Bull. Aust. Math. Soc. **114** (2026), 237–247
doi:10.1017/S0004972725100944

THE FERMAT–MERSENNE PROBLEM ON PYTHAGOREAN TRIPLES

HENRY (MAYA) ROBERT THACKERAY

(Received 17 November 2025; accepted 22 December 2025; first published online 2 March 2026)

Abstract

In the 17th century, a letter from Fermat to Mersenne considered the problem of finding the Pythagorean triples in which the hypotenuse and the sum of the other two sides are squares. We call this question the Fermat–Mersenne problem. Number-theoretic solutions of the problem are known, but they are complicated. We solve the Fermat–Mersenne problem by using a geometric approach that provides new insight. The argument involves stereographically projecting points onto an elliptic curve and applying complex multiplication on that curve.

2020 *Mathematics subject classification*: primary 11D25; secondary 11G05, 14H52, 14N05.

Keywords and phrases: Pythagorean triple, elliptic curve, stereographic projection, Fermat.

1. Introduction

We define a *Pythagorean triple* to be a triple (a, b, c) of integers such that

$$a^2 = b^2 + c^2 \quad \text{and} \quad a > 0.$$

Pythagorean triples have been a subject of study by mathematicians for millennia.

In the 17th century, a letter from Fermat to Mersenne considered the problem of finding the Pythagorean triples in which a and $b + c$ are squares [4, page 67]. We call this question the Fermat–Mersenne problem. In the letter, Fermat noted the surprising fact that of all (nontrivial) solutions, a solution with the smallest possible value of a is given by

$$(4687298610289, 1061652293520, 4565486027761).$$

Number-theoretic solutions of the Fermat–Mersenne problem are known (see [2] and [4, Section 12]); however, the arguments are complicated and the reader may be left wondering why they work.

In this paper, we solve the Fermat–Mersenne problem by using a geometric approach that provides new insight. Some of the relevant ideas appear in a textbook of Silverman on elliptic curves [6, pages 327–329], but no previous applications of

© The Author(s), 2026. Published by Cambridge University Press on behalf of Australian Mathematical Publishing Association Inc.

https://doi.org/10.1017/S0004972725100944 Published online by Cambridge University Press

these ideas in the literature explicitly focus on the Fermat–Mersenne problem, to the author's knowledge.

To motivate the strategy of this paper, let us consider the well-known simpler question of finding all Pythagorean triples. There are at least two standard approaches to the problem: a number-theoretic approach and a geometric approach. Both approaches start by dividing all entries of a general Pythagorean triple by their greatest common divisor; this converts the triple to a *primitive* Pythagorean triple, that is, a Pythagorean triple (a, b, c) where $\gcd(a, b, c) = 1$.

The number-theoretic approach [4, Section 2] uses the factorisation given by $c^2 = (a - b)(a + b)$ to show that each of the numbers $a \pm b$ is a square (respectively, twice a square) if c is odd (respectively, even). A variation on that theme uses the factorisation $a^2 = (b - ci)(b + ci)$ in $\mathbb{Z}[i]$ instead [3, pages 1–2].

In the geometric approach [6, page 13], the primitive Pythagorean triples correspond to rational points on the unit circle, which are transformed into rational points on a projective line by stereographic projection.

The Fermat–Mersenne problem asks for the Pythagorean triples (a, b, c) such that a and $b + c$ are squares. The number-theoretic approaches to the problem ([2] and [4, Section 12]) can be viewed as adaptations of the number-theoretic approach for general Pythagorean triples. In this paper, we adapt the geometric approach instead. We divide out by positive common factors, associate the resulting primitive solutions with rational points on a curve C and apply stereographic projection.

This time, the image of the projection will be an elliptic curve E of rank 1 instead of a projective line. The point from which we project will not be defined over $\mathbb{R}$; to compensate for that, we apply a tweak that involves complex multiplication on E so that the rational points on C correspond to the rational points on E.

The Fermat–Mersenne problem has infinitely many solutions because the elliptic curve E has infinitely many rational points. Apart from providing that insight, the geometric approach has a further advantage over the number-theoretic approach. The number-theoretic arguments involve chains of solutions that can have negative values of b or c, and no way is given to determine whether all of the entries in, say, the 10^{10}th solution in a chain are positive, apart from actually calculating the infeasibly large solution or doing something tantamount to that. In the geometric approach, the question 'Are all of the entries in the nth solution in a chain positive?' has a beautiful and unexpected answer that emerges organically from the geometry, and we can answer the question without calculating the nth solution. To the author's knowledge, that has not been done before.

We assume that the reader has background knowledge of abstract algebra, projective geometry and elliptic curves. Some of our notation is taken and/or adapted from Silverman's books [5, 6] on elliptic curves. Several routine manipulations involving points in projective space, as well as other calculations, are detailed in the supplementary material available at https://github.com/ThackerayMayaR/FermatMersenneAG. SageMath Version 10.0 (release date 20 May 2023) was used as an advanced calculator (for example, to determine multiples of points on an elliptic curve).

https://doi.org/10.1017/S0004972725100944 Published online by Cambridge University Press

We use the following formal definition of stereographic projection. In a projective space $\mathbb{P}^n$, let H be a hyperplane, let C be a smooth curve and let P_0 be a point that is on C but not on H. For each point P on C, we let L_P be the projective line through P_0 and P, except that if $P = P_0$, then we let L_P be the tangent line to C at P. The stereographic projection through P_0 from C to H is the map from C to H that sends each point P on C to the intersection of L_P and H.

2. Warmup: general Pythagorean triples

We briefly describe the standard argument [6, page 13] that uses stereographic projection to find all Pythagorean triples. Although the argument is well known, we include it here because the argument for the Fermat–Mersenne problem follows the same structure, so the simpler problem is worth keeping in mind.

For any Pythagorean triple (a, b, c), if $d = \gcd(a, b, c)$, then $(a/d, b/d, c/d)$ is a primitive Pythagorean triple. The Pythagorean triples are precisely the triples of the form (ka, kb, kc), where k is a positive integer and (a, b, c) is a primitive Pythagorean triple.

In the projective space $\mathbb{P}^2$ of points $(X_0 : X_1 : X_2)$, let C be the curve defined by $X_0^2 = X_1^2 + X_2^2$. The intersection of the affine plane $X_0 \neq 0$ with C is the affine unit circle $1 = X^2 + Y^2$, where the point (X, Y) in $\mathbb{A}^2$ corresponds to the projective point $(X_0 : X_1 : X_2) = (1 : X : Y)$ in $\mathbb{P}^2$. It is easily checked that the map $(a, b, c) \mapsto (a : b : c)$ from the set of primitive Pythagorean triples to $C(\mathbb{Q})$ is a bijection.

The point $(1 : 0 : 1)$ is on C. In $\mathbb{P}^2$, consider the stereographic projection through $(1 : 0 : 1)$ from C to the projective line $X_2 = 0$. For each point P on C, the projection sends P to a point $(t_0 : t_1 : 0)$ and we let $f(P)$ be the point $(t_0 : t_1)$ in $\mathbb{P}^1$. Calculations show that the map f is given by

$$f : C \to \mathbb{P}^1, \quad (X_0 : X_1 : X_2) \mapsto \left\{ \begin{array}{l} (X_0 - X_2 : X_1) \\ \quad \text{if } (X_0 : X_1 : X_2) \neq (1 : 0 : 1) \\ (X_1 : X_0 + X_2) \\ \quad \text{if } (X_0 : X_1 : X_2) \neq (1 : 0 : -1) \end{array} \right\}$$

and that f is an isomorphism over $\mathbb{Q}$; its inverse is given by

$$f^{-1} : \mathbb{P}^1 \to C, \quad (T_0 : T_1) \mapsto (T_0^2 + T_1^2 : 2T_0T_1 : T_1^2 - T_0^2).$$

(See Section 2 of the supplementary material.) It follows that f restricts to a bijection from $C(\mathbb{Q})$ to $\mathbb{P}^1(\mathbb{Q})$.

Therefore, the map $(a, b, c) \mapsto f((a : b : c))$ from the set of primitive Pythagorean triples to $\mathbb{P}^1(\mathbb{Q})$ is a bijection. In the reverse direction, if t_0 and t_1 are coprime integers that are not both zero, then it can be checked that the point $(t_0 : t_1) \in \mathbb{P}^1(\mathbb{Q})$ corresponds to the primitive Pythagorean triple $(t_0^2 + t_1^2, 2t_0t_1, t_1^2 - t_0^2)$ (if $t_0 + t_1$ is odd) or $((t_0^2 + t_1^2)/2, t_0t_1, (t_1^2 - t_0^2)/2)$ (if $t_0 + t_1$ is even). For a primitive Pythagorean triple (a, b, c) and the corresponding point $(t_0 : t_1) \in \mathbb{P}^1(\mathbb{Q})$, all entries of (a, b, c) are positive if and only if $t_0 \neq 0$ and $t_1/t_0 > 1$.

https://doi.org/10.1017/S0004972725100944 Published online by Cambridge University Press

3. The Fermat–Mersenne problem

We now consider the Fermat–Mersenne problem. To be explicit, we define a *Fermat–Mersenne tuple* to be a 5-tuple $(a, b, c, m, n) \in \mathbb{Z}^5$ such that

$$a^2 = b^2 + c^2, \quad a = m^2, \quad b + c = n^2 \quad \text{and} \quad n > 0.$$

To solve the Fermat–Mersenne problem, it is enough to find all Fermat–Mersenne tuples. To obtain the corresponding Pythagorean triples (a, b, c), we discard m and n. It is easily checked that each Pythagorean triple (a, b, c) obtained in this way comes from exactly two Fermat–Mersenne tuples, which are of the form (a, b, c, m, n) and $(a, b, c, -m, n)$ for some m and n.

For a Fermat–Mersenne tuple (a, b, c, m, n), if some positive integer p is prime and divides $\gcd(m, n)$, then $(a/p^2, b/p^2, c/p^2, m/p, n/p)$ is a Fermat–Mersenne tuple. (Note that p^4 divides $n^4 - m^4 = (b + c)^2 - (b^2 + c^2) = 2bc$, so p^3 divides bc, so p^2 divides b or p^2 divides c, but p^2 divides $n^2 = b + c$, so p^2 divides b and p^2 divides c.) We define a *primitive Fermat–Mersenne tuple* to be a Fermat–Mersenne tuple (a, b, c, m, n) such that $\gcd(m, n) = 1$. The Fermat–Mersenne tuples are precisely the tuples of the form $(k^2a, k^2b, k^2c, km, kn)$, where k is a positive integer and (a, b, c, m, n) is a primitive Fermat–Mersenne tuple.

To find all primitive Fermat–Mersenne tuples, we associate them with the rational points of a certain projective curve and we show that those points correspond to the rational points of a certain elliptic curve.

4. The projective curve

In the space $\mathbb{P}^3$ of points given by $(Y_0 : Y_1 : Y_2 : Y_3)$, consider the smooth curve C with the two defining equations $Y_0Y_1 = Y_2^2$ and $2Y_1^2 = Y_0^2 + Y_3^2$ (see [6, pages 22–23]). The intersection of the affine 3-space $Y_0 \neq 0$ with C is given by the equations $X = Y^2$ and $2Y^4 = 1 + Z^2$, where the point (X, Y, Z) in $\mathbb{A}^3$ corresponds to the projective point $(Y_0 : Y_1 : Y_2 : Y_3) = (1 : X : Y : Z) \in \mathbb{P}^3$. The two points of C that satisfy $Y_0 = 0$ are the points $(0 : 1 : 0 : \pm\sqrt{2})$, neither of which is in $C(\mathbb{Q})$.

PROPOSITION 4.1. *The map* $(a, b, c, m, n) \mapsto (1 : m^2/n^2 : m/n : (b - c)/n^2)$ *from the set of primitive Fermat–Mersenne tuples to* $C(\mathbb{Q})$ *is a bijection. For each point* $(1 : y^2 : y : z)$ *in* $C(\mathbb{Q})$*, the corresponding primitive Fermat–Mersenne tuple has all of its entries positive if and only if* $0 < y < 1$.

PROOF. We show the map is well defined. If (a, b, c, m, n) is a primitive Fermat–Mersenne tuple, then the rational numbers $y = m/n$ and $z = (b - c)/n^2$ satisfy

$$2y^4 = \frac{2m^4}{n^4} = \frac{2a^2}{n^4} = \frac{2(b^2 + c^2)}{n^4} = \frac{(b + c)^2 + (b - c)^2}{n^4} = 1 + z^2,$$

so $(1 : y^2 : y : z) \in C(\mathbb{Q})$.

We show the map is injective. Let the point $(Y_0 : Y_1 : Y_2 : Y_3)$ in $C(\mathbb{Q})$ be the image of some primitive Fermat–Mersenne tuple (a, b, c, m, n) under the map. The

https://doi.org/10.1017/S0004972725100944 Published online by Cambridge University Press

integers m and n are uniquely determined by the conditions $n > 0$, $\gcd(m, n) = 1$ and $Y_2/Y_0 = m/n$. The integers a, b and c are uniquely determined since $a = m^2$, $b = (n^2/2)(1 + (Y_3/Y_0))$ and $c = (n^2/2)(1 - (Y_3/Y_0))$.

We show the map is surjective. Let the point $P = (Y_0 : Y_1 : Y_2 : Y_3)$ be in $C(\mathbb{Q})$. Now, P must be of the form $(1 : y^2 : y : z)$ for some rational numbers y and z such that $2y^4 = 1 + z^2$. Let (m, n) be the unique pair of integers such that $n > 0$, $\gcd(m, n) = 1$ and $y = m/n$. Let $d = n^2 z$. The number d is in $\mathbb{Q}$ and

$$d^2 = n^4 z^2 = n^4(2y^4 - 1) = 2m^4 - n^4 \in \mathbb{Z},$$

so d is an integer with the same parity as n. It is easily checked that

$$\left(m^2, \frac{n^2 + d}{2}, \frac{n^2 - d}{2}, m, n\right)$$

is a primitive Fermat–Mersenne tuple that is sent to P by the map.

For a primitive Fermat–Mersenne tuple (a, b, c, m, n) and the corresponding point $(1 : y^2 : y : z)$ in $C(\mathbb{Q})$: n is always positive; $y > 0$ if and only if $m > 0$, in which case $a = m^2 > 0$; and we have $b > 0$ and $c > 0$ simultaneously if and only if $|z| < 1$ if and only if $|y| < 1$. □

5. The elliptic curve

In the space $\mathbb{P}^2$ of points given by $(X_0 : X_1 : X_2)$, consider the elliptic curve E with the defining equation $X_0 X_2^2 = X_1(X_1^2 + (1/2)X_0^2)$. The intersection of the affine plane $X_0 \neq 0$ with E is given by $Y^2 = X^3 + (1/2)X$, where (X, Y) corresponds to the point $(X_0 : X_1 : X_2) = (1 : X : Y) \in \mathbb{P}^2$. The one point of E that satisfies $X_0 = 0$ is the point $O = (0 : 0 : 1)$, which we take as the identity for the group law on E as usual.

The elliptic curve E has complex multiplication by $\mathbb{Z}[i]$, where the multiply-by-i map

$$[i] : E \to E, \quad (X_0 : X_1 : X_2) \mapsto (X_0 : -X_1 : iX_2)$$

is an isomorphism over $\mathbb{Q}(i)$. For each $z \in \mathbb{Z}[i]$, we write the multiply-by-z map as $[z] : E \to E : P \mapsto [z]P$ (see [5, page 107], [6, pages 69–70] and, more generally, the introductions to the theory of complex multiplication of elliptic curves in [5, Ch. 2] and [6, pages 425–429]).

The two points $R = (2 : -1 - i : 1 - i)$ and $(1 : 0 : 0)$ are on E, and they satisfy $[2]R = (8 : 2 : 3)$ and $[2](1 : 0 : 0) = O$. Each of the two maps

$$\mathbb{Z} \times (\mathbb{Z}/2\mathbb{Z}) \to E(\mathbb{Q}), \quad (t, u + 2\mathbb{Z}) \mapsto [t](8 : 2 : 3) + [u](1 : 0 : 0),$$
$$\mathbb{Z} \times \mathbb{Z} \times (\mathbb{Z}/2\mathbb{Z}) \to E(\mathbb{Q}(i)), \quad (s, t, u + 2\mathbb{Z}) \mapsto [s + ti]R + [u](1 : 0 : 0)$$

is a group isomorphism. (A proof may be given using the techniques of [6, Example 4.5 in Section III.4, Sections VII.1–3 and Proposition 4.9 in Section X.4]. This may also be checked using SageMath and a database like LMFDB; the elliptic curve E is isomorphic to the curve with Cremona label 256b2 [7]. See Section 3 of the supplementary material.)

https://doi.org/10.1017/S0004972725100944 Published online by Cambridge University Press

6. Correspondences between the two curves

The point $(1 : 0 : 0 : i)$ is on C. Starting with a point $P = (y_0 : y_1 : y_2 : y_3)$ on C, apply stereographic projection in $\mathbb{P}^3$ through $(1 : 0 : 0 : i)$ from C to the projective plane $Y_3 = 0$. We obtain a point $(x_0 : x_1 : x_2 : 0)$; let this correspond to the point $f(P) = (x_0 : x_1 : x_2)$ in $\mathbb{P}^2$.

PROPOSITION 6.1. *The map $f : C \to E$ is an isomorphism over $\mathbb{Q}(i)$.*

PROOF. Calculations show that f sends each point in C to a point in E, that f is given by

$$f : C \to E, \quad (Y_0 : Y_1 : Y_2 : Y_3) \mapsto \left\{ \begin{array}{l} (Y_0 + iY_3 : Y_1 : Y_2) \\ \quad \text{if } (Y_0 : Y_1 : Y_2 : Y_3) \neq (1 : 0 : 0 : i) \\ (2Y_1Y_2 : Y_2(Y_0 - iY_3) : Y_0(Y_0 - iY_3)) \\ \quad \text{if } (Y_0 : Y_1 : Y_2 : Y_3) \text{ is neither} \\ \quad (1 : 0 : 0 : -i) \text{ nor } (0 : 1 : 0 : \pm\sqrt{2}) \end{array} \right\}$$

and that the map

$$f^{-1} : E \to C, \quad (X_0 : X_1 : X_2) \mapsto \left\{ \begin{array}{l} (2X_1^2 + X_0^2 : 2X_0X_1 : 2X_0X_2 : i(2X_1^2 - X_0^2)) \\ \quad \text{if } (X_0 : X_1 : X_2) \neq (0 : 0 : 1) \\ (X_2^2 : X_1^2 : X_1X_2 : i(X_2^2 - X_0X_1)) \\ \quad \text{if } (X_0 : X_1 : X_2) \neq (1 : 0 : 0) \end{array} \right\}$$

is the inverse of f. (See Sections 4.1–4.3 of the supplementary material.) The maps f and f^{-1} are defined over $\mathbb{Q}(i)$, and the result follows. (The map f can be obtained from the map ϕ^{-1} in [6, pages 327–329] with $d = -1$, $a = 0$ and $b = 1/2$ by rearranging and renaming co-ordinates, post-composing with $[i]$ and taking the projective closure where necessary.) □

Table 1 lists some points on E and on C that correspond under f. It is easily checked that the maps

$$\begin{aligned} q : C \to C, \quad & (Y_0 : Y_1 : Y_2 : Y_3) \mapsto (Y_0 : Y_1 : -Y_2 : -Y_3), \\ r : C \to C, \quad & (Y_0 : Y_1 : Y_2 : Y_3) \mapsto (Y_0 : -Y_1 : iY_2 : Y_3) \end{aligned}$$

are isomorphisms over $\mathbb{Q}(i)$, and that every point P on C satisfies

$$f(P) + (1 : 0 : 0) = f(q(P)) \quad \text{and} \quad [i](f(P)) = f(r(P)).$$

(See Section 4.4 of the supplementary material.)

We would like to find an isomorphism from C to E over $\mathbb{Q}$ instead of over $\mathbb{Q}(i)$ so that points in $C(\mathbb{Q})$ correspond to points in $E(\mathbb{Q})$. Table 1 suggests that we consider the map $g : C \to E, P \mapsto [-i](f(P)) - R$ (which sends the rational points $(1 : 1 : 1 : -1)$ and $(1 : 169 : -13 : 239)$ on C to respectively the rational points O and $(8 : 2 : 3)$ on E).

PROPOSITION 6.2. *The map g is an isomorphism over $\mathbb{Q}$, so g restricts to a bijection from $C(\mathbb{Q})$ to $E(\mathbb{Q})$.*

https://doi.org/10.1017/S0004972725100944 Published online by Cambridge University Press

TABLE 1. Points on E and points on C that correspond under f. The point R is the point $(2 : -1 - i : 1 - i)$ in $E(\mathbb{Q}(i))$. Each point that is defined over $\mathbb{Q}$ is marked with an asterisk.

s	t	$[s + ti]R \in E$	$f^{-1}([s + ti]R) \in C$
0	−3	$(4394 : 13 - 3107i : 1 - 239i)$	$*\ (1 : 169 : 13 : 239)$
0	−2	$(8 : -2 : -3i)$	$(9 : -4 : -6i : -7i)$
0	−1	$(2 : 1 + i : -1 - i)$	$*\ (1 : 1 : -1 : -1)$
−3	0	$(4394 : -13 + 3107i : -239 - i)$	$(1 : -169 : -13i : 239)$
−2	0	$*\ (8 : 2 : -3)$	$(9 : 4 : -6 : -7i)$
−1	0	$(2 : -1 - i : -1 + i)$	$(1 : -1 : i : -1)$
0	0	$*\ (0 : 0 : 1)$	$(1 : 0 : 0 : i)$
1	0	$(2 : -1 - i : 1 - i)$	$(1 : -1 : -i : -1)$
2	0	$*\ (8 : 2 : 3)$	$(9 : 4 : 6 : -7i)$
3	0	$(4394 : -13 + 3107i : 239 + i)$	$(1 : -169 : 13i : 239)$
0	1	$(2 : 1 + i : 1 + i)$	$*\ (1 : 1 : 1 : -1)$
0	2	$(8 : -2 : 3i)$	$(9 : -4 : 6i : -7i)$
0	3	$(4394 : 13 - 3107i : -1 + 239i)$	$*\ (1 : 169 : -13 : 239)$

PROOF. By Proposition 6.1, the map g is an isomorphism over $\mathbb{Q}(i)$ and its inverse is $g^{-1} : E \to C,\ P \mapsto f^{-1}([i](P + R))$. Calculations yield the formulae for g and g^{-1}:

$$g : C \to E, \quad (Y_0 : Y_1 : Y_2 : Y_3) \mapsto (X_0 : X_1 : X_2)$$
$$= \left\{ \begin{array}{l} ((-Y_0 + 2Y_1 + Y_3)^2 : (Y_0 + Y_1 + 2Y_2)(-Y_0 + 2Y_1 + Y_3) : \\ Y_0^2 + Y_0Y_2 + Y_0Y_3 + 2Y_1^2 + 2Y_1Y_2 + 2Y_1Y_3 + 3Y_2Y_3) \\ \qquad \text{if } (Y_0 : Y_1 : Y_2 : Y_3) \text{ is neither } (1 : 1 : 1 : -1) \text{ nor } (1 : 1 : -1 : -1) \\ (2(Y_2 + Y_3)(Y_0 + Y_1 - 2Y_2) : -(Y_2 + Y_3)(Y_0 - 2Y_1 + Y_3) : \\ -(Y_0 + 2Y_1)(Y_0 - 2Y_1 + Y_3)) \quad \text{if } (Y_0 : Y_1 : Y_2 : Y_3) \text{ is not among} \\ \qquad (1 : 1 : \pm 1 : 1), (2 : -1 : i\sqrt{2} : -i\sqrt{2}) \text{ and } (2 : -1 : -i\sqrt{2} : i\sqrt{2}) \end{array} \right\},$$

$$g^{-1} : E \to C, \quad (X_0 : X_1 : X_2) \mapsto (Y_0 : Y_1 : Y_2 : Y_3)$$
$$= \left\{ \begin{array}{l} ((X_2^2 + X_1X_2 - X_0X_1)^2 : (X_1^2 + X_2^2)^2 : (X_1^2 + X_2^2)(X_2^2 + X_1X_2 - X_0X_1) : \\ (X_1^2 - X_2^2)(X_2^2 + X_1X_2 - X_0X_1) + 3X_1X_2(X_1^2 + X_2^2)) \\ \qquad \text{if } (X_0 : X_1 : X_2) \text{ is not among } (1 : 0 : 0), R \text{ and } (1 : 0 : 0) + R \\ ((X_0^2 - 4X_0X_1 + 2X_1^2)^2 : (-X_0^2 + 2X_1^2 - 2X_0X_2)^2 : \\ (X_0^2 - 4X_0X_1 + 2X_1^2)(-X_0^2 + 2X_1^2 - 2X_0X_2) : \\ (X_0^2 - 2X_1^2 + 2X_0X_2)(X_0^2 + 4X_0X_1 + 2X_1^2) + 6X_0X_2(X_0^2 - 4X_0X_1 + 2X_1^2)) \\ \qquad \text{if } (X_0 : X_1 : X_2) \text{ is not among } O, (2 : i\sqrt{2} : 0) + R \text{ and} \\ \qquad (2 : -i\sqrt{2} : 0) + R \end{array} \right\}.$$

(See Sections 4.5 and 4.6–4.7 of the supplementary material, respectively.) The maps g and g^{-1} are defined over $\mathbb{Q}$, and the result follows. □

https://doi.org/10.1017/S0004972725100944 Published online by Cambridge University Press

7. Results

The propositions proved so far imply the following result.

THEOREM 7.1. *The map* $(a, b, c, m, n) \mapsto g((1 : m^2/n^2 : m/n : (b-c)/n^2))$ *from the set of primitive Fermat–Mersenne tuples to* $E(\mathbb{Q})$ *is a bijection.*

In the reverse direction, the correspondence is as follows. For each P *in* $E(\mathbb{Q})$*, the point* $g^{-1}(P)$ *in* $C(\mathbb{Q})$ *is of the form* $(1 : y^2 : y : z)$ *for some rational numbers* y *and* z *such that* $2y^4 = 1 + z^2$*. Defining* m*,* n *and* d *as in the surjectivity-related part of the proof of Proposition 4.1, we find that*

$$\left(m^2, \frac{n^2+d}{2}, \frac{n^2-d}{2}, m, n\right)$$

is the corresponding primitive Fermat–Mersenne tuple.

For $t \in \mathbb{Z}$ and $u \in \{0, 1\}$, let us write $P_{t,u} = [t](8 : 2 : 3) + [u](1 : 0 : 0)$. If the tuple (a, b, c, m, n) corresponds to the point $P = P_{t,u} \in E$, then the following statements hold. Simultaneously negating m and swapping b with c corresponds to replacing P with $(1 : 0 : 0) + P$ (that is, replacing u with $1 - u$). Negating m corresponds to replacing P with $(8 : 2 : -3) - P$ (that is, replacing t with $-1 - t$). Therefore, since $(1 : 0 : 0) + (8 : 2 : -3) = (1 : 2 : 3)$, swapping b with c corresponds to replacing P with $(1 : 2 : 3) - P$ (that is, simultaneously replacing t with $-1 - t$ and replacing u with $1 - u$). Table 2 lists some rational points on E, the corresponding rational points on C and the corresponding primitive Fermat–Mersenne tuples (see Section 5.1 of the supplementary material).

We now consider the condition where all entries are positive in the primitive Fermat–Mersenne tuple corresponding to some $P = (x_0 : x_1 : x_2)$ in $E(\mathbb{Q})$. That happens if and only if the point $g^{-1}(P) = (1 : y^2 : y : z)$ in $C(\mathbb{Q})$ satisfies $0 < y < 1$. If we have $P = O$ or $P = (1 : 0 : 0)$, then $y = 1$ or $y = -1$, respectively. If we have $P \in E(\mathbb{Q}) - \{O, (1 : 0 : 0)\}$, then by the expression for g^{-1} in the proof of Proposition 6.2, we have $0 < y < 1$ if and only if $x_2^2 + x_1^2 < x_2^2 + x_1x_2 - x_0x_1$, that is, if and only if $x_1(x_0 + x_1 - x_2) < 0$, that is, if and only if $1 + x_1/x_0 < x_2/x_0$ (since $x_0x_1 > 0$). It is easily checked that this corresponds to $Y > 3$ in the representation of the affine part of E as $Y^2 = X^3 + (1/2)X$ (see Section 5.2 of the supplementary material).

It is now useful to consider E as a curve over $\mathbb{R}$. Define

$$\omega = 2\int_0^\infty \frac{dX}{\sqrt{X^3 + (1/2)X}} \quad \text{and} \quad \kappa = \frac{1}{\omega}\int_{1/4}^\infty \frac{dX}{\sqrt{X^3 + (1/2)X}}.$$

Note that $0 < \kappa < 1/2$.

THEOREM 7.2. *For* $t \in \mathbb{Z}$ *and* $u \in \{0, 1\}$*, the point* $P_{t,u}$ *corresponds to a primitive Fermat–Mersenne tuple with all entries positive if and only if the fractional part of* $\kappa t + u/2$ *is in the interval* $(0, 1/2 - \kappa)$*.*

https://doi.org/10.1017/S0004972725100944 Published online by Cambridge University Press

TABLE 2. Some rational points $P = P_{t,u}$ on E, and their associated rational points $g^{-1}(P_{t,u})$ on C and primitive Fermat–Mersenne tuples $T = (a, b, c, m, n)$.

(t, u)	$(-1, 0)$	$(0, 0)$	$(1, 0)$
$P_{t,u}$	$(8 : 2 : -3)$	$(0 : 0 : 1)$	$(8 : 2 : 3)$
$g^{-1}(P_{t,u})$	$(1 : 1 : -1 : -1)$	$(1 : 1 : 1 : -1)$	$(1 : 13^2 : -13 : 239)$
T	$(1, 0, 1, -1, 1)$	$(1, 0, 1, 1, 1)$	$(13^2, 120, -119, -13, 1)$
(t, u)	$(-1, 1)$	$(0, 1)$	$(1, 1)$
$P_{t,u}$	$(1 : 2 : 3)$	$(1 : 0 : 0)$	$(1 : 2 : -3)$
$g^{-1}(P_{t,u})$	$(1 : 1 : 1 : 1)$	$(1 : 1 : -1 : 1)$	$(1 : 13^2 : 13 : -239)$
T	$(1, 1, 0, 1, 1)$	$(1, 1, 0, -1, 1)$	$(13^2, -119, 120, 13, 1)$
(t, u)	$(2, 0)$		
$P_{t,u}$	$(8(6)^3 : 2(6)(7)^2 : -7(113))$		
$g^{-1}(P_{t,u})$	$(1343^2 : 1525^2 : -1343(1525) : -2750257)$		
T	$(1525^2, -473304, 2276953, -1525, 1343)$		
(t, u)	$(3, 0)$		
$P_{t,u}$	$(8(13)^3 : 2(13)(239)^2 : 239(57123))$		
$g^{-1}(P_{t,u})$	$(2372159^2 : 2165017^2 : 2372159(2165017) : -3503833734241)$		
T	$(2165017^2, 1061652293520, 4565486027761, 2165017, 2372159)$		
(t, u)	$(6, 0)$		
$P_{t,u}$	$(8(354962322)^3 : 2(354962322)(3262580153)^2 :$ $3262580153(10650393355715621873))$		
$g^{-1}(P_{t,u})$	$(17999572487701067948161^2 : 15512114571284835412957^2 :$ $17999572487701067948161(15512114571284835412957) :$ $-10409335321015716539793003182373866739389448 1)$		
T	$(15512114571284835412957^2,$ $10994562826492402323701701006850700359469372 0,$ $21403898147508118863494704189224567098858820 1,$ $15512114571284835412957, 17999572487701067948161)$		

PROOF. On E, the differential $(1/Y)\,dX$ is invariant under translation via elliptic-curve addition. Since $E(\mathbb{R})$ is connected, we deduce that the map

$$h : E(\mathbb{R}) \to \mathbb{R}/\mathbb{Z}, \quad P \mapsto \left(\frac{1}{\omega}\int_P^O \frac{dX}{Y}\right) + \mathbb{Z}$$

(where the integral is taken from P upwards along $E(\mathbb{R})$ to $Y \to +\infty$) is a topological group isomorphism. Going downwards along $E(\mathbb{R})$ corresponds to going in the increasing direction of $\mathbb{R}$ modulo $\mathbb{Z}$.

https://doi.org/10.1017/S0004972725100944 Published online by Cambridge University Press

We obtain $h(O) = 0 + \mathbb{Z}$, $h((1:0:0)) = (1/2) + \mathbb{Z}$ and $h((8:2:3)) = \kappa + \mathbb{Z}$, so for each $t \in \mathbb{Z}$ and each $u \in \{0, 1\}$, we find $h(P_{t,u}) = (\kappa t + u/2) + \mathbb{Z}$. In particular, we have $h((1:2:3)) = h(P_{-1,1}) = (1/2 - \kappa) + \mathbb{Z}$. The result follows. □

We can write κ in terms of a series. The binomial expansion for $(1 + X)^{-1/2}$ (see [1, (18.8), page 116]) implies that

$$\int_0^z X^{-1/2}\sqrt{2} \cdot (1 + 2X^2)^{-1/2}\, dX = \sqrt{2} \cdot \sum_{n=0}^{\infty} \binom{-1/2}{n} \frac{2^{n+1}}{4n+1} z^{2n+1/2}$$

for all z such that $0 < z < (1/2)\sqrt{2}$. It is easily checked that the integrals

$$\omega_1 = \int_{(1:0:0)}^{(8:2:3)} \frac{dX}{Y} \quad \text{and} \quad \omega_2 = \int_{[2](8:2:3)}^{(1:0:0)} \frac{dX}{Y}$$

(taken along $E(\mathbb{R})$ upwards) satisfy $\omega = 2(2\omega_1 + \omega_2)$ and $\kappa = (\omega_1 + \omega_2)/(4\omega_1 + 2\omega_2)$. By the equalities

$$(8:2:3) = (1:1/4:3/8) \quad \text{and} \quad [2](8:2:3) = (1:49/144:-791/1728),$$

we obtain

$$\omega_1 = \sqrt{2} \cdot \sum_{n=0}^{\infty} \binom{-1/2}{n} \frac{1}{(4n+1)8^n} \quad \text{and} \quad \omega_2 = \frac{7\sqrt{2}}{6} \sum_{n=0}^{\infty} \binom{-1/2}{n} \frac{2^n \cdot 7^{4n}}{(4n+1)12^{4n}}.$$

A calculation to 15 decimal places yields $\kappa = 0.341556449662819\cdots$ (see Section 5.3 of the supplementary material).

Without calculating the Fermat–Mersenne tuple corresponding to the pair $(t, u) = (10^{10}, 0)$, we can verify that not all of the entries in the tuple are positive: the fractional part of $10^{10}\kappa$ is $0.62819\cdots$, which is not in $(0, 1/2 - \kappa)$. However, for $(t, u) = (10^{10}, 1)$, all of the entries in the Fermat–Mersenne tuple are positive: the fractional part of $10^{10}\kappa + 1/2$ is $0.12819\cdots$, which is in $(0, 1/2 - \kappa)$.

We easily obtain the following result.

THEOREM 7.3. *The Fermat–Mersenne problem has infinitely many primitive solutions with all entries positive.*

PROOF. It is easily checked that for each real number x, if the fractional part of x is not among $1/2 - \kappa$, $1 - 2\kappa$, $3/2 - 3\kappa$, $1 - \kappa$, $3/2 - 2\kappa$ and $2 - 3\kappa$, then the fractional part of at least one of the eight numbers $x + \kappa T + U/2$ with $T \in \{0, 1, 2, 3\}$ and $U \in \{0, 1\}$ is in $(0, 1/2 - \kappa)$. The number κ is irrational since $(8:2:3)$ has infinite order in $E(\mathbb{Q})$. Therefore, for each nonnegative integer t_0, for at least one pair (t, u) in the set $\{t_0, t_0 + 1, t_0 + 2, t_0 + 3\} \times \{0, 1\}$, the corresponding primitive Fermat–Mersenne tuple has all of its entries positive. □

For illustration, we list the first 25 pairs (t, u) with $0 \leqslant t \in \mathbb{Z}$ and $u \in \{0, 1\}$, ordered by increasing t, such that $P_{t,u}$ corresponds to a primitive Fermat–Mersenne tuple with all entries positive:

https://doi.org/10.1017/S0004972725100944 Published online by Cambridge University Press

$$\begin{array}{llllllll} (3,0), & (6,0), & (9,0), & (12,0), & (15,0), & (18,0), & & \\ (22,1), & (25,1), & (28,1), & (31,1), & (34,1), & (37,1), & & \\ (41,0), & (44,0), & (47,0), & (50,0), & (53,0), & (56,0), & (59,0), & \\ (63,1), & (66,1), & (69,1), & (72,1), & (75,1), & (78,1). & & \end{array}$$

The pairs (t,u) with $t<0$ can be obtained from the pairs with $t\geqslant 0$ by simultaneously replacing t with $-1-t$ and replacing u with $1-u$; this swaps b with c in the tuples. The pair $(t,u)=(3,0)$ corresponds to Fermat's solution.

Supplementary material

Supplementary material for this paper is available from a GitHub repository at https://github.com/ThackerayMayaR/FermatMersenneAG.

Acknowledgements

I was supported by the University of Pretoria Research Development Programme during the completion of this work. Many thanks indeed to Mapundi Banda, Eder Kikianty, James Raftery and everyone else at the University of Pretoria for their generous support. Many thanks indeed to Quay van der Hoff, whose discussions with me about Pythagorean triples and geometry provided inspiration for this paper.

References

[1] G. J. Hademenos, M. R. Spiegel and J. Liu, *Mathematical Handbook of Formulas and Tables*, Schaum's Easy Outlines, Schaum's Outline Series (McGraw-Hill, New York, 2001).

[2] J.-L. Lagrange, 'Sur quelques problèmes de l'analyse de Diophante', in: *Nouveaux mémoires de l'Académie royale des sciences et belles-lettres de Berlin*, année 1777; *Oeuvres de Lagrange*, 4 (eds. J. A. Serret and G. Darboux) (Gauthier-Villars, Paris, 1867–1892), 377–398. https://gallica.bnf.fr/ark:/12148/bpt6k229223s/f379.

[3] D. A. Marcus, *Number Fields* (Springer-Verlag, New York, 1977).

[4] W. Sierpiński (translated by A. Sharma), *Pythagorean Triangles* (Dover Publications, Mineola, NY, 2003).

[5] J. H. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics, 151 (Springer-Verlag, New York, 1999).

[6] J. H. Silverman, *The Arithmetic of Elliptic Curves*, 2nd edn, Graduate Texts in Mathematics, 106 (Springer, New York, 2010).

[7] The LMFDB Collaboration, *The L-functions and Modular Forms Database*, Elliptic curve with LMFDB label 256.b2 (Cremona label 256b2) (2025). https://www.lmfdb.org/EllipticCurve/Q/256/b/2.

HENRY (MAYA) ROBERT THACKERAY, University of Pretoria,
Pretoria, 0002 South Africa
e-mail: maya.thackeray@up.ac.za

https://doi.org/10.1017/S0004972725100944 Published online by Cambridge University Press