ARITHMETIC PROGRESSIONS OF THREE SQUARES

KEITH CONRAD

1. Introduction

Here are the first 10 perfect squares (ignoring 0):

$$\mathbf{1},\ 4,\ 9,\ 16,\ \mathbf{25},\ 36,\ \mathbf{49},\ 64,\ 81,\ 100.$$

In this list is the arithmetic progression 1, 25, 49 (common difference 24). Searching further, another arithmetic progression of squares is 289, 625, 961 (common difference 336). Yet another is 529, 1369, 2209 (common difference 840). How can all examples be found?

In Section 2 we will use plane geometry to describe the 3-term arithmetic progressions of (nonzero) perfect squares in terms of rational points on the circle $x^2+y^2=2$. Since a^2, b^2, c^2 is an arithmetic progression if and only if $(a/d)^2, (b/d)^2, (c/d)^2$ is an arithmetic progression, where $d \neq 0$, there is not much difference between integral and rational arithmetic progressions of three squares, and in Section 3 we will describe 3-term arithmetic progressions of rational squares with a fixed common difference in terms of rational points on elliptic curves (Corollary 3.7). In the appendix, the link between elliptic curves and arithmetic progressions with a fixed common difference is revisited using projective geometry.

2. Progressions of squares and $x^2 + y^2 = 2$

For integers a, b, and c, to say a^2, b^2, c^2 is an arithmetic progression means $b^2-a^2 = c^2-b^2$, or equivalently $a^2 + c^2 = 2b^2$. Ignoring $b = 0$, b is nonzero and we divide by it to get

$$\left(\frac{a}{b}\right)^2 + \left(\frac{c}{b}\right)^2 = 2,$$

so $(a/b, c/b)$ is a rational point on the circle $x^2 + y^2 = 2$. Conversely, if x and y are rational and satisfy $x^2 + y^2 = 2$, write x and y with a common denominator as $x = a/b$ and $y = c/b$ where $a, b, c \in \mathbf{Z}$ with $b \neq 0$. Then $a^2 + c^2 = 2b^2$, so $c^2 - b^2 = b^2 - a^2$, which means a^2, b^2, c^2 is an arithmetic progression of squares in $\mathbf{Z}$. For example, $(17/25, 31/25)$ satisfies $x^2 + y^2 = 2$, so $17^2, 25^2, 31^2$ is an arithmetic progression (common difference 336). Finding *all* 3-term arithmetic progressions of perfect squares is thus essentially[1] equivalent to finding all rational points on the circle $x^2+y^2 = 2$. An obvious rational point on this circle is $(1, 1)$. Using lines through this point we will describe all other rational points on the circle.

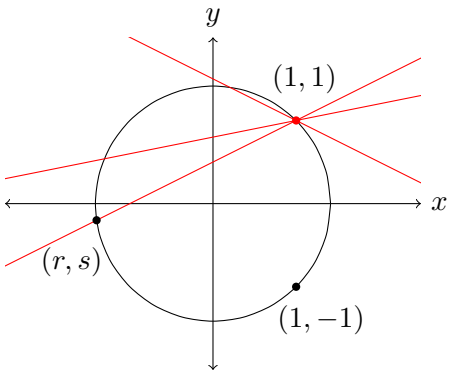
Theorem 2.1. *The points on $x^2 + y^2 = 2$ other than $(1, -1)$ are described by the formulas*

$$x = \frac{m^2 - 2m - 1}{m^2 + 1}, \quad y = \frac{-m^2 - 2m + 1}{m^2 + 1},$$

where $m \in \mathbf{R}$. If (x, y) and m correspond to each other, then x and y are rational if and only if m is rational.

[1]Arithmetic progressions a^2, b^2, c^2 and $(ka)^2, (kb)^2, (kc)^2$ lead to the same point on $x^2 + y^2 = 2$. There is a bijection between rational points and progressions a^2, b^2, c^2 that have $b > 0$ (to fix signs) and are *reduced*: $\gcd(a, b, c) = 1$.

Proof. Drawing a line through the point $(1,1)$ and computing the second point where this line crosses the circle $x^2+y^2=2$ will let us parametrize the points on the circle according to the slopes of the lines through $(1,1)$, except for $(1,-1)$, which is on a vertical line through $(1,1)$. We will see that rational points correspond to rational slopes.



Let (r,s) be a point on $x^2+y^2=2$ other than $(1,\pm1)$, as in the figure above. Draw the line through $(1,1)$ and (r,s). It is not vertical, so we can write the equation of the line as $y=mx+b$. Since the line goes through $(1,1)$, $b=1-m$. To find the coordinates of (r,s) in terms of m, note this point is on both the line and the circle. Let's substitute $mx+b=mx+(1-m)$ for y in the equation of the circle:

$$2=x^2+(mx+1-m)^2=(m^2+1)x^2+2m(1-m)x+(1-m)^2,$$

and after subtracting 2 and dividing by m^2+1 this is the same as

$$x^2+\frac{2m(1-m)}{m^2+1}x+\frac{m^2-2m-1}{m^2+1}=0. \tag{2.1}$$

The two points on the line and circle are $(1,1)$ and (r,s), so the roots of (2.1) must be $x=1$ and $x=r$. That is, the left side of (2.1) is $(x-1)(x-r)$, which has constant term r, so

$$r=\frac{m^2-2m-1}{m^2+1}.$$

Since (r,s) lies on the line $y=mx+(1-m)$,

$$s=mr+(1-m)=\frac{-m^2-2m+1}{m^2+1}.$$

We thus obtain correspondences from slopes to points (other than $(1,\pm1)$) and conversely:

$$m\mapsto\left(\frac{m^2-2m-1}{m^2+1},\frac{-m^2-2m+1}{m^2+1}\right),\ (x,y)\mapsto\frac{y-1}{x-1}. \tag{2.2}$$

There are two lines through $(1,1)$ that we neglected: the vertical line and also its tangent line to the circle, which is $y=-x+2$. The tangent line has slope $m=-1$, and in (2.2) the number $m=-1$ goes over to $(2/2,2/2)=(1,1)$. So we can extend the correspondence to associate $m=-1$ to the point $(1,1)$ itself. The two functions in (2.2) are mutually inverse mappings from all $m\neq-1$ to all points on $x^2+y^2=2$ besides $(1,\pm1)$, and if $m\longleftrightarrow(x,y)$ then x and y are rational if and only if m is rational. So the formula

$$\left(\frac{m^2-2m-1}{m^2+1},\frac{-m^2-2m+1}{m^2+1}\right) \tag{2.3}$$

describes all rational solutions (x, y) to $x^2+y^2 = 2$ other than $(1, -1)$ as m runs through all rational numbers. (We get $(1, -1)$ by setting $m = \infty$, corresponding to a vertical slope.) □

Table 1 lists some examples of rational points on $x^2 + y^2 = 2$ found using lines through $(1, 1)$ with rational slope and a corresponding 3-term arithmetic progression of squares by writing $x = a/b$ and $y = c/b$.

m	(x, y)	(a^2, b^2, c^2)
1	$(-1, -1)$	$(1, 1, 1)$
$1/2$	$(-7/5, -1/5)$	$(1, 25, 49)$
$-1/3$	$(-1/5, 7/5)$	$(1, 25, 49)$
$-5/3$	$(23/17, 7/17)$	$(49, 289, 529)$
$3/4$	$(-31/25, -17/25)$	$(289, 625, 961)$

TABLE 1.

3. Common Differences and Elliptic Curves

We now look at 3-term arithmetic progressions of *rational* squares having a fixed common difference (not equal to 0). For instance, 24 is the the common difference of 1, 25, 49, and it is also the common difference of

$$\left(\frac{1151}{70}\right)^2, \left(\frac{1201}{70}\right)^2, \left(\frac{1249}{70}\right)^2.$$

In fact, 24 is the common difference of an arithmetic progression of 3 rational squares not just twice, but infinitely often. We will see why using elliptic curves.

Theorem 3.1. *For rational $n \neq 0$, the triples of rational numbers (a, b, c) whose squares are an arithmetic progression with common difference n are in bijection with the rational solutions (m, k) of $nk^2 = m^3 - m$ where $k \neq 0$.*

Proof. Let (a, b, c) be a triple of rational numbers such that a^2, b^2, c^2 is an arithmetic progression with common difference n, so $b^2 - a^2 = n$ and $c^2 - b^2 = n$. The point $(a/b, c/b)$ lies on $x^2 + y^2 = 2$ and is not $(1, \pm 1)$ since $a/b \neq 1$, so Theorem 2.1 gives a parametric formula for a/b. Letting m be the slope of the line through $(1, 1)$ and $(a/b, c/b)$, so

$$m = \frac{c/b - 1}{a/b - 1} = \frac{c - b}{a - b}, \tag{3.1}$$

we have $a/b = (m^2 - 2m - 1)/(m^2 + 1)$ by Theorem 2.1. Therefore

$$\begin{aligned} n &= b^2 - a^2 \\ &= b^2\left(1 - \left(\frac{a}{b}\right)^2\right) \\ &= b^2\left(1 - \left(\frac{m^2 - 2m - 1}{m^2 + 1}\right)^2\right) \\ &= b^2\frac{4(m^3 - m)}{(m^2 + 1)^2} \\ &= \left(\frac{2b}{m^2 + 1}\right)^2 (m^3 - m), \end{aligned}$$

so $nk^2 = m^3 - m$, where

$$k = \frac{m^2+1}{2b} \neq 0. \tag{3.2}$$

Substituting (3.1) into (3.2),

$$k = \frac{((c-b)/(a-b))^2+1}{2b} = \frac{2b-a-c}{(a-b)^2}, \tag{3.3}$$

where we simplify using the relations $a^2 = b^2 - n$ and $c^2 = b^2 + n$.

Conversely, if $nk^2 = m^3 - m$ for some rational numbers k and m, where $k \neq 0$, set

$$b = \frac{m^2+1}{2k}, \quad a = \frac{b(m^2-2m-1)}{m^2+1}, \quad c = \frac{b(-m^2-2m+1)}{m^2+1}. \tag{3.4}$$

(These formulas are inspired by (3.2) and the parametrization of points on $x^2 + y^2 = 2$ in Theorem 2.1.) Substituting the formula for b into those for a and c in (3.4), we get

$$a = \frac{m^2-2m-1}{2k}, \quad c = \frac{-m^2-2m+1}{2k}.$$

The rational squares a^2, b^2, c^2 are an arithmetic progression with common difference n.

The correspondence we found between (a, b, c) and (m, k) is given by

$$(a, b, c) \mapsto \left(\frac{c-b}{a-b}, \frac{2b-a-c}{(a-b)^2}\right), \tag{3.5}$$

using (3.1) and (3.3), and

$$(m, k) \mapsto \left(\frac{m^2-2m-1}{2k}, \frac{m^2+1}{2k}, \frac{-m^2-2m+1}{2k}\right). \tag{3.6}$$

Check (3.5) and (3.6) are inverses of each other. □

Example 3.2. The arithmetic progression 1, 25, 49, with difference $n = 24$, arises as squares of 8 possible triples, including $(a, b, c) = (1, 5, 7)$ and $(a, b, c) = (-1, 5, -7)$. Substituting these triples (*not* the squares $(1, 25, 49)$) into (3.5) produces the pairs $(m, k) = (-1/2, 1/8)$ and $(m, k) = (2, 1/2)$, which both satisfy $24k^2 = m^3 - m$.

In (3.6) take $m = 10$, so $m^3 - m = 990 = 9 \cdot 110$. This is nk^2 for $k = 3$ and $n = 110$. Using (3.6) with $(m, k) = (10, 3)$, we obtain $a = 79/6$, $b = 101/6$, and $c = -119/6$. The squares $(79/6)^2$, $(101/6)^2$, and $(119/6)^2$ are an arithmetic progression with common difference $n = 110$.

Corollary 3.3. *For rational $n \neq 0$, the triples of rational numbers (a, b, c) whose squares are an arithmetic progression with common difference n are in bijection with the rational solutions (x, y) of the equation*

$$y^2 = x^3 - n^2x$$

where $y \neq 0$, by

$$(a, b, c) \mapsto \left(\frac{n(c-b)}{a-b}, \frac{n^2(2b-a-c)}{(a-b)^2}\right)$$

and

$$(x, y) \mapsto \left(\frac{x^2-2nx-n^2}{2y}, \frac{x^2+n^2}{2y}, \frac{-x^2-2nx+n^2}{2y}\right).$$

Proof. Theorem 3.1 identifies the triples (a, b, c) such that a^2, b^2, c^2 has common difference n, with the pairs (m, k) satisfying $nk^2 = m^3 - m$ where $k \neq 0$. We can pass between $nk^2 = m^3 - m$ and $y^2 = x^3 - n^2x$ by

$$(m, k) \mapsto (nm, n^2k), \quad (x, y) \mapsto \left(\frac{x}{n}, \frac{y}{n^2}\right).$$

Composing these with (3.5) and (3.6) expresses (a, b, c) in terms of (x, y) and conversely. □

Example 3.4. A solution to $y^2 = x^3 - 49x$ is $(x, y) = (-63/16, 735/64)$. Using Corollary 3.3 with $n = 7$ gives $a = 113/120$, $b = 337/120$, and $c = 463/120$. The progression $(113/120)^2$, $(337/120)^2$, and $(463/120)^2$ has common difference 7. What happens using the same (x, y) with $n = -7$?

In Section 2 we used $x^2 + y^2 = 2$ and here we use $y^2 = x^3 - n^2x$. Don't confuse their roles. The first one is related to all 3-term arithmetic progressions of rational squares, without concern over their common difference, while the second is related to the more refined question of whether or not there is such a progression with common difference n.

Remark 3.5. For historical reasons, an arithmetic progression of three rational squares is called a *congruum* and a positive integer n that occurs as the common difference of a congruum is called a *congruent number*.[2] For example, 24 is a congruent number since it is the common difference of the congruum 1, 25, 49. Dividing through by 4, we see that 6 is also a congruent number since it is the common difference of the congruum 1/4, 25/4, 49/4. By Example 3.4, 7 is a congruent number. The number 1 is *not* a congruent number: there is no arithmetic progression of three rational squares with common difference 1. Equivalently, by Corollary 3.3, the equation $y^2 = x^3 - x$ has no rational solutions with $y \neq 0$. This was conjectured by Fibonacci in the 1200s and first proved by Fermat in the 1600s. Among the integers from 1 to 10, the only congruent numbers are 5, 6, and 7. (For 5, use the arithmetic progression $(31/12)^2, (41/12)^2, (49/12)^2$.) That 1, 2, and 3 are not congruent numbers means there is no congruum with common difference equal to a perfect square, twice a perfect square, or three times a perfect square.

Next we will use standard theorems about elliptic curves to say something about the nature of the rational points on $y^2 = x^3 - n^2x$.

Theorem 3.6. *For rational $n \neq 0$, the only nonidentity rational points on $y^2 = x^3 - n^2x$ of finite order are $(0, 0)$, $(n, 0)$, and $(-n, 0)$.*

Proof. Our argument is taken from [1, p. 660]. Write $n = dk^2$, where d is a squarefree integer. There is a bijection from $y^2 = x^3 - n^2x$ to $y^2 = x^3 - d^2x$ by $(x, y) \mapsto (x/k^2, y/k^3)$, which preserves rationality of points and sends $(0, 0)$, $(n, 0)$, and $(-n, 0)$ to $(0, 0)$, $(d, 0)$, and $(-d, 0)$. Therefore, to show any *rational* point (x, y) with finite order has $y = 0$, there is no harm in replacing n with d, which means we may assume n is a squarefree integer.

A rational point $P = (x, y)$ with $y = 0$ has order 2 from the definition of the group law on elliptic curves, and these points are $(0, 0)$, $(n, 0)$, and $(-n, 0)$. If $y \neq 0$ we will show P has infinite order by contradiction. Assume $y \neq 0$ and P is a rational point of finite order. Then the Nagell–Lutz theorem implies the coordinates of P are in $\mathbf{Z}$. Set $P + P = (x', y')$.

[2]This term is not directly related to "congruence" in the sense of modular arithmetic, and while the term "congruent number" is well-known within number theory, the term "congruum" is essentially obsolete.

Since $P + P$ has finite order, its coordinates are also integers by Nagell–Lutz. The first coordinate of $P + P$ turns out to be

$$x' = \left(\frac{x^2 + n^2}{2y}\right)^2.$$

Using the condition $y^2 = x^3 - n^2x$, we have

$$x' - n = \left(\frac{x^2 - 2nx - n^2}{2y}\right)^2, \quad x' + n = \left(\frac{x^2 + 2nx - n^2}{2y}\right)^2.$$

So $x' - n, x', x' + n$ is an arithmetic progression of rational squares with common difference n. Write $x' - n = a^2$, $x' = b^2$, and $x' + n = c^2$. Since a, b, and c are rational and square to integers, they are themselves integers. Then $c^2 - a^2 = 2n$ is an even difference of squares. An even difference of squares is a multiple of 4 (since the only squares mod 4 are 0 and 1), so $2n \equiv 0 \bmod 4$. Thus n is even. Since $n = c^2 - b^2$ and a difference of integer squares is $0, 1$, or $3 \bmod 4$, we must have $n \equiv 0 \bmod 4$. This contradicts n being squarefree. □

For another proof of Theorem 3.6, using Dirichlet's theorem on primes in arithmetic progression, see [2, pp. 44–45].

Corollary 3.7. *If the rational number $n \neq 0$ is the common difference of a 3-term arithmetic progression of rational squares, then it is such a common difference for infinitely many progressions.*

Proof. By Corollary 3.3 a 3-term arithmetic progression of rational squares with common difference n leads to a rational point on the elliptic curve $y^2 = x^3 - n^2x$ where $y \neq 0$, and such a point has infinite order by Theorem 3.6. Therefore repeatedly adding the point to itself on the elliptic curve gives us infinitely many rational points on the curve, which each lead back to a new 3-term arithmetic progressions of rational squares with common difference n. □

Example 3.8. The 3-term arithmetic progression $(1, 25, 49)$ with common difference $n = 24$ is (a^2, b^2, c^2) for $(a, b, c) = (1, 5, 7)$, and this corresponds to the point $P = (-12, 72)$ on $y^2 = x^3 - 24^2x$ by the first correspondence in Corollary 3.3. The first few multiples of P on this elliptic curve are

$$2P = (25, -35), \quad 3P = \left(-\frac{6348}{1369}, -\frac{2568456}{50653}\right), \quad 4P = \left(\frac{1442401}{4900}, \frac{1726556399}{343000}\right).$$

Applying to these the second correspondence in Corollary 3.3 we get three triples (a, b, c) besides $(1, 5, 7)$ where a^2, b^2, c^2 is an arithmetic progression with common difference 24:

$$\left(\frac{1151}{70}, \frac{-1201}{70}, \frac{1249}{70}\right), \quad \left(\frac{4319999}{1319901}, \frac{-7776485}{1319901}, \frac{-10113607}{1319901}\right),$$
$$\left(\frac{1727438169601}{241717895860}, \frac{2094350404801}{241717895860}, \frac{-2405943600001}{241717895860}\right).$$

Remark 3.9. If (a, b, c) is a triple of nonzero rational numbers whose squares are in arithmetic progression with common difference $n \neq 0$, then seven other triples whose squares have common difference n are

$$(-a, b, c), \quad (a, -b, c), \quad (a, b, -c), \quad (-a, -b, c),$$
$$(-a, b, -c), \quad (a, -b, -c), \quad (-a, -b, -c).$$

Passing from these triples to points on $y^2 = x^3 - n^2x$, the sign changes in the coordinates have an interpretation in the group law on the elliptic curve. Say $(a, b, c) \longleftrightarrow (x, y)$ in Corollary 3.3. Each sign change on a, b, and c is an operation of order 2. It should correspond to an operation of order 2 on the points of $y^2 = x^3 - n^2x$. Using the group law, some operations of order 2 are $P \mapsto P + Q$ where Q is a point of order 2, and $P \mapsto -P + Q$ where Q is any point.

The inverse of (x, y) is $(x, -y)$, which corresponds by Corollary 3.3 to $(-a, -b, -c)$. The points of order 2 on $y^2 = x^3 - n^2x$ are $(0, 0)$, $(n, 0)$, and $(-n, 0)$. The sum of (x, y) and $(0, 0)$ is $(-n^2/x, n^2y/x^2)$, which corresponds by Corollary 3.3 to $(-a, b, -c)$. More generally, the sum of (x, y) and each of $(0, 0)$, $(n, 0)$, and $(-n, 0)$, as well as the sum of $(x, -y)$ and each of $(0, 0)$, $(n, 0)$, and $(-n, 0)$, gives us 6 points. See Table 2. The corresponding triples from Corollary 3.3 are collected in Table 3 and are exactly what we are looking for.

First Point	Second Point	Sum
(x, y)	$(0, 0)$	$(-n^2/x, n^2y/x^2)$
$(x, -y)$	$(0, 0)$	$(-n^2/x, -n^2y/x^2)$
(x, y)	$(n, 0)$	$(n(x + n)/(x - n), -2n^2y/(x - n)^2)$
$(x, -y)$	$(n, 0)$	$(n(x + n)/(x - n), 2n^2y/(x - n)^2)$
(x, y)	$(-n, 0)$	$(-n(x - n)/(x + n), -2n^2y/(x + n)^2)$
$(x, -y)$	$(-n, 0)$	$(-n(x - n)/(x + n), 2n^2y/(x + n)^2)$

TABLE 2. Addition on $y^2 = x^3 - n^2x$

Group Law	Sign Change
(x, y)	(a, b, c)
$(x, y) + (0, 0)$	$(-a, b, -c)$
$(x, y) + (n, 0)$	$(a, -b, -c)$
$(x, y) + (-n, 0)$	$(-a, -b, c)$
$(x, -y)$	$(-a, -b, -c)$
$(x, -y) + (0, 0)$	$(a, -b, c)$
$(x, -y) + (n, 0)$	$(-a, b, c)$
$(x, y) + (-n, 0)$	$(-a, -b, c)$

TABLE 3.

APPENDIX A. WORKING IN PROJECTIVE SPACE

Using projective geometry we will describe a different approach to Corollary 3.3 that bypasses Theorem 3.1, and ultimately Theorem 2.1.

Theorem A.1. *For rational $n \neq 0$, there is a bijection between the sets*

$$\{(r, s, t) : s^2 - r^2 = n, t^2 - s^2 = n\}, \quad \{(x, y) : y^2 = x^3 - n^2x, y \neq 0\},$$

such that (r, s, t) is rational if and only if (x, y) is rational. The correspondences are

$$(r, s, t) \mapsto \left(\frac{n(r - t)}{r - 2s + t}, \frac{2n^2}{r - 2s + t}\right)$$

and

$$(x, y) \mapsto \left(\frac{-x^2 + 2nx + n^2}{2y}, \frac{-x^2 - n^2}{2y}, \frac{-x^2 - 2nx + n^2}{2y}\right)$$

The correspondence here is not the same as in Corollary 3.3. We'll reconcile the discrepancy (it's off by an automorphism of the elliptic curve $y^2 = x^3 - n^2x$) after the proof.

Proof. We are interested in the conditions

$$s^2 - r^2 = n, \quad t^2 - s^2 = n.$$

Homogenize these as conditions on a point $[r, s, t, u] \in \mathbf{P}^3(\mathbf{R})$:

$$s^2 - r^2 = nu^2, \quad t^2 - s^2 = nu^2. \tag{A.1}$$

The solutions to (A.1) with $u = 0$ are the 4 points $[1, \pm 1, \pm 1, 0]$. These solutions don't correspond to what we're really interested in (which are the solutions $[r, s, t, 1]$), but we will make use of them in a geometric construction in projective space.

Each equation in (A.1) defines a surface in $\mathbf{P}^3(\mathbf{R})$, so we anticipate that the common solution set to both equations is a curve in $\mathbf{P}^3(\mathbf{R})$, just as two surfaces in $\mathbf{R}^3$ usually intersect in a curve (not another surface). With this in mind, let C denote the solution set to (A.1) in $\mathbf{P}^3(\mathbf{R})$. We will make a well-chosen projection from C into a plane and find an equation of the image of C, which will turn out to be $y^2 = x^3 - n^2x$.

Let $P = [1, 1, 1, 0]$ and $\Pi = \{[r, s, 0, u]\}$, so Π is a plane in $\mathbf{P}^3(\mathbf{R})$ not containing P. Define $f\colon C \to \Pi$ to be projection from P:

$$f(Q) = \overline{PQ} \cap \Pi,$$

where $\overline{PQ}$ when $Q = P$ means the tangent line to C at P. The line through $[1, 1, 1, 0]$ and $[r, s, t, u] \neq [1, 1, 1, 0]$ is the set of points

$$[\lambda + \mu r, \lambda + \mu s, \lambda + \mu t, \mu u],$$

which meets Π where $\lambda = -\mu t$. Thus $f([r, s, t, u]) = [r - t, s - t, 0, u]$. To find $f([1, 1, 1, 0])$, we need the tangent line to C at $[1, 1, 1, 0]$. The tangent plane to the surface $s^2 - r^2 = nu^2$ at $[1, 1, 1, 0]$ in $\mathbf{P}^3(\mathbf{R})$ is $r = s$, and the tangent plane to $t^2 - s^2 = nu^2$ at $[1, 1, 1, 0]$ in $\mathbf{P}^3(\mathbf{R})$ is $s = t$. The tangent line to C at P is the intersection of these two tangent planes, which is the line of points $[r, r, r, u]$. This meets Π in $[0, 0, 0, 1]$, so

$$f([r, s, t, u]) = \begin{cases} [r - t, s - t, 0, u], & \text{if } [r, s, t, u] \in C - [1, 1, 1, 0], \\ [0, 0, 0, 1], & \text{if } [r, s, t, u] = [1, 1, 1, 0]. \end{cases}$$

This formula suggests introduction of new variables for $[r, s, t, u] \in C - P$:

$$v = r - t, \quad w = s - t.$$

Then $r = t + v$ and $s = t + w$, so (A.1) becomes

$$(t + w)^2 - (t + v)^2 = nu^2, \quad t^2 - (t + w)^2 = nu^2,$$

which is

$$w^2 - v^2 + 2t(w - v) = nu^2, \quad -2tw - w^2 = nu^2. \tag{A.2}$$

We can eliminate t using (A.2) provided $w - v \neq 0$ or $w \neq 0$. Could $w - v = 0$ and $w = 0$? If so, then $s = t + w = t$ and $r = t + v = t$, and (A.2) implies $u = 0$, so $[r, s, t, u] = [1, 1, 1, 0] = P$, a contradiction. Hence we can solve for t using one equation

in (A.2) and substitute into the other equation in (A.2) to eliminate t. The result, after clearing denominators, is

$$2nu^2w + v^2w = w^2v + nu^2v. \tag{A.3}$$

This is satisfied by $[v, w, u]$ coming from points on $C - P$. These are the first, second, and fourth coordinates of f on $C - P$. Since $f(P) = [0, 0, 0, 1]$, we are led to take $[v, w, u] = [0, 0, 1]$ at $P = [1, 1, 1, 0]$, which also satisfies (A.3). Sending $[r, s, t, u]$ on the curve C to $[v, w, u]$ on the curve (A.3) in $\mathbf{P}^2(\mathbf{R})$ is a bijection.

In Table 4 we list each point on C with $u = 0$, its image in $[v, w, u]$ coordinates, the projective tangent line to (A.3) at the point, and where the tangent line meets (A.3). Only for the first point in Table 4 does the tangent line meet the curve (A.3) just at the point itself. So, to put (A.3) in Weierstrass form, we want to move $[v, w, u] = [0, 0, 1]$ to $[0, 1, 0]$ and move its tangent line to the line at infinity.

$[r, s, t, u]$	$[v, w, u]$	Tangent line	Meets (A.3)
$[1, 1, 1, 0]$	$[0, 0, 1]$	$v = 2w$	$[0, 0, 1]$
$[1, -1, 1, 0]$	$[0, 1, 0]$	$v = 0$	$[0, 1, 0], [0, 0, 1]$
$[1, 1, -1, 0]$	$[1, 1, 0]$	$v = w$	$[1, 1, 0], [0, 0, 1]$
$[1, -1, -1, 0]$	$[1, 0, 0]$	$w = 0$	$[1, 0, 0], [0, 0, 1]$

TABLE 4.

Set

$$v' = v, \quad w' = u, \quad u' = v - 2w.$$

This is an invertible linear change of variables ($v = v', w = (v' - u')/2, u = w'$) and it has the desired effect at $[0, 0, 1]$ and its tangent line: $[v, w, u] = [0, 0, 1]$ has $[v', w', u'] = [0, 1, 0]$ and the line $v = 2w$ becomes the line $u' = 0$. Using $[v', w', u']$ coordinates, (A.3) becomes

$$4nu'w'^2 = v'^3 - u'^2v'.$$

Multiply by n^3:

$$u'(2n^2w')^2 = (nv')^3 - n^2u'^2(nv'). \tag{A.4}$$

Now set

$$x = nv' = nv = n(r - t), \quad y = 2n^2w' = 2n^2u, \quad z = u' = v - 2w = r - 2s + t.$$

In these coordinates, (A.4) becomes a Weierstrass equation:

$$y^2z = x^3 - n^2xz^2.$$

Table 5 lists the $[x, y, z]$ coordinates of the 4 points on C with $u = 0$. They are the 4 rational points of finite order on $y^2 = x^3 - n^2x$, or equivalently the rational points that play no role in the correspondence of Corollary 3.3.

The overall change of variables $[r, s, t, u] \mapsto [x, y, z]$ is

$$[r, s, t, u] \mapsto [n(r - t), 2n^2u, r - 2s + t].$$

When $u \neq 0$ and we scale u to 1, this becomes

$$[r, s, t, 1] \mapsto [n(r - t), 2n^2, r - 2s + t] = \left[\frac{n(r - t)}{r - 2s + t}, \frac{2n^2}{r - 2s + t}, 1\right]. \tag{A.5}$$

$[r,s,t,u]$	$[x,y,z]$
$[1,1,1,0]$	$[0,1,0]$
$[1,-1,1,0]$	$[0,0,1]$
$[1,1,-1,0]$	$[-n,0,1]$
$[1,-1,-1,0]$	$[n,0,1]$

TABLE 5.

(To see that $r-2s+t \neq 0$, assume otherwise: $r+t=2s$. Combining this with the arithmetic progression condition $r^2+t^2=2s^2$, we get $r=s$ after a little algebra, so $nu^2=s^2-r^2=0$, hence $u=0$, a contradiction.) The inverse of (A.5), for $y \neq 0$, is

$$[x,y,1] \mapsto \left[\frac{-x^2+2nx+n^2}{2y}, \frac{-x^2-n^2}{2y}, \frac{-x^2-2nx+n^2}{2y}, 1\right]$$

□

Example A.2. When $n=6$, Table 6 lists the 8 rational triples that square to the arithmetic progression $1/4, 25/4, 49/4$ and the corresponding rational points on $y^2=x^3-36x$.

(r,s,t)	(x,y)
$(1/2,5/2,7/2)$	$(18,-72)$
$(-1/2,5/2,7/2)$	$(12,-36)$
$(1/2,-5/2,7/2)$	$(-2,8)$
$(1/2,5/2,-7/2)$	$(-3,-9)$
$(-1/2,-5/2,7/2)$	$(-3,9)$
$(1/2,-5/2,-7/2)$	$(12,36)$
$(-1/2,5/2,-7/2)$	$(-2,-8)$
$(-1/2,-5/2,-7/2)$	$(18,72)$

TABLE 6.

For a triple (a,b,c) satisfying $b^2-a^2=n$ and $c^2-b^2=n$, the corresponding point (x,y) on $y^2=x^3-n^2x$ using Corollary 3.3 is

$$\left(\frac{n(c-b)}{a-b}, \frac{n^2(2b-a-c)}{(a-b)^2}\right), \tag{A.6}$$

while Theorem A.1 sends (a,b,c) to

$$\left(\frac{n(a-c)}{a-2b+c}, \frac{2n^2}{a-2b+c}\right). \tag{A.7}$$

These different correspondences are related to each other by an automorphism of $y^2=x^3-n^2x$. Specifically, if we run through the operations in Table 2, the function

$$(x,y) \mapsto \left(\frac{-n(x-n)}{x+n}, \frac{-2n^2y}{(x+n)^2}\right) = (x,y)+(-n,0)$$

takes (A.6) to (A.7) and conversely, and it is an involution (order 2).

Let's see how a change in the plane of projection in the proof of Theorem A.1 changes the calculations. Project from $P=[1,1,1,0]$ to the plane $\{[0,s,t,u]\}$ instead of to the plane

$\{[r,s,0,u]\}$. Projection from P to $\{[0,s,t,u]\}$ is given by $f([r,s,t,u]) = [0,s-r,t-r,u]$, and the change of variables $v = s-r$ and $w = t-r$ leads to the plane curve

$$2nu^2v + v^2w = w^2v + nu^2w \tag{A.8}$$

rather than (A.3). (How is the equation different?) The $[v,w,u]$ coordinates of P, once again, are $[0,0,1]$, and the tangent line to (A.8) at $[0,0,1]$ is $w = 2v$ (not $v = 2w$). This tangent line meets the curve at no other point. We move $[0,0,1]$ to $[0,1,0]$ and its tangent line to the line at infinity using

$$v' = v, \quad w' = u, \quad u' = w - 2v.$$

Use the inverse of this change of variables to turn (A.8) into

$$\begin{aligned} nu'w'^2 &= -2v'^3 - 3v'^2u' - v'u'^2 \\ &= -v'(2v' + u')(v' + u') \\ &= (-v')(-2v' - u')(-v' - u') \end{aligned}$$

Now multiply by $4n^3$ and set $x = n(-2v'-u')$, $y = 2n^2w'$, and $z = u'$, so $y^2z = (x+nz)x(x-nz) = x^3 - n^2xz^2$. Tracing out the overall change of variables gives the correspondence

$$(r,s,t) \mapsto \left(\frac{n(r-t)}{r-2s+t}, \frac{2n^2}{r-2s+t} \right),$$

which is exactly the same as the one in Theorem A.1.

References

[1] W. A. Coppel, "Number Theory: An Introduction to Mathematics. Part B," Springer-Verlag, New York, 2006.

[2] N. Koblitz, "Introduction to Elliptic Curves and Modular Forms," 2nd ed., Springer–Verlag, New York, 1993.