The primes that Euclid forgot

Paul Pollack and Enrique Treviño

Abstract

Let $q_1 = 2$. Supposing that we have defined q_j for all $1 \le j \le k$, let q_{k+1} be a prime factor of $1 + \prod_{j=1}^{k} q_j$. As was shown by Euclid over two thousand years ago, $q_1, q_2, q_3, \dots$ is then an infinite sequence of distinct primes. The sequence $\{q_i\}$ is not unique, since there is flexibility in the choice of the prime q_{k+1} dividing $1 + \prod_{j=1}^{k} q_j$. Mullin suggested studying the two sequences formed by (1) always taking q_{k+1} as small as possible, and (2) always taking q_{k+1} as large as possible. For each of these sequences, he asked whether every prime eventually appears. Recently, Booker showed that the second sequence omits infinitely many primes. We give a completely elementary proof of Booker's result, suitable for presentation in a first course in number theory.

1 Introduction.

The following is one version of Euclid's proof that there are infinitely many primes. Start with $q_1 = 2$. Supposing that q_j has been defined for $1 \le j \le k$, continue the sequence by choosing a prime q_{k+1} for which

$$q_{k+1} \mid 1 + \prod_{j=1}^{k} q_j. \tag{1}$$

Then 'at the end of the day', the list $q_1, q_2, q_3, \dots$ is an infinite sequence of distinct prime numbers.

Of course, the sequence $\{q_i\}$ obtained in this way is not unique, since the relation (1) is often satisfied by several choices of the prime q_{k+1}. Mullin [4] suggested two natural ways of dispensing with the ambiguity. First, we could agree that at each step, we always choose the smallest prime q_{k+1} satisfying (1); this leads to the sequence (numbered `A000945` in the Online Encyclopedia of Integer Sequences, or OEIS [6])

$$2, 3, 7, 43, 13, 53, 5, 6221671, 38709183810571, 139, 2801, 11, 17, 5471, \dots. \tag{2}$$

Alternatively, we might always choose the largest possible q_{k+1}, resulting in the sequence (`A000946` in the OEIS)

$$2, 3, 7, 43, 139, 50207, 340999, 2365347734339, 4680225641471129, \dots. \tag{3}$$

We call (2) and (3) the *first* and *second Euclid–Mullin sequences*, respectively. For each of (2) and (3), Mullin raised the question of whether every prime eventually appears. Shanks [5] conjectured on probabilistic grounds (bolstered by computations of Wagstaff; cf. [7]) that every prime is eventually reached by (2), but essentially nothing about the first Euclid–Mullin sequence has been rigorously established. The second Euclid–Mullin sequence was investigated by Cox and van der Poorten [2]. They showed that all of 5, 11, 13, 17, 19, 23, 29, 31, 37, 41, and 47 are missing and conjectured that in fact infinitely many primes fail to appear in (3). The Cox–van der Poorten conjecture was very recently confirmed by Booker [1].

Theorem (Booker)**.** *The second Euclid–Mullin sequence omits infinitely many primes.*

There are two key ingredients in Booker's proof. The first is quadratic reciprocity for the Jacobi symbol, which is a staple of many first courses in number theory. In addition to this elementary theorem, Booker also makes use of some fairly intricate results in analytic number theory, specifically work of Burgess from the 1960s on upper bounds for short character sums.

A simple statement calls out for a simple proof! In this note, we present a variant of Booker's proof where all of the analytic number theory is replaced by very simple-to-prove statements about the distribution of squares and nonsquares modulo a prime. There is a cost for this, certainly; our quantitative bounds are weaker than what follows from Burgess's estimates. However, we believe that given how simple Booker's theorem is to state, there is some value in writing out a proof that is accessible to as wide an audience as possible.

Notation

Throughout the paper, we reserve the letter p for a prime variable. We use $\left(\frac{a}{m}\right)$ for the usual Legendre–Jacobi symbol.

2 Preliminaries on the distribution of squares and nonsquares modulo a prime.

Recall that an integer a not divisible by p is called a *quadratic residue modulo* p if the congruence $x^2 \equiv a \pmod{p}$ is solvable and a *quadratic nonresidue* otherwise. We let $\ell(\square, p)$ denote the length of the longest run $a+1, a+2, \ldots, a+\ell$ of consecutive quadratic residues mod p, and we let $\ell(\boxtimes, p)$ denote the longest run of consecutive quadratic nonresidues. If we wish integers congruent to 0 modulo p to be allowed in the run, we will write ℓ' in place of ℓ in both cases.

In this section, we show that all of $\ell(\square, p)$, $\ell(\boxtimes, p)$, $\ell'(\square, p)$, and $\ell'(\boxtimes, p)$ are smaller than $2\sqrt{p}$. As a prelude, we prove an upper bound on the smallest positive quadratic nonresidue modulo p, which we denote by $n_2(p)$.

Lemma 1. *Let p be an odd prime. Then $n_2(p) < \frac{1}{2} + \sqrt{p}$.*

Proof. Let $n = n_2(p)$. Since $p < n\lceil p/n \rceil < p+n$, the least nonnegative residue of $n\lceil p/n \rceil$ modulo p lies in the open interval $(0, n)$. So $n\lceil p/n \rceil$ is a quadratic residue modulo p. Since n is a quadratic nonresidue, the ratio $\frac{n\lceil p/n \rceil}{n} = \lceil p/n \rceil$ is also a nonresidue. So by the minimality of n, it must be that $1 + p/n > \lceil p/n \rceil \geq n$. Hence,

$$\left(n - \frac{1}{2}\right)^2 < n^2 - n + 1 \leq p, \quad \text{and so} \quad n < \frac{1}{2} + \sqrt{p}. \qquad \square$$

Lemma 2. *Let $1 \leq n < p$ be a quadratic nonresidue modulo p. Then*

$$\ell(\square, p) \leq \max\{p/n, n-1\}.$$

Proof. Let $\ell = \ell(\square, p)$, and choose $a \in \mathbf{Z}$ so that all of $a+1, a+2, \ldots, a+\ell$ are quadratic residues modulo p. Multiplying by n, we obtain a sequence $na+n, na+2n, \ldots, na+\ell n$ of quadratic nonresidues modulo p, each of which differs from the previous by n. Suppose now that $\ell > p/n$. In this case, every quadratic residue modulo p can be considered mod p as being walled inside one of the intervals $(na+jn, na+(j+1)n)$ with $1 \leq j < \lceil p/n \rceil$, or inside $(na + \lceil p/n \rceil n, na+n+p)$. Thus, any run of quadratic residues has length bounded by $n-1$. So either $\ell \leq p/n$ or $\ell \leq n-1$, exactly as claimed in the lemma. $\square$

We can now establish an upper bound on the length of any sequence of consecutive squares modulo p.

Proposition 3. *If p is an odd prime, then $\ell'(\square, p) < 2\sqrt{p}$.*

Proof. We first rule out long runs of squares containing a multiple of p. Suppose first that -1 is not a square modulo p. Then any such run of squares can be viewed, modulo p, as a subset of the interval $[0, n_2(p))$, and thus has length at most $n_2(p)$. On the other hand, if -1 is a square modulo p, then such a run can be viewed as a subset of $(-n_2(p), n_2(p))$, and so has length at most $2n_2(p) - 1$. Consequently,

$$\ell'(\square, p) \leq \max\{2n_2(p) - 1, \ell(\square, p)\}.$$

By Lemma 1, we have $2n_2(p) - 1 < 2\sqrt{p}$. Thus, it suffices to show that $\ell(\square, p) < 2\sqrt{p}$. If there is any quadratic nonresidue in the half-open interval $(\frac{1}{2}\sqrt{p}, 2\sqrt{p}]$, then this bound on $\ell(\square, p)$ follows from Lemma 2. So let us suppose otherwise. By Lemma 1, $n_2(p) < \frac{1}{2} + \sqrt{p} < 2\sqrt{p}$, and so $n_2(p) \leq \frac{1}{2}\sqrt{p}$. With $n := n_2(p)$, each of the integers $k^2 n$ with $1 \leq k < p$ is a quadratic nonresidue mod p. If we pick k as large as possible with

$$k^2 n \leq \frac{1}{2}\sqrt{p},$$

then the lack of nonresidues in $(\frac{1}{2}\sqrt{p}, 2\sqrt{p}]$ implies that

$$(k+1)^2 n > 2\sqrt{p}.$$

Subtracting the first inequality from the second yields $(2k+1)n > \frac{3}{2}\sqrt{p} \geq 3k^2 n$, and thus $2k+1 > 3k^2$. But this inequality is false for each $k \geq 1$. This proves that $\ell(\square, p) < 2\sqrt{p}$ and completes the proof of the proposition. □

It is easier to rule out long runs of nonsquares mod p.

Proposition 4. *For each odd prime p, we have $\ell'(\boxtimes, p) < 2\sqrt{p}$.*

Proof. Every nonresidue or multiple of p can be considered mod p as being walled within the interval $(j^2, (j+1)^2)$, for some $1 \leq j < \lfloor\sqrt{p}\rfloor$, or within the interval $(\lfloor\sqrt{p}\rfloor^2, p+1)$. The number of integers in an interval of the first kind is $2j < 2\sqrt{p}$, while the number of integers in $(\lfloor\sqrt{p}\rfloor^2, p+1)$ is $p - \lfloor\sqrt{p}\rfloor^2 < p - (\sqrt{p}-1)^2 < 2\sqrt{p}$. □

Remarks. Much of this section is adapted from the charming book of Gelfond and Linnik [3]. Lemma 1 and its proof appear, with trivial changes, as that text's Theorem 9.3.1, while the proof of Proposition 4 comes from the discussion at the bottom of p. 179. The only novelty is our proof of Proposition 3. Gelfond and Linnik state that result as Theorem 9.3.2, but it seems that their proof is incomplete.

3 Proof of the main theorem.

Throughout this section, the second Euclid–Mullin sequence is denoted q_1, q_2, $q_3, \ldots$. The main theorem is contained in the following proposition.

Proposition 5. *Let $Q_1, Q_2, \ldots, Q_r$ be the smallest r primes omitted from the second Euclid–Mullin sequence, where $r \geq 0$. Then there is another omitted prime smaller than*

$$12^2 \left(\prod_{i=1}^{r} Q_i \right)^2 . \tag{4}$$

Remark. Using the results of Burgess, Booker showed that the exponent 2 in (4) can be replaced with any real number larger than $\frac{1}{4\sqrt{e}-1} = 0.178734\ldots$, provided that 12^2 is also replaced by a possibly larger constant.

Proof. Let $X = 12^2 \left(\prod_{i=1}^{r} Q_i\right)^2$. Let us suppose for the sake of contradiction that every prime $p \leq X$ except $Q_1, \ldots, Q_r$ appears in the second Euclid–Mullin sequence. Let p be the prime in $[2, X]$ that is last to appear in the sequence $\{q_i\}$, and say p appears as the nth term q_n. Then p is the largest prime dividing $1 + q_1 \cdots q_{n-1}$. Moreover, since each prime smaller than p that is not a Q_i is one of $q_1, \ldots, q_{n-1}$, the only other possible prime factors of $1 + q_1 \cdots q_{n-1}$ are $Q_1, \ldots, Q_r$. Thus, we must have

$$1 + q_1 \cdots q_{n-1} = Q_1^{e_1} Q_2^{e_2} \cdots Q_r^{e_r} p^e$$

for some exponents $e_1, \ldots, e_r \geq 0$ and $e \geq 1$.

We claim it is possible to choose a natural number $d \le X$ satisfying both of the congruences

$$d \equiv 1 \pmod 4, \quad d \equiv -1 \pmod{Q_1 \cdots Q_r}, \tag{5}$$

as well as

$$\left(\frac{d}{p}\right) = \left(\frac{-1}{p}\right). \tag{6}$$

Suppose for the moment that this has been proved. Since $d \le X$ and d is coprime to $Q_1 \cdots Q_r p$, every prime dividing d is among the primes $q_1, \ldots, q_{n-1}$. So if we write $d = d_0 d_1^2$, where d_0 is squarefree, then $d_0 \mid q_1 \cdots q_{n-1}$. Hence,

$$\begin{aligned}\left(\frac{d}{1+q_1\cdots q_{n-1}}\right) &= \left(\frac{1+q_1\cdots q_{n-1}}{d}\right) \\ &= \left(\frac{1+q_1\cdots q_{n-1}}{d_0}\right)\left(\frac{1+q_1\cdots q_{n-1}}{d_1^2}\right) \\ &= \left(\frac{1}{d_0}\right)\cdot\left(\left(\frac{1+q_1\cdots q_{n-1}}{d_1}\right)\right)^2 = 1\cdot 1 = 1.\end{aligned}$$

(The very first equality uses quadratic reciprocity for the Jacobi symbol.) On the other hand, we have $\left(\frac{d}{Q_i}\right) = \left(\frac{-1}{Q_i}\right)$ for each $i = 1, 2, \ldots, r$ and $\left(\frac{d}{p}\right) = \left(\frac{-1}{p}\right)$, so that

$$\begin{aligned}\left(\frac{d}{1+q_1\cdots q_{n-1}}\right) &= \left(\prod_{i=1}^{r}\left(\frac{d}{Q_i}\right)^{e_i}\right)\cdot\left(\frac{d}{p}\right)^{e} \\ &= \left(\prod_{i=1}^{r}\left(\frac{-1}{Q_i}\right)^{e_i}\right)\cdot\left(\frac{-1}{p}\right)^{e} \\ &= \left(\frac{-1}{1+q_1\cdots q_{n-1}}\right) = -1,\end{aligned}$$

using in the last step that $1 + q_1 \cdots q_{n-1} = 1 + 2\prod_{1<i<n} q_i \equiv 3 \pmod 4$. This is a contradiction.

It remains to establish the existence of a $d \le X$ satisfying (5) and (6). The conditions (5) are satisfied by every integer $d \equiv A \pmod M$, where $A := 2Q_1 \cdots Q_r - 1$ and $M := 4Q_1 \cdots Q_r$. To obtain (6), we look for a small nonnegative integer k with $\left(\frac{Mk+A}{p}\right) = \left(\frac{-1}{p}\right)$. Equivalently, fixing M' satisfying $MM' \equiv 1 \pmod p$, we seek a nonnegative integer k with

$$\left(\frac{k + AM'}{p}\right) = \left(\frac{-M'}{p}\right).$$

By the results of section 2, we can find such a $k \le \max\{\ell'(\square, p), \ell'(\boxtimes, p)\} < 2\sqrt{p}$. Then the corresponding d satisfies

$$0 < d = Mk + A < 2M\sqrt{p} + M < 3M\sqrt{p} \le 3M\sqrt{X}.$$

Since $3M = 12Q_1 \cdots Q_r = \sqrt{X}$, we find that $d < X$. This completes the proof. $\square$

Acknowledgments.

We are grateful to Carl Pomerance and the anonymous referee for their thoughtful suggestions. In particular, the current form of Proposition 3 is due to the referee; our original result was slightly weaker. We also thank Yuliia Glushchenko for help with the Russian original of [3].

References

[1] A. Booker, On Mullin's second sequence of primes, *Integers* **12A** (2012) article A4, 10 pages, `http://www.integers-ejcnt.org/vol12a.html`.

[2] C. D. Cox and A. J. van der Poorten, On a sequence of prime numbers, *J. Austral. Math. Soc.* **8** (1968) 571–574.

[3] A. O. Gel′fond and Yu. V. Linnik, *Elementary Methods in the Analytic Theory of Numbers*. Pergamon Press, Oxford, 1966.

[4] A. A. Mullin, Recursive function theory (a modern look at a Euclidean idea), *Bull. Amer. Math. Soc.* **69** (1963) 737.

[5] D. Shanks, Euclid's primes, *Bull. Inst. Combin. Appl.* **1** (1991) 33–36.

[6] N. J. A. Sloane, The On-Line Encyclopedia of Integer Sequences, published electronically at `http://oeis.org`.

[7] S. S. Wagstaff, Jr., Computing Euclid's primes, *Bull. Inst. Combin. Appl.* **8** (1993) 23–32.

Department of Mathematics, University of Georgia, Athens, GA 30602
pollack@uga.edu

Department of Mathematics and Computer Science, Lake Forest College, Lake Forest, IL 60045
trevino@mx.lakeforest.edu