frac{z_0^2}{z_0^2+1})-z_0z_1(\frac{z_0^2}{z_0^2+1}+1)}{(z_0z_1)^2-z_2^2-z_3^2-z_4^2}(z_1)\\ \beta&=\frac{1-\frac{z_0^2}{z_0^2+1}}{2}+\frac{z_2(1-\frac{z_0^2}{z_0^2+1})-z_0z_1(\frac{z_0^2}{z_0^2+1}+1)}{(z_0z_1)^2-z_2^2-z_3^2-z_4^2}(z_2)\\ \gamma&=\frac{z_2(1-\frac{z_0^2}{z_0^2+1})-z_0z_1(\frac{z_0^2}{z_0^2+1}+1)}{(z_0z_1)^2-z_2^2-z_3^2-z_4^2}(z_3)\\ \delta&=\frac{z_2(1-\frac{z_0^2}{z_0^2+1})-z_0z_1(\frac{z_0^2}{z_0^2+1}+1)}{(z_0z_1)^2-z_2^2-z_3^2-z_4^2}(z_4)\end{aligned}$$

Furthermore, let

$$p = z_0\alpha \ , \ q = \frac{-\beta}{z_0} \ , \ r = \frac{-\gamma}{z_0} \ , \ s = \frac{-\delta}{z_0}$$

Then the rational Hamiltonians $x = p + q\boldsymbol{i} + r\boldsymbol{j} + s\boldsymbol{k}$ *and* $y = \alpha + \beta\boldsymbol{i} + \gamma\boldsymbol{j} + \delta\boldsymbol{k}$ *solve the equation* $x^2 + y^2 = 1$.
Conversely any rational quaternion solution (x, y) *to* $x^2 + y^2 = 1$ *where* $x = p + q\boldsymbol{i} + r\boldsymbol{j} + s\boldsymbol{k}$ *and* $y = \alpha + \beta\boldsymbol{i} + \gamma\boldsymbol{j} + \delta\boldsymbol{k}$ *is obtained in this way provided* $\alpha, q, r, s \neq 0$.

Proof. We have already proved the first statement.
For the converse, note that any rational Hamiltonian solution (x, y) to $x^2 + y^2 = 1$ defines a point Q satisfying (8). Upon calculating P_λ from λ via (9), one can form the line $L = QP_\lambda$ through P_λ and Q which will have rational slope by the rationality of Q and P_λ. □

Acknowledgements

This project began at the California State University Channel Islands 2012 Math REU. The author is particularly grateful to Dr. Fernando Barrera-Mora for posing such a stimulating question and his personal and academic mentorship. The author would also like to sincerely thank Dr. Alex Buium who has mentored the author on this project at UNM, and for continuing to push the author to develop as a mathematician.

References

[1] Colin Maclachlan and Alan W. Reid. *The Arithmetic of Hyperbolic 3-Manifolds*. Springer, 2003.

[2] Jean-Pierre Serre. *A Course in Arithmetic*. Springer, 1973.

[3] I.R. Shafarevich. *Basic Algebraic Geometry*, volume 1. Springer-Verlag, 1994.