Journal of Integer Sequences, Vol. 15 (2012),
Article 12.2.5

Rational Distance Sets on $x\,y = 1$

Allan J. MacLeod
Statistics, O.R. and Mathematics Group
University of the West of Scotland
High St.
Paisley
Scotland PA1 2BE
allan.macleod@uws.ac.uk

Abstract

We consider the problem of finding sets of points on $xy = 1$, where all of the inter-point distances are rational. The search for such points has links to both congruent and concordant numbers.

1 Introduction

Consider a curve in two dimensions, given in the form $f(x, y) = 0$. Let $P = \{P_1, P_2, \ldots, P_n\}$ be a set of n distinct points. How many of the $n(n-1)/2$ inter-point distances can we make rational? This problem is obviously related to the discussion in section D20 of Guy's book [5].

If the curve is a straight line then there are clearly an infinite number of points, so we usually restrict the points in P to have no more than two on any line.

For the circle $f(x, y) = x^2 + y^2 - 1$, let μ and θ be two distinct angles with $s = \tan\mu$ and $t = \tan\theta$ both rational. Let $P_1 = (\cos 4\mu, \sin 4\mu)$ and $P_2 = (\cos 4\theta, \sin 4\theta)$, then the distance from P_1 to P_2 is

$$\frac{4|s-t||1+st|}{(1+s^2)(1+t^2)}$$

which is clearly rational. Thus there are an infinite number of distinct points on the unit circle with rational distances from each other. This normally forces a second restriction on P - no more than 3 points on any circle.

Very recently, Solymosi and de Zeeuw [9] proved that lines and circles are the only two-dimensional curves that give an infinite number of rational distances.

Even before this, Campbell [1] discussed the problem for the basic parabola $y = x^2$. Based on an early preprint on this investigation, the present author found one of the first examples of a set of 4 acceptable points on the parabola with all 6 inter-point distances rational. Choudhry [2] also discussed this parabola, and showed how to find 5 points with 9 distances rational.

The current work discusses this problem for the rectangular hyperbola

$$x\,y = 1. \tag{1}$$

After this paper was initially submitted, Goins and Mugo [4] released a preprint which is clearly extremely related to this discussion, but from a different perspective. They consider the general conic section

$$axy + bx + cy + d = 0$$

with $a \neq 0$ and $ad \neq bc$. They show that, if the congruent number elliptic curve

$$Y^2 = X^3 - D^2 X \qquad\qquad D = \frac{ad - bc}{2a^2}$$

has rank greater than 0, then there are an infinite number of sets of 4 points on the conic, with the usual conditions on lines and circles.

For the rectangular hyperbola $xy = 1$ we have $D = -1/2$, but it is straight-forward that the elliptic curve $Y^2 = X^3 - X/4$ is equivalent to $V^2 = U^3 - 4U$ which asks if 2 is a congruent number. It is an old result that this is not the case, see Chapter XVI of Dickson's History [3].

So the Goins-Mugo result does not apply in this special case.

2 Basic Results

Let $P = (p, 1/p)$ and $Q = (q, 1/q)$ be on the hyperbola with $p \neq q$. Then the distance is given by

$$|PQ|^2 = (p-q)^2 + (1/p - 1/q)^2 = \frac{(p-q)^2}{p^2q^2}(1 + p^2q^2) \tag{2}$$

Clearly, we can go a long way to making this rational if we restrict p and q to being rational themselves, and we assume from now on that all points are themselves rational. Thus $|PQ|$ will be rational if $1 + p^2q^2 = u^2$ for $u \in \mathbb{Q}$.

Thus, we can assume, without loss of generality, that

$$p\,q = \frac{a^2 - 1}{2a} \equiv \phi(a) \tag{3}$$

where $a \in \mathbb{Q}$.

Let $Q' = (-q, -1/q)$ which is also on the curve, and

$$|PQ'| = \frac{(p+q)^2}{p^2q^2}(1 + p^2q^2)$$

so if $|PQ|$ rational so is $|PQ'|$. Thus if we have a point with negative coordinates, we can always replace it with one with positive ones. We thus assume, from now on, that all points are in the first quadrant.

It should be noted that we do not lose anything by this, since we can never have Q and Q' in P, as this would require $1+q^4$ to be a square, which is impossible as shown by Fermat.

As stated in the introduction, the basic assumption in rational distance sets is that we look for no more than 2 points on a single line or more than 3 points on a single circle. The hyperbola meets $y = ax + b$ where

$$ax^2 + bx - 1 = 0$$

so that any line can only meet the hyperbola at a maximum of 2 points, so the first condition is automatically satisfied.

For a circle, assume $R = (r, 1/r)$ with $r \neq p, q$, then the unique circle through P, Q, R meets the hyperbola at a fourth point with x-coordinate $1/(pqr)$.

3 Three Points

Suppose we have points P, Q, R, then, if the 3 inter-point distances are rational, we require

$$p\,q = \frac{a^2-1}{2a} \qquad p\,r = \frac{b^2-1}{2b} \qquad q\,r = \frac{c^2-1}{2c} \tag{4}$$

with $a, b, c \in \mathbb{Q}$.

Thus

$$\frac{a^2-1}{2ap}\,\frac{b^2-1}{2bp} = \frac{c^2-1}{2c} \tag{5}$$

so that

$$p^2 = \frac{(a^2-1)(b^2-1)c}{2ab(c^2-1)}$$

which implies that there must exist a rational e with

$$e^2 = 2abc(a^2-1)(b^2-1)(c^2-1) \tag{6}$$

Define $a = A/N$ and $b = B/N$, with $A, B, N \in \mathbb{Z}$, so that

$$2ab(a^2-1)(b^2-1) = \frac{2AB(A^2-N^2)(B^2-N^2)}{N^6}$$

and, if we define $f = eN^3$ and $2AB(A^2-N^2)(B^2-N^2) = KM^2$, where K is a square-free integer, we get

$$f^2 = KM^2(c^3-c)$$

Now, define $y = Kf/M$ and $x = Kc$, giving

$$E_K : y^2 = x^3 - K^2x \tag{7}$$

This is an elliptic curve, and, in fact, is the elliptic curve related to the congruent number problem. This forms the basis for the book by Koblitz [6].

The curve E_K has the obvious rational points $(0,0),(K,0),(-K,0)$, which give $c = 0,1,-1$ respectively, which cause problems with the identity $qr = 2c/(c^2-1)$. Thus to have a practical solution we need another rational point, which means that the rank of E_K must be greater than 0.

The famous result of Tunnell [10] shows that this will be the case if K is $\equiv 5,6,7 \bmod 8$, and possibly when K is $\equiv 1,2,3 \bmod 8$.

For example, when $a = 3/2, b = 4/3$, we have $2AB(A^2-N^2)(B^2-N^2) = 181440 = 35 \times 72^2$, so that $K = 35, M = 72$. The curve E_{35} has rank 0 and so there are no trios of points in this case.

Alternatively, when $a = 4/3, b = 2/1$, we have $2AB(A^2-N^2)(B^2-N^2) = 9072 = 7 \times 36^2$, giving $K = 7, M = 36$. The curve E_7 has rank 1 with, for example, the point $(25,120)$. This gives $c = 25/7$, and $pq = 7/24$ and $pr = 3/4$ so that

$$qr = \frac{21}{96p^2} = \frac{288}{175}$$

leading to $p = 35/96$, $q = 4/5$ and $r = 72/35$.

We now analyse what happens when we add torsion points to points of infinite order. As stated, the curve has 3 finite torsion points $(0,0),(K,0),(-K,0)$. Let (g,h) be a point of infinite order giving a value of c, which we call c_1, and leading to the 3 points on the hyperbola $(p_1, 1/p_1)$, $(q_1, 1/q_1)$ and $(r_1, 1/r_1)$.

Forming $(g,h)+(0,0)$ gives $x = -K^2/g$, which gives a new value of c given by $c_2 = -1/c_1$. Thus $c_2/(c_2^2-1) = c_1/(c_1^2-1)$ and so $p_2 = p_1$, giving the same set of three points.

Forming $(g,h)+(K,0)$ gives $x = K(g+K)/(g-K)$ so $c_3 = (c_1+1)/(c_1-1)$ and $p_3 = p_1(c_1^2-1)/2c_1$. Thus $q_3 = 1/r_1$ and $r_3 = 1/q_1$, and we have a different set of three points $(1/r_1, r_1)$, $(1/q_1, q_1)$ and $(p_3, 1/p_3)$. We can invert each of the x-coordinates to give the set $(q_1, 1/q_1)$, $(r_1, 1/r_1)$ and $(1/p_3, p_3)$. Note, however, that

$$p_1 q_1 r_1 \frac{1}{p_3} = p_1 \, \frac{(a^2-1)}{2ap_1} \, \frac{(b^2-1)}{2bp_1} \, \frac{2c_1}{(c_1^2-1)p_1} = 1$$

so the four points actually lie on a circle.

Similarly, if we add $(g,h)+(-K,0)$, we get the same situation.

Finally, in this section, note that, if p,q,r give 3 points with rational distances, the point $1/(pqr)$ (on the circle through the three points) is at a rational distance from the other points.

4 Four Points

Suppose we wish a fourth point $S = (s, 1/s)$ to have a rational distance to each of P, Q, R. We assume $pqrs \neq 1$, so that the four points do not lie on a circle.

Then we require

$$1 + p^2s^2 = \square \qquad 1 + q^2s^2 = \square \qquad 1 + r^2s^2 = \square \tag{8}$$

Consider the first two conditions, noting that p, q, r are known quantities. We have

$$p\,s = \frac{f^2-1}{2f} \qquad\qquad q\,s = \frac{g^2-1}{2g} \tag{9}$$

with $f, g \in \mathbb{Q}$, giving

$$p\,f(g^2-1) - q(f^2-1)g = 0$$

This quadratic must have rational roots, so the discriminant must be a rational square, giving

$$h^2 = q^2(f^2-1)^2 + 4p^2f^2$$

with $h \in \mathbb{Q}$, and so, defining $Y = qh, X = qf$, we have the quartic

$$Y^2 = X^4 + (4p^2 - 2q^2)X^2 + q^4 \tag{10}$$

This quartic has an obvious rational point $(0, q^2)$, so is birationally equivalent to the elliptic curve

$$V^2 = U(U+p^2)(U+q^2) \tag{11}$$

with $f = V/(q(U+p^2))$.

Since $p, q \in \mathbb{Q}$, express $p = J/I$, $q = L/I$, $U = Z/I^2$, $V = W/I^3$ with $I, J, L \in \mathbb{Z}$, so that

$$W^2 = Z(Z+J^2)(Z+L^2) \qquad , \qquad f = \frac{W}{L(Z+J^2)} \tag{12}$$

This is the elliptic curve for a specific subset of Euler's concordant forms, namely $x^2+J^2y^2 = \square$, $x^2+L^2y^2 = \square$, as discussed by Ono [7]. The curve has

(a) 3 points of order 2, at $(0,0), (-J^2,0), (-L^2,0)$,

(b) 4 points of order 4 at $(JL, \pm JL(J+L))$ and $(-JL, \pm JL(J-L))$,

(c) the point at infinity.

It is even possible to have points of order 8, so the torsion subgroup is usually $\mathbb{Z}_2 \times \mathbb{Z}_4$ but could be $\mathbb{Z}_2 \times \mathbb{Z}_8$. None of these torsion points lead to a non-trivial value of s.

Note that r is already a solution to equation (9), which gives a point on this curve. From equation (4), let $X_1 = q\,b$ and (X_1, Y_1) be the solution of (10) then

$$U = \frac{X_1^2 + Y_1 - q^2}{2}$$

gives a point on (10), meaning that the curves all have rank at least 1.

We now investigate the effect of adding torsion points to a point on the curve. Suppose (Z_0, W_0) is a point on the elliptic curve so that $W_0^2 = Z_0(Z_0+J^2)(Z_0+L^2)$, and let $f_0 = W_0/(L(Z_0+J^2))$, from which we find a value for s.

Adding $(0,0)$ gives $Z_1 = J^2L^2/Z_0$ and $W_1 = -J^2L^2W_0/Z_0^2$ leading to

$$f_1 = -\frac{LW_0}{Z_0(Z_0+L^2)} = -\frac{L(Z_0+J^2)}{W_0} = -\frac{1}{f_0}$$

Adding $(-J^2, 0)$ gives

$$Z_2 = \frac{-J^2(Z_0 + L^2)}{Z_0 + J^2} \qquad , \qquad W_2 = \frac{W_0 J^2(L^2 - J^2)}{(Z_0 + J^2)^2}$$

which just gives $f_2 = -f_0$.

Adding $(-L^2, 0)$ gives

$$Z_3 = \frac{-L^2(Z_0 + J^2)}{Z_0 + L^2} \qquad , \qquad W_3 = \frac{W_0 L^2(J^2 - L^2)}{(Z_0 + L^2)^2}$$

which just gives $f_3 = 1/f_0$.

These 3 new values of f just lead to the same values of s. If, however, we add the points of order 4 we do get a different point.

To understand the effect of adding the points of order 4, it is simpler to use the elliptic curve given in equation (10). Let (U_0, V_0) be a non-torsion rational point on the curve, which gives

$$s_0 = \frac{U_0^2 - p^2q^2}{2pqV_0} \tag{13}$$

Now, consider adding the point of order 4 given by $(pq, pq(p+q))$. Using a symbolic algebra package gives

$$s_4 = \frac{2(U_0^2 + U_0(p^2+q^2) - V_0(p+q) + p^2q^2)(U_0(p+q) - V_0)}{-(U_0 - pq)(U_0 + pq)(U_0^2 + U_0(2p^2 + 2pq + 2q^2) - 2V_0(p+q) + p^2q^2)}$$

which does not seem too helpful.

Using $V_0^2 = U_0^3 + (p^2+q^2)U_0^2 + p^2q^2U_0$, however, allows us to simplify this to

$$s_4 = \frac{2V_0}{U_0^2 - p^2q^2} = \frac{1}{pqs_0} \tag{14}$$

which is just the fourth point on the hyperbola and the circle through p, q, s. The other points of order 4 also give this value, which we disallow.

5 Numerical Results

To find size 3 and 4 rational distance sets, we need to determine points of infinite order on both types of elliptic curves. Determining the rank of an elliptic curve and a full set of generators is a non-trivial process. We avoid this problem, and use both a simple search procedure and a very simple descent procedure to determine independent points of infinite order moderately quickly. All the programming was done using the software package Pari.

For the search, we determine the minimal form of the curve and search this for points with integer coordinates up to a specified size. Clearly, we must restrict the search on the infinite component, and we often must also do this on the closed finite component. Thus it is possible that we might miss a possible generator.

For the descent, we note that the curves we must search are of the general form

$$y^2 = x^3 + Gx^2 + Hx \tag{15}$$

A rational point on such curves has form $(du^2/v^2, duw/v^3)$ where d is squarefree and $\gcd(d, v) = 1$. Substituting gives

$$dw^2 = d^2u^4 + dGu^2v^2 + Hv^4$$

so that $d|H$, allowing us to find possible values of d easily.

We have

$$4dw^2 = 4d^2u^4 + 4dGu^2v^2 + 4Hv^4 = (2du^2 + Gv^2)^2 - (G^2 - 4H)v^4$$

and we find that, in both equations (7) and (12), the corresponding values of G and H give $G^2 - 4H = \Box = C^2$ say.

Thus, define $Z = 2w$, $X = 2du^2 - Gv^2$ and $Y = Cv^2$, leading to $X^2 = Y^2 + dZ^2$. This has a simple parametric solution $Y = p^2 - dq^2$, $Z = 2pq$ and $X = p^2 + dq^2$. This gives

$$\frac{u^2}{v^2} = \frac{(C-G)p^2 + d(C+G)q^2}{2d(p^2 - dq^2)} \tag{16}$$

We generate small-size pairs (p, q), with $\gcd(p, q) = 1$, compute the right-hand-side of this ratio and test whether it is square. We find several non-integer point of infinite order using this approach, which are usually generators, but might not be.

Combining the above two approaches, we find k independent points of infinite order $G_1, \ldots, G_k$ and then compute

$$a_1G_1 + \ldots + a_kG_k + T \tag{17}$$

with T a torsion-point and $|a_i|$ less than some preset limit. Using this allows us to find, after a reasonable amount of computation, the following table of size 4 rational distance sets on $x\,y = 1$.

TABLE 1
Size 4 rational distance sets

p	q	r	s
77/340	15/56	96/55	77/18
14/65	60/77	462/325	26/9
11/60	117/418	5681/17490	80/39
27/80	320/231	319/168	55/19
287/1380	595/1254	715/238	99/10
3/11	1275/2288	319/416	52/45
7/78	145/264	25/28	864/235
437/702	63/46	8/5	697/210
9/34	9675/16898	208/81	3689/390
207/434	221/300	160/161	91/24
21/110	424/1071	39/62	24/5
2/9	876/1771	4125/5168	884/495
715/2352	1548/16575	34/33	28/17

The method of Choudhry, for finding larger sets, is based on the fact that (s, s^2) and (t, t^2) have a rational distance if $s + t = \phi(k)$ for $k \in \mathbb{Q}$. For the hyperbola, $(s, 1/s)$ and $(t, 1/t)$ have a rational distance if $s\,t = \phi(k)$. So we move from an additive approach to a multiplicative one. This makes finding relations such as those given by Choudhry much more difficult.

6 Acknowledgement

The author would like to express sincere thanks to the anonymous referee and the Editor for several very helpful comments on both submissions of this paper.

References

[1] G. Campbell, Points on $y = x^2$ at rational distance, *Math. Comp.*, **73** (2004), 2093–2108.

[2] A. Choudhry, Points at rational distances on a parabola, *Rocky Mt. J. Math.*, **36** (2006), 413–424.

[3] L. E. Dickson, *History of the Theory of Numbers Vol. 2: Diophantine Analysis*, Chelsea, 1971.

[4] E. H. Goins and K. Mugo, Points on hyperbolas at rational distance, preprint, http://arxiv.org/abs/1108.0690.

[5] R. K. Guy, *Unsolved Problems in Number Theory*, 3rd edition, Springer, 2004.

[6] N. Koblitz, *Introduction to Elliptic Curves and Modular Forms*, Springer, 1984.

[7] K. Ono, Euler's concordant forms, *Acta Arith.*, **65** (1996), 101–123.

[8] J. H. Silverman and J. Tate, *Rational Points on Elliptic Curves*, Springer, 1992.

[9] J. Solymosi and F. de Zeeuw, On a question of Erdös and Ulam, *Disc. & Comp. Geom.*, **43** (2010), 393–401.

[10] J. B. Tunnell, A classical Diophantine problem and modular forms of weight 3/2, *Invent. Math.* **72** (1983), 323–334.

2010 *Mathematics Subject Classification*: Primary 11D25; Secondary 11Y50, 11G05.
Keywords: hyperbola, rational distance set, elliptic curve, congruent number, concordant form.

Received April 21 2011; revised versions received October 10 2011; January 10 2012. Published in *Journal of Integer Sequences*, January 14 2012.

Return to Journal of Integer Sequences home page.