References

1. Owen O'Shea, *The call of the primes: surprising patterns, peculiar puzzles, and other marvels of mathematics*, Prometheus Books, Amherst (2016).
2. P. Cull, M. Flahive and R. Robson, *Difference equations: from rabbits to chaos*, Springer, New York (2005).

10.1017/mag.2019.18

STANLEY R. HUDDY
Fairleigh Dickinson University, Teaneck, NJ, USA
e-mail: *srh@fdu.edu*
MICHAEL A. JONES
Mathematical Reviews, Ann Arbor, MI, USA
e-mail: *maj@ams.org*

103.04 Does Euclid's construction miss infinitely many primes?

Proposition 20 of Book IX of Euclid's *Elements* translates (see [1]) as: "Prime numbers are more than any assigned multitude of prime numbers". Euclid proved that any given set of primes can be enlarged by adding at least one other prime. If this process is continued, it certainly produces infinitely many primes, but does it produce them all or do some get missed out? If so, how many and which ones are missing? Euclid's method as it stands seems to me unresponsive to such questioning, but we can begin to get answers if we replace primes by prime powers whilst retaining the essence of Euclid's argument.

Let S_1 be any finite set of prime powers (with just one power for each prime involved) and define sets S_2, S_3, … inductively as follows. Suppose that $S_k = \{p_1^{a_1}, \ldots, p_m^{a_m}\}$ has already been defined for some $k \in \mathbb{N}$, where $p_1, \ldots, p_m$ are distinct primes and $a_1, \ldots, a_m$ are positive integers. Then there exist unique primes $q_1, \ldots, q_n$ together with positive integers $b_1, \ldots, b_n$ such that

$$p_1^{a_1} p_2^{a_2} \ldots p_m^{a_m} + 1 = q_1^{b_1} q_2^{b_2} \ldots q_n^{b_n}. \tag{1}$$

Now define $S_{k+1} = \{p_1^{a_1}, \ldots, p_m^{a_m}, q_1^{b_1}, \ldots, q_n^{b_n}\}$. No prime q_j can equal one of the primes p_i, for the right-hand side of (1) would be exactly divisible by any such prime, but the left-hand side would not. So S_{k+1} strictly contains S_k and we have a strictly increasing chain of sets

$$S_1 \subset S_2 \subset \ldots \subset S_k \subset S_{k+1} \subset \ldots$$

which yields Euclid's result that there are infinitely many primes.

Let $S = \bigcup_{i \geqslant 1} S_i$ be the union of all the sets in our chain. We wish to know which primes have a power in S. Naturally, this may depend on our choice of the initial finite set, S_1. Once S_1 has been fixed, S itself is determined. This means that if you have a favourite prime and wish it to be included in S, you can ensure that this happens by placing it in S_1. Note also

https://doi.org/10.1017/mag.2019.19 Published online by Cambridge University Press

that some power of 2 must lie in S, since, if no such power is in S_1, it must appear in S_2. We shall prove the following result.

Theorem: Given any initial finite set S_1, there are infinitely many primes $p \equiv 2 \pmod 3$ that have no power in S.

First we prove a proposition.

Proposition: There are infinitely many primes $p \equiv 2 \pmod 3$.

Proof: Let $p_1, p_2, \ldots, p_k$ be any finite set of odd primes $p_i \equiv 2 \pmod 3$, and consider the number

$$Q = 3p_1p_2\ldots p_k + 2.$$

Since primes congruent to 1 (mod 3) form a multiplicatively closed set and $Q \equiv 2 \pmod 3$, Q must have a prime divisor $p \equiv 2 \pmod 3$. Clearly $p \neq p_i$, because $Q \equiv 2 \pmod{p_i}$, for $i = 1, 2, \ldots, k$. Therefore no finite collection of primes congruent to 2 (mod 3) can be complete.

Proof of Theorem: Using the proposition and the fact that S_2 is a finite set, it is sufficient to show that if $p^t \in S \backslash S_2$ for some positive integer t, then $p = 3$ or $p \equiv 1 \pmod 3$.

Let p be a prime and t be a positive integer such that $p^t \in S \backslash S_2$. Then there is a least positive integer k such that $p^t \in S_{k+2}$. Let $P = p_1^{a_1}\ldots p_m^{a_m}$ be the product of all the elements of S_k and let $Q = q_1^{b_1}\ldots q_n^{b_n}$ be the product of all elements of S_{k+1} that are not in S_k. From (1), $P + 1 = Q$. By our construction, the product of all the elements of S_{k+2} that are not in S_{k+1} is

$$PQ + 1 = P(P - 1) + 1 = P^2 - P + 1.$$

Now, by our definition of k, the power p^t is in S_{k+2} but not in S_{k+1}. So

$$P^2 - P + 1 \equiv 0 \pmod p. \tag{2}$$

We know that $p \neq 2$, for some power of 2 lies in S_2. Hence there is an integer r, unique modulo p, such that

$$2r \equiv 1 \pmod p. \tag{3}$$

From (2) and (3),

$$4(P - r)^2 \equiv 4P^2 - 4P + 1 \equiv -3 \pmod p,$$

so, if $p \neq 3$, then -3 is a quadratic residue modulo p.

Recall that, for any integer a such that $p \nmid a$, the Legendre symbol is defined to be

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is a quadratic residue modulo } p, \\ -1 & \text{if } a \text{ is a quadratic non-residue modulo } p. \end{cases}$$

https://doi.org/10.1017/mag.2019.19 Published online by Cambridge University Press

When $p \neq 3$, we have

$$\left(\frac{p}{3}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right) = \left(\frac{-3}{p}\right) = 1,$$

the first equation by quadratic reciprocity (see [2]) and the second by the multiplicative property of the Legendre symbol. Hence $p \equiv 1 \pmod 3$.

Acknowledgement: I am grateful to the referee for pointing out the neat proof of the proposition and for improving the quadratic reciprocity argument.

References

1. T. L. Heath, *The thirteen books of Euclid's Elements* (2nd edn), Dover (1956).
2. H. Davenport, *The higher arithmetic* (8th edn), Cambridge University Press (2008).

10.1017/mag.2019.19

K. ROBIN McLEAN
Department of Mathematical Sciences, University of Liverpool, Liverpool L69 7ZL
e-mail: *krmclean@liv.ac.uk*

103.05 Sums of integers

The purpose of this Note is to draw attention to a new way for proving the well-known fact that $1 + 2 + \ldots + n = \frac{1}{2}n(n+1)$. Our proof involves looking at a symmetry property of a certain polynomial and also using Vieta's formula. For alternative approaches of this same result, we refer the reader to [1, 2, 3, 4] and the very recent [5].

Let n be a positive integer. The polynomial

$$p_n(x) = (x-1)(x-2)\ldots(x-n),$$

has roots $r_i = i$ where $i = 1, 2, \ldots, n$. Furthermore, p_n satisfies a symmetry relation with respect to the midpoint of its roots, $\frac{1}{2}(n+1)$, which reads $p_n\left(\frac{1}{2}(n+1)+x\right) = (-1)^n p_n\left(\frac{1}{2}(n+1)-x\right)$ and is straightforward to verify. Therefore, the polynomial $q_n(x) = p_n\left(\frac{1}{2}(n+1)+x\right)$ is even or odd, according to whether n is even or odd, so that $q_n(x)$ contains either only even powers of x or only odd powers of x. We thus have

$$q_n(x) = \sum_{k=0}^{n} a_{n-k}x^{n-k} = a_n x^n + a_{n-2}x^{n-2} + a_{n-4}x^{n-4} + \ldots . \quad (1)$$

Now, let s_i denote the ith root of q_n, so that $\frac{1}{2}(n+1) + s_i = r_i = i$ is the corresponding root of p_n. Vieta's formula and (1) combined give us $0 = a_{n-1} = -(s_1 + s_2 + \ldots + s_n)$. From this we conclude:

$$1 + 2 + \ldots + n = \sum_{i=1}^{n} r_i = \sum_{i=1}^{n}\left(\frac{n+1}{2} + s_i\right) = n\frac{(n+1)}{2} + \sum_{i=1}^{n} s_1 = \frac{n(n+1)}{2}.$$

https://doi.org/10.1017/mag.2019.19 Published online by Cambridge University Press