Arithmetic Progressions with Three Parts in Prescribed Ratio and a Challenge of Fermat

Kenneth Fogarty Cormac O'Sullivan Bronx Community College City University of New York Bronx, NY 10453 kwfogarty@dmcom.net cormac.osullivan@bcc.cuny.edu

The arithmetic progression 1, 2, 3 can be broken into two consecutive pieces that have equal sums by the relation 1 + 2 = 3. The first author, in the problem pages of the journals [1] and [2], wondered if an arithmetic progression could be found that breaks into *three* consecutive pieces with equal sums. Here are some examples that come close:

$$4+5+6 = 7+8 = (9+10+11)/2,$$

$$3+5+7+9 = 11+13 = (15+17+19+21)/3,$$

$$(6+7+8+9)/2 = (10+11+12+13+14)/4 = 15$$

This appealing question has a simple answer that turns out to be related to a certain Diophantine equation considered by Euler, namely

$$x^4 - x^2 y^2 + y^4 = z^2 \tag{1}$$

where we are looking for integer solutions. In turn (1) is related to the possibility of finding four squares as the consecutive terms of an arithmetic progression, a challenge issued by Fermat in 1640. We'll unravel this connection and further address the question of arithmetic progressions with three parts in other fixed ratios. We close the article with four open questions which we hope the reader will take as an invitation to further explore some of the mysteries of Diophantine equations.

Reduction to a Diophantine equation

So far we have been talking about sequences of integers. We may just as easily ask these questions for arithmetic progressions of real numbers. By an *n*-term arithmetic progression we therefore mean real numbers e_1, e_2, \dots, e_n with common difference $e_{i+1} - e_i = \Delta > 0$ for $1 \leq i < n$. If n = a + b + c, with positive integers a, b, c, let

$$S_1 = \sum_{i=1}^{a} e_i, \ S_2 = \sum_{i=a+1}^{a+b} e_i, \ S_3 = \sum_{i=a+b+1}^{n} e_i$$
(2)

be the sums of the first a, the middle b and the final c terms.

The question we are trying to answer in this article is: What are the possibilities for the ratios $S_1 : S_2 : S_3$? In particular, as we investigate in this section, can we ever have $S_1 = S_2 = S_3$? Clearly dividing each term in an arithmetic progression by the same number does not alter the ratios $S_1 : S_2 : S_3$ so after dividing by Δ we may make the simplifying assumption that the common difference of our progressions is always 1. Using $1+2+\cdots+n=n(n+1)/2$ we have

$$\begin{split} 2S_1 &= a(2e_1-1+a) = a(2e_{a+1}-1-a), \\ 2S_2 &= b(2e_{a+1}-1+b) = b(2e_{a+b+1}-1-b), \\ 2S_3 &= c(2e_{a+b+1}-1+c). \end{split}$$

Setting $S_1 = S_2$ we find

$$2e_{a+1} - 1 = \frac{a^2 + b^2}{a - b}.$$
(3)

Similarly $S_2 = S_3$ implies

$$2e_{a+b+1} - 1 = \frac{b^2 + c^2}{b - c}.$$
(4)

Since $e_{a+b+1} = e_{a+1} + b$ we may solve for e_{a+1} in equations (3) and (4) to get

$$2b = \frac{b^2 + c^2}{b - c} - \frac{a^2 + b^2}{a - b}.$$

Rearranging we obtain the relation

$$ab^{2} + a^{2}b + bc^{2} + b^{2}c - ac^{2} - a^{2}c - 2abc = 0.$$
 (5)

Note that if any two of the positive integers a, b, c are equal then (5) implies that all three must be equal. Therefore by (3) and (4) we must have a, b, c all distinct.

PROPOSITION 1. There exists an arithmetic progression with beginning, middle and end having equal sums (with a, b and c terms respectively) if and only if there exist positive distinct integers a, b, c satisfying equation (5).

Proof. We have proved one direction. In the other, given such a, b, c let e_{a+1} be the rational number satisfying equation (3) and set $e_1 = e_{a+1} - a$. Then, as we have seen, the arithmetic progression $e_1, e_1+1, \dots, e_1+a+b+c-1$ has the desired property. Also note that, if we like, we can make each term an integer by multiplying by 2(a - b). This completes the proof.

Suppose we have integers a, b, c satisfying (5). Trying to solve for b we get

$$b^{2}(a+c) + b(a-c)^{2} - ac(a+c) = 0$$
(6)

which has discriminant

$$\delta = (a - c)^4 + 4ac(a + c)^2 = a^4 + 14a^2c^2 + c^4$$

Set p = a + c and q = a - c then $\delta = q^4 + p^2(p^2 - q^2)$. We have $b = (\sqrt{\delta} - q^2)/(2p)$ which implies that we must have

$$p^4 - p^2 q^2 + q^4 = r^2 \tag{7}$$

for some r. Conversely if p and q are integers satisfying (7) then

$$a = p(p+q), \ b = \sqrt{p^4 - p^2 q^2 + q^4} - q^2, \ c = p(p-q)$$

are easily shown to satisfy (6). In this way (5) and (6) have solutions if and only if (7) does. Equations like this, where we are concerned with finding only integer or only rational solutions, are called Diophantine equations in honor of Diophantus of Alexandria who lived in the third century, it is thought [3], and wrote the *Arithmetic* where many such equations are solved.

In fact $p^4 - p^2q^2 + q^4$ can be a square only if $p = \pm q$ or pq = 0. This is a result of Euler [4]. For completeness we include an elegant proof by "infinite descent" of this fact due to Pocklington [5]. The result is also mentioned in Dickson's encyclopedic *History of the Theory of Numbers* [6, p. 638].

This method of proof, first employed by Fermat, is very useful in proving negative statements such as that a certain equation has no (or only trivial) integer solutions. As we shall see, from an assumed initial solution to an equation a new, strictly smaller, solution is constructed. Repeat the argument and an infinite chain of solutions, descending in size, appears. But this contradicts the fact that our solutions are bounded positive integers and hence finite in number. Thus our initial assumption of a solution to the equation was false.

Pocklington's proof uses the following well known result parameterizing Pythagorean triples.

LEMMA 2. Let $x^2 + y^2 = z^2$ for positive integers x, y, z with gcd(x, y) = 1. 1. Necessarily one of x, y (say y) is even and there exist integers u, v with gcd(u, v) = 1, u > v > 0 such that

$$x = u^2 - v^2$$
, $y = 2uv$, $z = u^2 + v^2$.

For a proof see the classic text by Hardy and Wright [7, Theorem 225].

PROPOSITION 3. If $p^4 - p^2q^2 + q^4 = r^2$ for positive integers p, q then p = q.

Proof. Assume that p, q > 0 are integer solutions to the above equation with gcd(p,q) = 1. Suppose also that q is even (we will treat the case of p, q odd later) and that pq is minimal. We have

$$(p^2 - q^2)^2 + (pq)^2 = r^2$$
(8)

and $gcd(p^2 - q^2, pq) = 1$ so that, by the lemma,

$$p^2 - q^2 = u^2 - v^2, (9)$$

$$pq = 2uv. (10)$$

Considering the first equation (9) modulo 4 we see that v is even. In plainer language, since a square must have remainder 0 or 1 when divided by 4, the only possibility is that v^2 is divisible by 4. Next let

$$\alpha = \gcd(p, u), \ \beta = \gcd(p, v), \ \gamma = \gcd(q, u), \ \delta = \gcd(q, v)$$

with α, β, γ odd and δ even. We have by (10)

$$p = \alpha \beta, \ q = 2\gamma \delta, \ u = \alpha \gamma, \ v = \beta \delta.$$

Putting these back into (9) we obtain

$$\beta^2(\alpha^2 + \delta^2) = \gamma^2(\alpha^2 + 4\delta^2). \tag{11}$$

We want to demonstrate next that $gcd(\alpha^2 + \delta^2, \alpha^2 + 4\delta^2)$ equals 1 or 3. To see this suppose d divides both $A = \alpha^2 + \delta^2$ and $B = \alpha^2 + 4\delta^2$. Then dwill be a divisor of $B - A = 3\delta^2$ and $4A - B = 3\alpha^2$. Since α and δ are relatively prime d must be a factor of 3. Taking d as large as possible shows that $gcd(\alpha^2 + \delta^2, \alpha^2 + 4\delta^2)$ is a factor of 3 as we said. But it cannot be 3 since 3 does not divide $\alpha^2 + \delta^2$ (squares must have remainders 0 or 1 when divided by 3). So we've managed to show that $gcd(\alpha^2 + \delta^2, \alpha^2 + 4\delta^2) = 1$. Combine this with the easy fact that $gcd(\beta, \gamma) = 1$ and we see which parts of each side of (11) are relatively prime. Hence we must have

$$\beta^2 = \alpha^2 + (2\delta)^2, \tag{12}$$

$$\gamma^2 = \alpha^2 + \delta^2. \tag{13}$$

Applying the lemma again to (12) we find $\alpha = \xi^2 - \eta^2$ and $\delta = \xi \eta$. Replacing these in (13) we get

$$(\xi^2 - \eta^2)^2 + (\xi\eta)^2 = \gamma^2.$$

This is of the same form as the original equation and we see that

$$\xi \eta = \delta < 2\gamma \delta = q < pq,$$

contradicting the initial claim that pq was minimal and proving that there are no solutions with p or q even.

We treat the remaining case that solutions p, q are both odd. Equation (8) and the lemma now imply that

$$p^2 - q^2 = 2uv, \ pq = u^2 - v^2,$$

provided $p \neq q$. Also one of u, v is necessarily even. Therefore

$$(u^2 - v^2)^2 + (uv)^2 = (pq)^2 + \frac{(p^2 - q^2)^2}{4} = \left(\frac{p^2 + q^2}{2}\right)^2$$

which we have already seen is impossible. This completes the proof of the proposition.

So, if we look for a solution to (5) with positive distinct integers a, b, cand a > c > 0 say, then we must have p = a + c = a - c = q implying that c = 0. Thus we have answered our original question.

PROPOSITION 4. It is impossible for an arithmetic progression to have equal beginning, middle and end sums.

Four squares in arithmetic progression

Fermat wrote to Mersenne in May 1640, [8]. He included four challenges for Frenicle de Bessy, a number theorist in Paris:

Pour savoir si M. Frenicle ne procède point par tables, proposez lui de

- (i) Trouver un triangle rectangle duquel l'aire soit un nombre quarré;
- (ii) Trouver deux quarréquarrés desquels la somme soit quarréquarrée;
- (iii) Trouver quatre quarrés en proportion arithmétic continue;
- (iv) Trouver deux cubes desquels la somme soit cube;

S'il vous répond que jusques à un certain nombre de chiffres il a éprouvé que ces questions ne trouvent point de solution, assurezvous qu'il procède par tables.

The first asks for a right-angled triangle (with integer length sides) whose area is a square. Using lemma 2 this reduces to finding integer solutions for $x^4 - y^4 = z^2$ as shown in [6, p. 615].

The fourth and second ask for solutions to $x^3 + y^3 = z^3$ and $x^4 + y^4 = z^4$. This was only the second time he had mentioned to his correspondents these cases of what became known as his Last Theorem. In about 1636 he sent Mersenne the same two problems and asked him to propose them to St. Croix. According to Dickson it was probably soon after, in 1637, that he made his famous note in the margin of his copy of Diophantus' Arithmetic.

The third challenge asks for four squares in arithmetic progression and this turns out to be related to our original question. Fermat seems to have been the first to look for such squares [6, p. 440]. That they do not exist follows from the fact that $x^4 - x^2y^2 + y^4 = z^2$ has only trivial solutions. We cannot be sure, but this might be what Fermat had in mind.

We can prove that four squares cannot be in arithmetic progression quite easily using proposition 4 and the fact that the sum of the first n odd numbers is the nth square

$$1 + 3 + 5 + \dots + (2n - 1) = n^2$$
.

(This has an easy geometric proof - can you find it? See Nelsen's proof without words [9] for something similar.) Thus if A^2, B^2, C^2, D^2 are four consecutive terms of an arithmetic progression with 0 < A < B < C < D we can take the sequence of consecutive odd numbers $2A + 1, 2A + 3, \dots, 2D - 1$ and see that

$$(2A+1) + (2A+3) + \dots + (2B-1) = (2B+1) + (2B+3) + \dots + (2C-1)$$
$$= (2C+1) + (2C+3) + \dots + (2D-1)$$

which contradicts proposition 4.

By the same reasoning we cannot have four triangular numbers in arithmetic progression. More generally it follows from proposition 4 that for any integers A, B, C, D and any real r we cannot have

$$A(A+r), B(B+r), C(C+r), D(D+r)$$

in arithmetic progression.

Euler's contribution

Euler proved in 1780 [4] that the product of four consecutive positive terms of an arithmetic progression cannot be a square. We will apply this result to find another proof of proposition 4. Assume that we have an arithmetic progression with equal beginning, middle and end sums. It leads to a solution of (6). We may rewrite (6) as

$$b(a-c)^2 = (a+c)(ac-b^2).$$

Letting p = a + c, q = a - c as before we find

$$4bq^2 = p(p^2 - q^2 - 4b^2)$$

and consequently

$$q^{2}(p+4b) = (p-2b)p(p+2b)$$

In terms of a, b, c this is

$$(a-c)^{2}(a+c+4b) = (a+c-2b)(a+c)(a+c+2b).$$

If we multiply both sides of the above by (a + c + 4b) we see that

$$(a+c-2b)(a+c)(a+c+2b)(a+c+4b)$$

is a square. According to Euler this is impossible and we have a second proof of proposition 4.

To close this circle of ideas we prove Euler's result. Suppose that there exist relatively prime integers $m, n \ge 1$ so that

$$m(m+n)(m+2n)(m+3n) = r^2.$$
(14)

We must have gcd(m, m + 2n) dividing 2, gcd(m + n, m + 3n) dividing 2 and gcd(m, m + 3n) dividing 3, eight possibilities in all. This means that any prime bigger than 3 cannot appear in different terms of the factorization on the left-hand side of (14). Thus m, m + n, m + 2n and m + 3n are each squares except for possible extra factors of 2 or 3. Checking the eight cases we see, for example, that $\{m, m + n, m + 2n, m + 3n\} = \{2A^2, B^2, 2C^2, D^2\}$ is not possible. This is because dividing $2A^2, B^2, 2C^2$ and D^2 by 4 produces remainders 2, 1, 2 and 1 if each of A, B, C and D are odd. But no arithmetic progression can have such remainders. One of A, B, C and D may be even but here too, checking each case, the remainders do not correspond to arithmetic progressions. It is routine to verify, modulo 3 and 4, that the only three possibilities for m, m + n, m + 2n and m + 3n are

- (i) $\{A^2, B^2, C^2, D^2\}$
- (ii) $\{6A^2, B^2, 2C^2, 3D^2\}$ or
- (iii) $\{3A^2, 2B^2, C^2, 6D^2\}$

with A, B, C and D relatively prime in pairs. We know that (i) is impossible. We'll prove that (ii) cannot occur. Employ the identity

$$2(m(m+2n) - (m+n)(m+3n)) = m(m+n) - (m+2n)(m+3n)$$

from [5] to get

$$4A^2C^2 - B^2D^2 = A^2B^2 - C^2D^2.$$
 (15)

Set

$$\alpha = 2AC, \quad \beta = BD, \quad \gamma = AB + CD \quad \text{and} \quad \delta = AB - CD.$$
 (16)

Then we obtain $\alpha^2 - \beta^2 = \gamma \delta$ from (15) and $2\alpha\beta = \gamma^2 - \delta^2$ from (16). Therefore

$$(\alpha^2 - \beta^2)^2 + \alpha^2 \beta^2 = \xi^2$$

for some ξ and by proposition 3 we must have $\alpha = \beta$ which yields a contradiction. Part (iii) follows with an identical argument (as does part (i)) and this completes the proof.

Euler [4] used a slightly different approach. See also the discussion in Dickson [6, p. 635]. Interestingly, finding integer solutions to the general equation

$$m(m+n)(m+2n)\cdots(m+(k-1)n) = r^w,$$
 (17)

(or showing they don't exist) has resisted many authors. The case with n = 1 has a long history as described in Johnson [10] where relatively simple proofs of various cases are given. It was eventually completely settled by Erdös and Selfridge in a paper entitled "The product of consecutive integers is never a power", [11]. Recently Saradha [12] has shown that the only nontrivial solution to (17) (with $k \ge 3$ and $n \le 22$ and w = 2) has (m, n, k) = (18, 7, 3).

Back to Fermat's four challenges

Returning to Fermat's four challenges, we have seen that their impossibility follows, respectively, from the lack of nontrivial solutions to the Diophantine equations

- (i) $x^4 y^4 = z^2$,
- (ii) $x^4 + y^4 = z^2$,
- (iii) $x^4 x^2y^2 + y^4 = z^2$,
- (iv) $x^3 + y^3 = z^3$.

Frenicle did finally prove that $x^4 - y^4 = z^2$ has no nontrivial solutions with help from Fermat, [6, p. 617]. He also came up with a formula supplying three squares in progression [6, p. 435]. But it fell to Euler to prove the impossibility of the first two cases of Fermat's Last Theorem [6, p. 545, p. 618] and that four squares cannot be in a progression as we have seen [4].

Did Fermat himself have proofs? He certainly claimed that all four had only trivial solutions. We can only know with certainty that he had proved (i) and (ii). These two proofs, essentially identical, are rare examples of Fermat supplying his detailed arguments [6, p. 615], [13, p. 79]. Quoting from Weil, [13, p. 114]: "At that early date, Fermat had perhaps no more than plausibility arguments for the fact that these problems have no solution; but eventually he must have obtained a formal proof also for the third one, since we are told so by Billy in his *Inventum Novum*", [14].

We cannot be sure what this formal proof of (iii) was since no trace of it appears in Fermat's writings. Weil laments that Billy did not find out more: "How grateful we should be to the good Jesuit, had he shown some curiosity toward such 'negative' statements ..."

One candidate is that he worked directly with the equation $x^4 - x^2y^2 + y^4 = z^2$ and showed it has only trivial solutions using a proof like that of proposition 3. This is appealing because the equations (i) to (iv) above are so similar.

A second way, outlined by Weil and based on subsequent results of Euler that Fermat may have anticipated, is to work with the elliptic curve

$$y^{2} = -x(x-1)(x-4).$$
(18)

It may be shown by descent that this curve has only trivial rational solutions. This implies that four squares cannot be in arithmetic progression, as shown in [13, pp. 130 - 149]. It is an easy exercise to transform (14) into (18). This is done by Erdélyi [15].

A third approach, due to Erdélyi [15], is to rewrite (14) as

$$(m2 + 3mn + n2)2 = r2 + n4.$$
 (19)

He then shows, using lemma 2, that any solution in positive integers of (19) is impossible because each solution yields another making the quantity

(m+n)(m+2n) smaller. This again is a classical proof by descent that Fermat could have used (he, of course, invented this technique). So, in summing up, there is no shortage of plausible ways Fermat could have proved this theorem.

As for the final challenge (iv), the proof of the impossibility of $x^3 + y^3 = z^3$ can be made to follow the same general lines but is harder than the others. It was probably not out of the reach of the 'Prince of Amateurs' though, see the discussion in Mahoney's biography of Fermat [16, p. 357] and also Weil's thoughts [13, p. 118].

Arithmetic progressions with other ratios

We extend the discussion by letting $(S_1 : S_2 : S_3)$ denote the ratios of the sums (2). We have shown that (1 : 1 : 1) is impossible. Here are some ratios involving the numbers 1, 2, 3 that are possible:

(1:1:2)	4, 5, 6; 7, 8; 9, 10, 11,	
(1:1:3)	$1, 2; \ 3; \ 4, 5,$	
(1:2:2)	6, 7, 8; 9, 10, 11, 12; 13, 14, 15	
(1:2:3)	1; 2; 3,	
(1:3:2)	3; 4, 5; 6,	
(1:3:3)	2, 3; 4, 5, 6; 7, 8,	
(2:1:3)	12, 13, 14, 15, 16; 17, 18; 19, 20, 21, 22, 23.	(20)

Of course by changing the signs of each term in a sequence we can get the ratios in reversed order so that for example -5, -4; -3; -2, -1 yields (3 : 1 : 1). As with proposition 1 we may reduce the existence question to a Diophantine equation.

PROPOSITION 5. There exists an arithmetic progression with three parts of a, b and c terms and $(S_1 : S_2 : S_3) = (x : y : z)$ if and only if there exist positive integers a, b, c satisfying

$$(xb - ya)c(b + c) + (zb - yc)a(a + b) = 0$$
(21)

with the restriction $xb \neq ya$ (or equivalently $zb \neq yc$).

We leave the proof to the reader. If this sequence exists and its terms differ by 1 then, similarly to (3), its first term e_1 must satisfy

$$2e_1 = \frac{ya^2 + xb^2}{ya - xb} - 2a + 1.$$

In the examples (20) we always have a = c. This is not a coincidence. When a = c equation (21) reduces to xb - ya = ya - zb or 2ya = (x + z)band the restriction becomes $x \neq z$. This yields

PROPOSITION 6. For positive integers x, y, z with $x \neq z$ there exists an arithmetic progression with three parts in ratio $(S_1 : S_2 : S_3) = (x : y : z)$.

Proof. We may simply take a = c = x + z and b = 2y. By proposition 5 the desired progression exists completing the proof.

From this we obtain, for example

- (2:2:3) 16, 17, 18, 19, 20; 21, 22, 23, 24; 25, 26, 27, 28, 29,
- (2:3:3) 20, 21, 22, 23, 24; 25, 26, 27, 28, 29, 30; 31, 32, 33, 34, 35.

Note that, since (21) is homogeneous in a, b and c, any single solution yields an infinite family of solutions $\lambda a, \lambda b, \lambda c$ for λ a positive integer.

Next we look for progressions with ratios (x : y : x). One way to solve (21) is to look for solutions of the form c(b+c) = wa(a+b) and xb-yc = w(ya-xb). From the first of these equations let c = a + b and wa = b + c. Therefore a = 2, b = w - 1, c = w + 1 and we require w > 1. This yields arithmetic progressions with ratios $(3w + 1 : w^2 - 1 : 3w + 1)$ parameterized by w > 1. This solution, (when w = 5 and after multiplying by -2) gives

$$(2:3:2)$$
 3, 5, 7, 9, 11, 13; 15, 17, 19, 21; 23, 25.

A simpler example for this ratio is 1, 2, 3; 4, 5; 6. The remaining possibilities for ratios involving 1, 2, 3 are (1 : 2 : 1), (1 : 3 : 1), (2 : 1 : 2), (3 : 1 : 3) and (3 : 2 : 3). Trying to solve (21) for b we have

$$b^{2}(xc + za) + b(za^{2} + xc^{2} - 2yac) - yac(a + c) = 0.$$

A necessary and sufficient condition for integer solutions is that the discriminant

$$z^{2}a^{4} + x^{2}c^{4} + (2(2y+x)(2y+z) - 4y^{2})a^{2}c^{2}$$

is a square. Looking for the ratio (2 : 1 : 2), for example, we need $a^4 + 7a^2c^2 + c^4$ to be a square. Using the techniques of proposition 3 it can be seen [5], [17] that this is impossible. Thus no arithmetic progression exists with beginning and end sums twice the middle sum. The other four possibilities are unresolved.

We finish with four challenges to the reader:

- (i) For which values of x, y is (x : y : x) a set of possible ratios for an arithmetic progression?
- (ii) For positive integers x, y, z with x ≠ z is there a way to construct an arithmetic progression with the ratio (x : y : z) and strictly positive terms? For example with (x : y : z) = (3 : 2 : 1) proposition 6 yields -3; -2; -1 but with more work we find

(3:2:1) 9, 10, 11, \cdots , 24, 25, 26; 27, 28, 29, 30, 31, 32, 33; 34, 35, 36.

- (iii) How many arithmetic progressions (with common difference $\Delta = 1$ say and parts of any size a, b, c but with gcd(a, b, c) = 1) can represent a given ratio (x : y : z)?
- (iv) When is it possible for the product of m consecutive terms of an arithmetic progression to be an nth power?

Acknowledgment We thank the anonymous referees for their many improvements to the exposition and the additional reference.

References

 NY State Math. Teachers' Journal, Edited by M. C. Sachs, 48 (1998), no. 1, 56.

- [2] NY State Math. Teachers' Journal, Edited by E. C. Wallace, 49 (1999), no. 1, 56.
- [3] I. G. Bashmakova, *Diophantus and Diophantine equations*, Mathematical Association of America, 1997.
- [4] L. Euler, Mém. Acad. Sc. St. Petersbourg 8 années 1817-18, Euler Opera Omnia, Ser 1, Edited by R. Fueter, vol. 5, 1944, pp. 48–60. (Latin)
- [5] H. C. Pocklington, Some Diophantine Impossibilities, *Cambridge Phil. Soc.* 17 (1914), 108–121.
- [6] L. E. Dickson, *History of the theory of numbers*, vol. II, Chelsea, 1920.
- [7] G. H. Hardy and E. M. Wright, An introduction to the theory of numbers, 5th ed., Clarendon Press, 1979.
- [8] Oeuvres de Fermat, Edited by C. Henry and P. Tannery, vol. II, 1894, pp. 194–195.
- [9] R. B. Nelsen, Proof Without Words: The Cube as an Arithmetic Sum, this MAGAZINE, 76 (2006), no. 2, 136.
- [10] L. Johnson, On the Diophantine Equation $x(x+1)\cdots(x+n-1) = y^k$, Amer. Math. Monthly, **47** (1940), no. 5, 280–289.
- [11] P. Erdös and J. L. Selfridge, The product of consecutive integers is never a power, *Illinois J. Math.* **19** (1975), 292–301.
- [12] N. Saradha, Squares in products with terms in an arithmetic progression, Acta Arithmetica 86 (1998), no. 1, 27–43.
- [13] A. Weil, Number Theory, An approach through history, Birkhauser, 1984.
- [14] J. de Billy, Inventum Novum, Oeuvres de Fermat, Editored by C. Henry and P. Tannery, vol. III, 1894, pp. 325–398.

- [15] T. Erdélyi, On the equation $a(a+d)(a+2d)(a+3d) = x^2$, Amer. Math Monthly 107 (2000), no. 2, 166–169.
- [16] M. S. Mahoney, The Mathematical Career of Pierre de Fermat, 2nd ed., Princeton Univ. Press, 1994.
- [17] J. H. E. Cohn, Squares in arithmetic progressions I, II, Math. Scand. 52 (1983), no. 1, 5–23.