ON SUMS OF CONSECUTIVE TRIANGULAR NUMBERS

Dipika Subramaniam
Department of Mathematics and Computer Science, Lake Forest College, Lake Forest, Illinois
subramaniamd@mx.lakeforest.edu

Enrique Treviño
Department of Mathematics and Computer Science, Lake Forest College, Lake Forest, Illinois
trevino@lakeforest.edu

Paul Pollack
Department of Mathematics, University of Georgia, Athens, Georgia
pollack@uga.edu

Received: , Revised: , Accepted: , Published:

Abstract

By a *triangular number*, we mean one of the numbers $\Delta_n := \frac{1}{2}n(n+1)$, for $n = 1, 2, 3, \ldots$. In a recent *Math Horizons* note, Matthew McMullen suggested studying triangular sums of consecutive triangular numbers. In other words, one seeks solutions to equations of the form

$$\Delta_n + \cdots + \Delta_{n+(k-1)} = \Delta_m.$$

McMullen classified the solutions when $2 \le k \le 5$; there are no solutions when $k = 4$, while in the other cases, there are infinitely many solutions. He asked if there is a value of $k > 4$ for which there are no solutions. Here we show that there are solutions for every square value of k larger than 4, but that for almost all values of k (asymptotically 100%), there are no solutions.

1. Introduction

By a *triangular number*, we mean a member of the sequence

$$\Delta_n := \frac{1}{2}n(n+1), \qquad n = 1, 2, 3, \ldots.$$

(Some authors include 0 as a triangular number; for our purposes it is convenient to leave 0 out.) Triangular numbers feature prominently in the history of number theory. Probably the most famous example is the July 10, 1796 entry in Gauss's mathematical diary (see [4]):

ΕΥΡΗΚΑ! $\mathrm{num} = \Delta + \Delta + \Delta$.

Expressed in less telegraphic notation: Every positive integer is a sum of three triangular numbers, where 0 is allowed. About 30 years later (1828), in a treatise on elliptic functions, Legendre published a simple formula for the number of representations of a nonnegative integer n as a sum of four triangular numbers (again, allowing 0): For every $n \in \mathbb{N}_0$,

$$\#\{(x,y,z,w) \in \mathbb{N}_0 : \frac{x(x+1)}{2} + \frac{y(y+1)}{2} + \frac{z(z+1)}{2} + \frac{w(w+1)}{2} = n\} = \sigma(2n+1),$$

where $\sigma(m) = \sum_{d|m} d$.

In a recent note in *Math Horizons* [7], McMullen suggested investigating the solutions to equations of the form

$$\Delta_n + \cdots + \cdots + \Delta_{n+(k-1)} = \Delta_m. \tag{1}$$

In other words: When is a sum of consecutive triangular numbers also triangular? McMullen found all solutions for $k = 2, 3, 4, 5$; when $k = 4$ there is no solution, while in the three other cases, there are infinitely many solutions, corresponding to solutions to certain Pell equations. The note ends with the following question:

> Every value of k except $k = 4$ that I looked at yields at least one valid solution. Is there a $k > 4$ where our problem has no solution?

We prove two theorems concerning solutions to (1). First, we show that $k = 4$ is the only square value for which (1) lacks solutions.

Theorem 1. *Let $k > 4$ be a square. Then* (1) *has solutions. In other words, there* do *exist k consecutive triangular numbers that add up to a triangular number.*

In the opposite direction, we show that for almost all values of k, there are no solutions to (1). Thus, the answer to McMullen's question is a definite YES !

Theorem 2. *Let $K(x)$ denote the number of integers $2 \leq k \leq x$ for which* (1) *has solutions. Then $K(x) = O(x/(\log x)^{1/2})$. In particular, $K(x)/x \to 0$, so that the set of k for which* (1) *is solvable has asymptotic density* 0.

Theorem 1 obviously implies that $K(x) \gg \sqrt{x}$. There is a large gap between $\sqrt{x}$ and $x/(\log x)^{1/2}$, and it is natural to ask which of these functions is closer to the truth about $K(x)$. We believe it is the latter; indeed, we conclude the paper with a heuristic argument suggesting that $K(x) \gg x/(\log x)^{3/2}$.

2. When k is a square: Proof of Theorem 1

Elementary manipulations show that (1) is equivalent to

$$(2m+1)^2 - k(2n+k)^2 = \frac{(k-1)(k^2+k-3)}{3}. \tag{2}$$

Up to this point we have not used that k is a square. But if we now let $k = a^2$, then (2) becomes

$$(2m+1-a(2n+a^2))(2m+1+a(2n+a^2)) = \frac{(a-1)(a+1)(a^4+a^2-3)}{3}. \tag{3}$$

(This factorization is noted already in [7].) To prove Theorem 1, we must show that (3) has a solution in positive integers m, n. We consider separately the cases when a is even vs. when a is odd.

2.1. When a is even

Since k is even, we have $a \geq 3$. Choosing

$$m = \frac{a^2(a^2-2)(a^2+2)}{12}, \quad n = \frac{a(a-2)(a^3+2a^2+4a+2)}{12},$$

the first factor on the left-hand side of (3) is 1, while the second factor is equal to the right-hand side of (3); thus, (3) holds. Since a is even, both numerators in the expressions defining m and n are multiples of 4. Taking cases for a mod 3, we find that both numerators are also multiples of 3. Thus, m and n are integers. Finally, since $a \geq 3$, one sees easily that $m, n > 0$.

2.2. When a is odd

In this case, the left-hand side of (3) is a product of two even numbers. Dividing by 2 leads to the system of equations

$$\begin{aligned} m - an + \frac{1-a^3}{2} &= d \\ m + an + \frac{1+a^3}{2} &= d', \end{aligned} \tag{4}$$

for some positive integers d and d' satisfying

$$dd' = \frac{(a-1)(a+1)(a^4+a^2-3)}{12}. \tag{5}$$

We subdivide this case further according to the value of a modulo 3:

- When $a \equiv 1 \pmod 3$, both $d = \frac{a+1}{2}$ and $d' = \frac{(a-1)(a^4+a^2-3)}{6}$ are positive integers, and (5) holds. Solving (4) with these values of d, d' leads to

  $$m = \frac{a^2(a-1)(a^2+1)}{12}, \quad n = \frac{(a+2)(a-3)(a^2+1)}{12}.$$

  Reasoning as in the case of even a, we find that m, n are positive integers.

- If $a \equiv 0$ or 2 mod 3, then $d = \frac{a-1}{2}$ and $d' = \frac{(a+1)(a^4+a^2-3)}{6}$ are positive integers. These choices lead to

  $$m = \frac{a^5+a^4+a^3+a^2-12}{12}, \qquad n = \frac{(a+3)(a-2)(a^2+1)}{12}.$$

  Again, one checks easily that m, n are positive integers.

3. Equation (1) usually has no solutions: Proof of Theorem 2

We require the following lemma.

Lemma 3. *Let $q > 3$ be a prime number. Suppose that $k \in \mathbb{Z}$ is such that*

(i) *k is not a square modulo q,*

(ii) *$q \parallel k^2 + k - 3$.*

Then there are no k consecutive triangular numbers that add up to a triangular number.

Proof. Assume for a contradiction that k satisfies (i) and (ii) but that (1) has a solution. Then there are positive integers m, n satisfying (2). Let $x = 2m + 1$ and $y = 2n + k$, so that $x^2 - ky^2$ represents the left-hand side of (2). Condition (i) guarantees that k is not congruent to 1 modulo q. Thus, q is coprime to $k - 1$. Condition (ii) now implies that

$$q \parallel \frac{(k-1)(k^2+k-3)}{3} = x^2 - ky^2.$$

If q divides one of x or y, then q divides the other, since $x^2 \equiv ky^2 \pmod{q}$ and q is coprime to k. But then $q^2 \mid x^2 - ky^2$, a contradiction. So q is coprime to both x and y, forcing $(x/y)^2 \equiv k \pmod{q}$. This contradicts (i). $\square$

We will also use the following consequence of the Chebotarev density theorem (or the weaker Frobenius density theorem); a readable modern reference is [8].

Proposition 4. *Suppose that $f(x) \in \mathbb{Z}[x]$ is monic and irreducible over $\mathbb{Q}$, with $\deg f(x) = n$. Let L be the splitting field of $f(x)$ over $\mathbb{Q}$. Fix a partition $\langle k_1, \ldots, k_r \rangle$ of n (that is, a tuple of positive integers $k_1 \geq k_2 \geq \cdots \geq k_r$ with $k_1 + \cdots + k_r = n$). Let δ be the proportion of elements of $\mathrm{Gal}(L/\mathbb{Q})$ which, when viewed as permutations on the roots of $f(x)$, have cycle type $\langle k_1, \ldots, k_r \rangle$. For all but finitely many primes p, the polynomial $f(x)$ factors as a product of distinct monic irreducible polynomials modulo p, and δ is the proportion of primes for which these irreducibles have degrees $k_1, \ldots, k_r$.*

In Proposition 4, "proportion of primes" is meant in the same sense as in the Chebotarev density theorem. The version of that theorem proved by Artin in [1] implies that the number of primes $p \leq x$ for which f factors mod p into irreducibles of degrees $k_1, \ldots, k_r$ is

$$\delta \cdot \pi(x) + O(x/(\log x)^2). \tag{6}$$

(In (6), the implied constant is allowed to depend on f, which we view as fixed.)

Lemma 5. *Let $\mathcal{A}$ be the set of primes p for which the polynomial $g(x) = x^2 + x - 3$ has two distinct roots mod p, neither of which is a square mod p, and let $\mathcal{B}$ be the set of primes p for which $g(x)$ has two distinct roots mod p, exactly one of which is a square mod p. The proportion of primes in $\mathcal{A}$ is $\frac{1}{8}$, while the proportion of primes in $\mathcal{B}$ is $\frac{1}{4}$.*

Proof. Let $f(x) = x^4 + x^2 - 3$. Then f is irreducible over $\mathbb{Q}$, the splitting field L of f over $\mathbb{Q}$ has degree 8, we have $\mathrm{Gal}(L/\mathbb{Q}) \cong D_4$, and under an appropriate numbering of the roots of f, the Galois group of $L/\mathbb{Q}$ can be identified with the subgroup

$$\{(1), (1324), (12)(34), (1423), (34), (13)(24), (12), (14)(23)\}$$

of S_4. All of this follows immediately from the easily-checkable criteria of [6] concerning quartics $x^4 + ax^2 + b$; see in particular that paper's Theorems 2 and 3.

Suppose that $p \in \mathcal{A}$. Thus, g splits over $\mathbb{F}_p$,

$$g(x) = (x - \theta_1)(x - \theta_2) \quad \text{for some } \theta_1 \neq \theta_2 \in \mathbb{F}_p.$$

Moreover,

$$f(x) = g(x^2) = (x^2 - \theta_1)(x^2 - \theta_2),$$

where the two quadratic factors are distinct and irreducible over $\mathbb{F}_p$. Conversely, suppose that g splits over $\mathbb{F}_p$ and that f factors as a product of distinct monic irreducibles of degree 2. Then the roots of g, say θ_1 and θ_2, must be nonsquares in $\mathbb{F}_p$; otherwise, $x^2 - \theta_1$ or $x^2 - \theta_2$ will contribute a linear factor to f. Thus, using Prob to denote proportions of primes (the notation chosen to suggest probability), we see that

$$\text{Prob}(p \in \mathcal{A}) = \text{Prob}(g \text{ splits } \& \ f \text{ factors as } \langle 2, 2\rangle).$$

(When we write "f factors as $\langle k_1, \ldots, k_r\rangle$", we mean that f factors as a product of distinct monic irreducibles of degrees $k_1, \ldots, k_r$.)

We may rewrite the right-hand side of the last display as

$$\begin{aligned}&\text{Prob}(g \text{ splits}) - \text{Prob}(g \text{ splits } \& \ f \text{ factors as } \langle 4\rangle) - \\ &\qquad \text{Prob}(g \text{ splits } \& \ f \text{ factors as } \langle 2,1,1\rangle) - \text{Prob}(g \text{ splits } \& \ f \text{ factors as } \langle 1,1,1,1\rangle).\end{aligned}$$

The first subtracted term is 0; if g has the root θ mod p, then $x^2 - \theta$ is a factor of f over $\mathbb{F}_p$, so f cannot be irreducible. The final two subtracted terms are unchanged if we omit the condition that g splits. Indeed, f factoring as $\langle 2,1,1\rangle$ or $\langle 1,1,1,1\rangle$ implies that f has a root θ; then f also has the root $-\theta$, and as long as $q \neq 3$, those two roots are distinct. Hence, $x^2 - \theta^2 \mid f(x) = g(x^2)$. But this implies that θ^2 is a root of g. Since g is a quadratic with a root, g splits. (The roots are distinct since we are assuming $f(x) = g(x^2)$ factors as a product of distinct monic irreducibles.) So by Proposition 4 together with our determination of the Galois group of f, these final two probabilities are $\frac{2}{8}$ and $\frac{1}{8}$, respectively. Finally, the probability that g splits mod p is $\frac{1}{2}$, by applying Proposition 4 to g. We conclude that

$$\text{Prob}(p \in \mathcal{A}) = \frac{1}{2} - 0 - \frac{2}{8} - \frac{1}{8} = \frac{1}{8}.$$

A similar argument works to determine $\text{Prob}(p \in B)$. Here it is easy to see that

$$\text{Prob}(p \in \mathcal{B}) = \text{Prob}(g \text{ splits } \& \ f \text{ factors as } \langle 2,1,1\rangle).$$

But as noted at the end of the last paragraph,

$$\text{Prob}(g \text{ splits } \& \ f \text{ factors as } \langle 2,1,1\rangle) = \text{Prob}(f \text{ factors as } \langle 2,1,1\rangle) = \frac{2}{8} = \frac{1}{4}.$$

This completes the proof. □

We are now ready to prove Theorem 2.

Proof of Theorem 2. We use $\mathcal{A}$ and $\mathcal{B}$ with the same meanings as in Lemma 5. Let p be a prime in $\mathcal{A}$. The conditions (i) and (ii) of Lemma 3 will then be satisfied for all k in $2p-2$ residue classes modulo p^2. Indeed, if r is either of the two roots of x^2+x-3 modulo p — both of which are nonsquares mod p by assumption — and $k \equiv r \pmod{p}$, then $q \parallel k^2+k-3$ unless k is congruent modulo p^2 to the unique lift of r mod p to a root of x^2+x-3 modulo p^2. Similarly, for each $p \in \mathcal{B}$, the conditions (i) and (ii) of Lemma 3 are satisfied for all k in $p-1$ residue classes modulo p^2. But if k is counted by $K(x)$, then k does not satisfy (i) and (ii) for any p. In particular, considering for now only those $p \in \mathcal{A} \cup \mathcal{B}$ not exceeding $z := (\log x)^{1/2}$, we see that k is confined to N residue classes modulo $P := \prod_{p \le z} p^2$, where

$$\frac{N}{P} = \prod_{\substack{p \le z \\ p \in \mathcal{A}}} \left(1 - \frac{2p-2}{p^2}\right) \prod_{\substack{p \le z \\ p \in \mathcal{B}}} \left(1 - \frac{p-1}{p^2}\right)$$

Continuing, we note that we may ignore the contribution to $K(x)$ from k satisfying

$$p^2 \mid k^2+k-3 \quad \text{for some prime } p > z. \tag{7}$$

Indeed, for each prime p, there are at most two roots of k^2+k-3 modulo p. As long as $p \neq 13$, each root mod p lifts to a unique mod p^2, by Hensel's lemma. Thus, if $p^2 \mid k^2+k-3$, then k is confined to a certain two residue classes modulo p^2, and the corresponding number of $k \le x$ is at most $2x/p^2+2$. Also, if $k \le x$ and $p^2 \mid k^2+k-3$, we certainly have $p \le 2x$ (for large x). Thus, the total number of $k \le x$ for which (7) holds is

$$\le \sum_{z < p \le 2x} \left(\frac{2x}{p^2} + 2\right) \ll x \sum_{m > z} \frac{1}{m^2} + \pi(2x) \ll \frac{x}{(\log x)^{1/2}}.$$

Since our goal is to show $K(x) = O(x/(\log x)^{1/2})$, this contribution is acceptable.

Suppose now that $p > z$. If $p \in \mathcal{A} \cup \mathcal{B}$, and $p \mid k^2+k-3$ where k is a nonsquare modulo p, then either $p^2 \mid k^2+k-3$ — in which case, p was counted in the last paragraph already — or conditions (i) and (ii) of Lemma 3 hold. Thus, if k is counted by $K(x)$ and k was not accounted for in the last paragraph, then k avoids 2 residue classes mod p for those $p \in \mathcal{A}$ and one residue classes mod p for those $p \in \mathcal{B}$.

Let $R \bmod P$ denote any one of the N residue classes modulo P not eliminated in the first paragraph of the proof. We may assume that $0 \le R < P$. Suppose k is counted by $K(x)$, that k does not satisfy (7), and that $k \equiv R \pmod{P}$. Then $k = Pu + R$, where $0 \le u \le x/P$. By our work in the last paragraph, k, and hence u, avoids two residue classes modulo each prime $p \in \mathcal{A} \cap (z, x]$ and one residue class modulo each prime $p \in \mathcal{B} \cap (z, x]$. Applying Brun's sieve, the number of choices of u, and hence k, is

$$\ll \frac{x}{P} \prod_{\substack{p \in \mathcal{A} \\ z < p \le x}} \left(1 - \frac{2}{p}\right) \prod_{\substack{p \in \mathcal{B} \\ z < p \le x}} \left(1 - \frac{1}{p}\right).$$

(This follows from the first half Theorem 2.2 of [5]; the parameter "A" in that result can be taken to be 2, since the height x up to which we sieve satisfies $x \le (x/P)^2$ for large enough x.) Now summing on possible Rs, we see that the total number of values of k encountered this way is

$$\ll x\frac{N}{P}\prod_{\substack{p\in\mathcal{A}\\ z<p\le x}}\left(1-\frac{2}{p}\right)\prod_{\substack{p\in\mathcal{B}\\ z<p\le x}}\left(1-\frac{1}{p}\right).$$

Turning attention to the factor $\frac{N}{P}$, we note that $1-\frac{2p-2}{p^2}\le(1-\frac{2}{p})(1+O(1/p^2))$, and $1-\frac{p-1}{p^2}\le(1-\frac{1}{p})(1+O(1/p^2))$. Since $\prod_p(1+O(1/p^2))=O(1)$, we deduce that $\frac{N}{P}\ll\prod_{\substack{p\in\mathcal{A}\\ p\le z}}\left(1-\frac{2}{p}\right)\prod_{\substack{p\in\mathcal{B}\\ p\le z}}\left(1-\frac{1}{p}\right)$. Hence, the right-hand side of the last display is

$$\ll x\prod_{\substack{p\in\mathcal{A}\\ p\le x}}\left(1-\frac{2}{p}\right)\prod_{\substack{p\in\mathcal{B}\\ p\le x}}\left(1-\frac{1}{p}\right).$$

The right-hand side of this new display does not exceed

$$x\exp\Bigg(-2\sum_{\substack{p\in\mathcal{A}\\ p\le x}}\frac{1}{p}-\sum_{\substack{p\in\mathcal{B}\\ p\le x}}\frac{1}{p}\Bigg).$$

We finish by substituting in the estimates

$$\sum_{\substack{p\in\mathcal{A}\\ p\le x}}\frac{1}{p}=\frac{1}{8}\log\log x+O(1)\quad\text{and}\quad\sum_{\substack{p\in\mathcal{B}\\ p\le x}}\frac{1}{p}=\frac{1}{4}\log\log x+O(1);$$

these follow from Lemma 5, the estimate (6), and partial summation. □

Remark. One can show that $K(x)/x\to 0$ without using the Chebotarev (or Frobenius) density theorem. It is not difficult to prove directly that the primes $p\in\mathcal{B}$ with $p>3$ are precisely those with $\left(\frac{-3}{p}\right)=-1$ and $\left(\frac{13}{p}\right)=1$. Quadratic reciprocity, along with a sufficiently strong form of Dirichlet's theorem, then implies that the proportion of primes in $\mathcal{B}$ is $\frac{1}{4}$. Sieving only by the primes in $\mathcal{B}$ in the above proof is sufficient to yield the estimate $K(x)=O(x/(\log x)^{1/4})$.

4. A heuristic lower bound on $K(x)$

We find it plausible that the following conditions should hold simultaneously for $\gg x/(\log x)^{3/2}$ primes $p\le x$:

(i) $p\equiv 7\pmod{24}$,

(ii) p^2+p-3 is not divisible by any prime q for which p mod q is a nonsquare,

(iii) the real quadratic field $\mathbb{Q}(\sqrt{p})$ has class number 1.

Examples of primes p satisfying these conditions are $p = 7, 31, 103$, and 127.

The same kind of sieve-based reasoning underlying the proof of Theorem 2 suggests that (i) and (ii) hold for $\gg \pi(x)/(\log x)^{1/2} \gg x/(\log x)^{3/2}$ primes $p \le x$.[1] The Cohen–Lenstra heuristics [2, 3] suggest that (iii), by itself, holds for a positive proportion — roughly 75.45% — of primes p. Lacking any reason for believing the contrary, we believe that a positive proportion of the p surviving (i) and (ii) should also satisfy (iii). Indeed, we suspect that (i) and (ii) are statistically independent of (iii). This is supported by the computational evidence; for instance, of the 9824 primes $p \equiv 7 \pmod{24}$ not exceeding 10^6, 4417 of them satisfy conditions (i) and (ii), and 3451 satisfy condition (iii). The ratio $\frac{3451}{4417}$ is $\approx 78.13\%$. For comparison, 61320 of the 78498 primes $p \le 10^6$ satisfy (iii), and $\frac{61320}{78498} \approx 78.12\%$.

Now suppose that p satisfies (i)–(iii). Let $k = p$. We will show that (1) has a solution by finding positive integers m, n satisfying (2). Hence, k will be counted by $K(x)$, and the lower bound $K(x) \gg x/(\log x)^{3/2}$ "follows".

For notational convenience, we let

$$T = \frac{(k-1)(k^2+k-3)}{3}.$$

Let q be any odd prime dividing T. Our assumptions imply that k is a square modulo q, and so q splits or ramifies in $\mathbb{Q}(\sqrt{k})$. When $q = 2$, we have that $2 \parallel T$. The prime 2 ramifies in $\mathbb{Q}(\sqrt{k})$ since the field discriminant is the even integer $4k$. So every prime dividing T is split or ramified.

The ring $\mathbb{Z}[\sqrt{k}]$ is the full ring of integers of the class number 1 field $\mathbb{Q}(\sqrt{k})$. Thus, for each prime q dividing T, we can choose an element $x_q + y_q\sqrt{k} \in \mathbb{Z}[\sqrt{k}]$ with $N(x_q + y_q\sqrt{k}) = \pm q$. Working modulo 8 shows that we must have

$$N(x_2 + y_2\sqrt{k}) = 2,$$

(i.e., the plus sign must hold), and that for each odd prime q dividing T,

$$N(x_q + y_q\sqrt{k}) = \chi(q)q,$$

where $\chi(\cdot)$ is the nontrivial Dirichlet character modulo 4. (Thus, $\chi(q) = \pm 1$ with the sign chosen to make $\chi(q) \equiv q \pmod 4$.) Define

$$\alpha = \prod_{q^\alpha \parallel T} (x_q + y_q\sqrt{k})^\alpha \in \mathbb{Z}[\sqrt{k}].$$

Then

$$N\alpha = T \cdot \chi(T/2).$$

It is not difficult to check that since $k \equiv 7 \pmod{24}$, we have $T/2 \equiv 1 \pmod 4$, and so in fact $N\alpha = T$.

Changing the signs of the components of α if necessary, we obtain an element

$$\beta = s + t\sqrt{k}$$

[1] Using the sieve, one can show unconditionally that there are $\ll x/(\log x)^{3/2}$ primes $p \le x$ for which (i) and (ii) hold, and that there are $\gg x/(\log x)^{3/2}$ primes $p \le x$ that satisfy (i) and a weak form of (ii), where (ii) is required only for q up to a small power of x.

with norm T and $s, t \geq 0$. Since $s^2 - kt^2 = T \equiv 2 \pmod 4$ and $k \equiv 7 \pmod 8$, we must have that s, t are odd. Thus, we can write $s = 2m + 1$ and $t = 2n + k$ for some integers m, n. Then

$$(2m+1)^2 - k(2n+k)^2 = T,$$

which is (2). However, we do not know that m, n are positive here; for that, we need $s > 1$ and $t > k$. To ensure this, we replace β with $\beta\epsilon^m$, where ϵ is the fundamental unit of $\mathbb{Z}[\sqrt{k}]$, and m is large enough to give the needed inequalities on s and t.

Acknowledgments

We would like to thank Eduardo Dueñez for a helpful suggestion that inspired the idea for the lower bound heuristic. We would also like to thank the Richter program in Lake Forest College for funding the last two authors. During the writing of this paper, the first author was supported by NSF award DMS-1402268.

References

[1] E. Artin, Über eine neue Art von L-Reihen, *Abh. Math. Sem. Univ. Hamburg* **3** (1924), 89–108.

[2] H. Cohen and H. W. Lenstra, Jr., Heuristics on class groups, *Number Theory (New York, 1982)*, Lecture Notes in Math., vol. 1052, Springer, Berlin, 1984, pp. 26–36.

[3] ———, Heuristics on class groups of number fields, *Number Theory, Noordwijkerhout 1983 (Noordwijkerhout, 1983)*, Lecture Notes in Math., vol. 1068, Springer, Berlin, 1984, pp. 33–62.

[4] J. J. Gray, A commentary on Gauss's mathematical diary, 1796–1814, with an English translation, *Exposition. Math.* **2** (1984), 97–130.

[5] H. Halberstam and H.-E. Richert, *Sieve Methods*, London Mathematical Society Monographs, vol. 4, Academic Press, London-New York, 1974.

[6] L.-C. Kappe and B. Warren, An elementary test for the Galois group of a quartic polynomial, *Amer. Math. Monthly* **96** (1989), 133–137.

[7] M. McMullen, Playing with blocks, *Math Horiz.* **25** (2018), no. 4, 14–15.

[8] M. Rosen, Polynomials modulo p and the theory of Galois sets, *Theory and Applications of Finite Fields*, Contemp. Math., vol. 579, Amer. Math. Soc., Providence, RI, 2012, pp. 163–178.