# On Generalizations of the Second Euclid-Mullin Sequence

Jordan Clark and Lori Watson

**Abstract**

The second Euclid-Mullin sequence is an infinite sequence of primes which arises from a variation on Euclid's proof of the infinitude of primes. Booker showed this sequence omits infinitely many primes. Pollack and Treviño showed the same thing with a completely elementary proof. We adapt the Pollack and Treviño argument to show certain related sequences also omit infinitely many primes.

## 1 Introduction

One version of Euclid's well-known proof of the infinitude of primes is as follows: Start with $q_1 = 2$. With a list of primes $q_1, \ldots, q_{n-1}$ having been determined, the sequence is continued by choosing the $n$th prime $q_n$ to be a prime divisor of $1 + \prod_{i=1}^{n-1} q_i$. Since $1 + \prod_{i=1}^{n-1} q_i$ is relatively prime to the first $n-1$ primes in the sequence, at each step we find a new prime, and we conclude that there must be infinitely many primes.

Note that at a given step, $1 + \prod_{i=1}^{n-1} q_i$ may be composite, and as such there may be several choices for $q_n$. In 1963, Mullin [5] suggested generating the sequence $\{q_i\}_{i=1}^{\infty}$ by placing some restrictions on the choice of $q_n$. Rather than allowing *any* choice of prime divisor of $1 + \prod_{i=1}^{n-1} q_i$, one can require that the smallest prime divisor be chosen. In this way, we obtain the first Euclid-Mullin sequence. Alternatively, one can require that at each step the greatest prime divisor is chosen. This leads to the second Euclid-Mullin sequence. For each sequence, Mullin asked whether every prime appears as a term in the sequence. In the case of the first Euclid-Mullin sequence, this question is still open; in fact, it is unknown whether 41 appears as a term in the sequence.

For the second Euclid-Mullin sequence, much more is known. In 1967, Cox and van der Poorten [3] showed that the second Euclid-Mullin sequence omits every prime $p \leq 53$ besides $2, 3, 7$, and 43, and they conjectured that infinitely many primes are omitted by the sequence. In 2012, Booker [1] proved their conjecture.

In their paper, Cox and van der Poorten showed that if certain primes appeared, the second Euclid-Mullin sequence would satisfy an inconsistent system of congruences. In his proof, Booker used this same essential idea to prove Cox and van der Poorten's conjecture. In 2014 Pollack and Treviño [6] provided an elementary version of Booker's argument (again, based on an inconsistent system of congruences). It is this more elementary argument we adapt below for certain Euclid-Mullin-like sequences. Specifically, we construct sequences denoted $EML(a, c; q)$, depending on a given prime $q$, a scaling factor $c$, and a "shift" $a$, which omit infinitely many primes. We then construct a Euclid-Mullin-like sequence in the ring $\mathbb{Z}[i]$ and attempt an adaptation of the Pollack and Treviño proof to this sequence.

## 2 Euclid-Mullin-Like sequences

To construct a Euclid-Mullin-like sequence, we proceed as follows: We fix integers $a$ and $c$ and a prime $q_1 = q$. Having chosen the first $n-1$ primes of the sequence, we choose the $n$th prime to be the largest prime divisor of $a + c\prod_{i=1}^{n-1} q_i$. We refer to the sequence arising from these choices as the $EML(a, c; q)$ sequence. The second Euclid-Mullin sequence, for example, is the $EML(1, 1; 2)$ sequence.

### 2.1 The second Euclid-Mullin sequence

**Theorem 2.1** (Booker)**.** *The $EML(1,1;2)$ sequence omits infinitely many primes*

Booker's proof has two key components: one being quadratic reciprocity and the other a result on upper bounds for certain character sums. Pollack and Treviño also use quadratic reciprocity, but they exchange the bounds on character sums for simpler-to-prove statements about distributions of squares and non squares modulo a prime. Their elementary proof of comes at the expense of worse quantitative bounds. Since our work adapts the elementary argument, presumably each of the bounds given below could be improved by using bounds on character sums.

## 3 $EML$ sequences missing infinitely many primes

In this section, we present a full proof that the sequence $EML(2,c;3)$ omits infinitely many primes when $c$ is an odd positive integer. We then explain the changes needed to adapt the proof to other $EML$ sequences. To begin with, we state a lemma regarding quadratic residues and non residues.

**Lemma 3.1** (Pollack and Treviño)**.** *If $p$ is an odd prime, then the length of any sequence of consecutive squares modulo $p$ is strictly less than $2\sqrt{p}$.*

**Theorem 3.2.** *The sequence $EML(2,c;3)$ misses infinitely many primes*

The theorem is a consequence of the following proposition:

**Theorem 3.3.** *Let $q_1 = 3$ and let $c$ be an odd positive integer. Let $Q_1, \dots, Q_r$ be the smallest $r$ primes omitted from $EML(2,c;3)$ (we allow the possibility that $r = 0$, in which case $Q_1 \cdots Q_r$ is the empty product). Then there is another omitted prime smaller than*

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

*Proof.* Suppose by way of contradiction that every prime $p \le X$ except $Q_1, \dots, Q_r$ appears in the sequence. Let $p$ be the prime in $[2, X]$ that is last to appear in the sequence $\{q_i\}$, and say $p$ is the $n$th term $q_n$. Then $p$ is the largest prime dividing $2 + cq_1 \cdots q_{n-1}$. Since every prime smaller than $p$ that is not one of the $Q_i$ must be one of $q_1, \dots, q_{n-1}$, the only other possible prime factors of $2 + cq_1 \cdots q_{n-1}$ are $Q_1, \dots, Q_r$. So,

$$2 + cq_1 \cdots q_{n-1} = Q_1^{e_1} Q_2^{e_2} \cdots Q_r^{e_r} p^e$$

for some exponents $e_1, \dots, e_r \ge 0$ and $e \ge 1$. We claim that it is possible to choose a natural number $d \le X$ satisfying the following conditions

$$d \equiv 5 \pmod 8, \quad d \equiv 1 \pmod{Q_1 \cdots Q_r} \tag{1}$$

and

$$\left(\frac{d}{p}\right) = \left(\frac{1}{p}\right). \tag{2}$$

Suppose such a $d$ exists. Since $d \le X$ and $d$ is coprime to $Q_1 \cdots Q_r p$, every prime dividing $d$ is among the primes $q_1, \dots, q_{n-1}$. So if we write $d = d_0 d_1^2$, where $d_0$ is squarefree, then $d_0 \mid cq_1 \cdots q_{n-1}$ and $d_0 \equiv 5 (\mathrm{mod}\ 8)$. Hence,

$$\left(\frac{d}{2+cq_1\cdots q_{n-1}}\right)=\left(\frac{2+cq_1\cdots q_{n-1}}{d}\right)=\left(\frac{2+cq_1\cdots q_{n-1}}{d_0}\right)\left(\frac{2+cq_1\cdots q_{n-1}}{d_1^2}\right)$$

$$=\left(\frac{2}{d_0}\right)\left(\frac{2+cq_1\cdots q_{n-1}}{d_1^2}\right)=\left(\frac{2}{d_0}\right)\left(\frac{2+cq_1\cdots q_{n-1}}{d_1}\right)^2=-1\cdot 1=-1.$$

The first and fourth equality are each using that $d\equiv 5 \pmod 8$. On the other hand, we also have $\left(\frac{d}{Q_i}\right)=\left(\frac{1}{Q_i}\right)$ for each $i=1,2,\ldots,r$, and $\left(\frac{d}{p}\right)=\left(\frac{1}{p}\right)$ by (2), so

$$\left(\frac{d}{2+cq_1\cdots q_{n-1}}\right)=\left(\prod_{i=1}^{r}\left(\frac{d}{Q_i}\right)^{e_i}\right)\cdot\left(\frac{d}{p}\right)^e$$

$$=\left(\prod_{i=1}^{r}\left(\frac{1}{Q_i}\right)^{e_i}\right)\cdot\left(\frac{1}{p}\right)^e$$

$$=\left(\frac{1}{2+cq_1\cdots q_{n-1}}\right)=1.$$

This is a contradiction.

We now establish that there is an integer $d\le X$ satisfying (1) and (2). Condition (1) is satisfied for any $d=Mk+A$, where $M\coloneqq 4Q_1\cdots Q_r$ and $A\coloneqq 2Q_1\cdots Q_r+1$ (though $Q_1\cdots Q_r$ may be the empty product as noted earlier, in this case as $2+cq_1\cdots q_{n-1}$ is always odd, we take $Q_1=2$). To obtain (2), 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 Lemma 3.1 we know the longest run of quadratic residues or non residues is less than $2\sqrt{p}$, so we can find $0\le k<2\sqrt{p}$. 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 $d<X$, thus completing the proof. □

**Proposition 3.4.** *For a positive odd integer $c$ and a positive integer $j$, the sequences $EML(1,c;2)$, $EML(1,2c;2)$,$EML(-1,c;2)$ and $EML(-1,2^jc;2)$ omit infinitely many primes.*

Each of the above statements follows from propositions similar to Theorem 3.3. In what follows, we make several conventions. First, $Q_1,\ldots,Q_r$ are the first $r$ primes omitted by the sequence (where we again allow $r=0$). Second, for each sequence we assume $p$ is the last prime in $[2,X]$ to appear in the sequence (say $p$ is the $n$th term), where $X$ is some integer depending on the sequence. Third, as $q_1=2$, we assume without loss of generality that $n>1$ so that $q_n=p>2$ and we can freely use the Jacobi symbol to obtain the necessary contradictions. The other changes needed for each of the proofs are provided below.

(a) For the sequence $EML(1,c;2)$, Pollack and Treviño's proof works with only cosmetic changes. In place of (1) and (2) we require $d<X=12^2\left(\prod_{i=1}^{r}Q_i\right)^2$ such that

$$d\equiv 1 \pmod 4,\quad d\equiv -1 \pmod{Q_1\cdots Q_r} \tag{3}$$

and

$$\left(\frac{d}{p}\right) = \left(\frac{-1}{p}\right). \tag{4}$$

The conditions are then satisfied by an integer $d = Mk + A$ where $M \coloneqq 4Q_1 \cdots Q_r$, $A \coloneqq 2Q_1 \cdots Q_r - 1$, and $k < 2\sqrt{p}$.

(b) For the sequence $EML(1, 2c; 2)$ we require $d < X = 6^2 \left(\prod_{i=1}^{r} Q_i\right)^2$ such that

$$d \equiv 2 \pmod{Q_1 \cdots Q_r} \tag{5}$$

and

$$\left(\frac{d}{p}\right) = \left(\frac{2}{p}\right). \tag{6}$$

The conditions are satisfied by $d = Mk + 2$, where $M \coloneqq 2Q_1 \cdots Q_r$ and $k < 2\sqrt{p}$.

(c) For the sequence $EML(-1, c; 2)$ we require $d < X = 12^2 \left(\prod_{i=1}^{r} Q_i\right)^2$ such that

$$d \equiv 3 \pmod 4 \qquad\qquad d \equiv 1 \pmod{Q_1 Q_2 \cdots Q_r} \tag{7}$$

and

$$\left(\frac{d}{p}\right) = \left(\frac{1}{p}\right), \tag{8}$$

The conditions are satisfied by $d = Mk + A$, where $M \coloneqq 4Q_1 \cdots Q_r$, $A \coloneqq 2Q_1 \cdots Q_r + 1$ and $k < 2\sqrt{p}$.

(d) For the sequence $EML(-1, 2^j c; 2)$ we require $d < X = 12^2 \left(\prod_{i=1}^{r} Q_i\right)^2$ such that

$$d \equiv 1 \pmod 4, \;\; d \equiv -1 \pmod{Q_1 Q_2 \cdots Q_r} \tag{9}$$

and

$$\left(\frac{d}{p}\right) = \left(\frac{-1}{p}\right). \tag{10}$$

The conditions are satisfied by $d = Mk + A$, where $M \coloneqq 4Q_1 \cdots Q_r$, $A \coloneqq 2Q_1 \cdots Q_r - 1$ and $k < 2\sqrt{p}$.

# 4 Where Difficulties Arise

## 4.1 $EML(1, 4; 2)$

Suspiciously, we have proofs that the sequences $EML(1, c; 2)$ and $EML(1, 2c; 2)$ omit infinitely many primes for $c$ odd, but have not provided proofs that the sequences $EML(1, 2^j c; 2)$ omit infinitely many primes for $j > 1$. It is in these cases that difficulties begin to arise. In the proofs given above, we arrive at a contradiction by showing that for the denominator $a + cq_1 \cdots q_{n-1}$ and a carefully chosen numerator $d$ the Jacobi symbol is not well-defined. We do this by first flipping the symbol and considering only the value of the Jacobi symbol on the square-free part of $d$ and then by using the multiplicativity of the symbol

to show that with the exact same numerator and denominator, the Jacobi symbol takes on the opposite value. To achieve this contradiction, we must be able to show that either due to the shift $a$ in the sequence $EML(a, c; q)$ and/or due to congruence conditions placed on $d$, the symbol $(\frac{d}{a+cq_1\cdots q_{n-1}})$ will, when viewed properly, return a value of $-1$.

If we look at the proof of Theorem 3.3, for example, we see that with the shift of $a = 2$ and the condition that $d$ (and hence the square-free part of $d$) is $5 \pmod 8$, the Jacobi symbol returns $-1$ after we flip the symbol. We can then easily control congruence conditions to force the symbol to return 1 when viewed differently. When we have a sequence $EML(1, 2^j c; 2)$, for $j > 1$, however, the argument breaks down. In this case, since $q_1 = 2$ and $j > 1$, we are ultimately considering how the Jacobi symbol behaves when its denominator $1 + 2^j cq_1 \cdots q_{n-1}$ is congruent to 1 modulo 8. Crucially, we need $d$ to be small enough so that all of its prime divisors are among the primes $2, q_2, \ldots, q_{n-1}$ and the primes dividing $c$. If for such a $d$, we try to invert the symbol and then consider how it behaves we are forced to conclude that $(\frac{d}{1+2^j cq_1\cdots q_{n-1}}) = (\frac{1}{d_0})$ ($d_0$ being the square free part of $d$), which is always 1, no matter what $d_0$ is. In the other direction, since $1 + 2^j cq_1 \cdots q_{n-1}$ is $1 \pmod 8$, it is difficult to find a numerator $*$ so that $(\frac{*}{1+2^j cq_1\cdots q_{n-1}})$ is $-1$. This then hints at a limitation to the arguments used above: when working with the sequence $EML(a, c; q)$, if $a$ is a square and $a + cq_1 \cdots q_{n-1}$ does not have any obvious non-square residue classes, deriving a contradiction using the Jacobi symbol becomes harder. What, then, can be shown?

For $EML(1, 4; 2)$, at least, we can show that not every prime appears in the sequence. To show this, we start with the following lemma:

**Lemma 4.1.** *If $t = 1 + 4q_1 \cdots q_n$, then $t \neq x^4$ for any $x \in \mathbb{Z}$.*

*Proof.* Suppose $t = x^4$. Then $1 + 4q_1 \cdots q_n = x^4$, so:

$$4q_1 \cdots q_n = x^4 - 1 = (x - 1)(x + 1)(x^2 + 1)$$

Since $t$ is odd implies $x$ is odd, each of $x - 1,\ x + 1,\ x^2 + 1$ must be even. Since then either $(x - 1)$ or $(x + 1) \equiv 0 (\text{mod } 4)$, the right hand side is divisible by $2^4$. But the left hand side is only divisible by $2^3$ since $q_1 = 2$ and the other primes are odd. □

**Proposition 4.2.** *The prime 7 does not appear in the sequence $EML(1, 4; 2)$.*

*Proof.* One can check that for this sequence, $q_2 = 3$ and $q_3 = 5$. Then since every prime less than 7 appears as some $q_i$, if 7 appears as the largest prime divisor of $1 + 4q_1 \cdots q_{n-1}$ for some $n$ then 7 must be the only prime divisor. So $1 + 4q_1 \cdots q_{n-1} = 7^m$ for some $m$. Considering this equality $\pmod 5$, we see that

$$1 + 4q_1 \cdots q_n = 7^m \equiv 2^m \pmod 5$$

Since $q_3$=5 we have

$$1 \equiv 2^m \pmod 5,$$

thus $m \equiv 0 \pmod 4$. Therefore $1 + 4q_1 \cdots q_n$ must be a fourth power, contradicting the lemma. □

# 5 Beyond the Integers

Euclid's proof that there are infinitely many primes works with minor changes in rings other than $\mathbb{Z}$ (see for example [2]). One might hope that analogues of Euclid-Mullin-like sequences might arise in other rings as well. To that end we next consider a Euclid-Mullin-like sequence in the ring of Gaussian integers $\mathbb{Z}[i]$. As when working over $\mathbb{Z}$, we can consider sequences of prime elements in $\mathbb{Z}[i]$. Other notions will need to be reinterpreted for our new setting. When constructing our sequence and obtaining the $n$th prime, say $\omega$, we will need to choose among four associate primes (if $\omega$ is prime, then so are $-\omega$ and $\pm i\omega$). We say an integer $\alpha = a + bi \in \mathbb{Z}[i]$, is *odd* if its norm $N(\alpha) = a^2 + b^2$ is odd; we say an odd integer $\alpha$ is *primary* if $\alpha \equiv 1 \pmod{(i+1)^3}$. In our sequence, we will choose at each step the unique primary associate of a prime $\omega$. Rather than using quadratic reciprocity and the Jacobi symbol, we use biquadratic reciprocity and the biquadratic residue symbol, which we review below. The biquadratic residue symbol is best understood when dealing with primary integers; it is for this reason we choose the primary associate of a prime at each step.

## 5.1 Biquadratic Reciprocity

Biquadratic (or quartic) reciprocity is the appropriate tool to use in place of quadratic reciprocity when working with prime elements in $\mathbb{Z}[i]$. Rather than using the Jacobi symbol $(\frac{a}{n})$ to detect when an integer $a$ is a quadratic residue modulo an odd prime $n \in \mathbb{Z}$, we use the biquadratic symbol $\left[\frac{\alpha}{\pi}\right]$ to detect wheter an element $\alpha \in \mathbb{Z}[i]$ is a biquadratic residue (i.e., fourth-power) modulo an odd prime $\pi \in \mathbb{Z}[i]$. There is a unique integer $0 \leq k \leq 3$ such that $\alpha^{(N(\pi)-1)/4} \equiv i^k \pmod{\pi}$ and $\left[\frac{\alpha}{\pi}\right]$ is defined to be $i^k$. In particular, $\left[\frac{\alpha}{\pi}\right] = 1$ if and only if $x^4 - \alpha$ has a solution modulo $\pi$. Below, we summarize relevant facts about primary integers and biquadratic reciprocity, and extend the biquadratic symbol to arbitrary primary integers (see [4]).

- We extend the symbol so that, if the numerator is kept fixed, then the symbol is totally multiplicative.. That is, if $\beta = \pi_1^{e_1} \cdots \pi_n^{e_n}$, then
$$\left[\frac{\alpha}{\beta}\right] = \left[\frac{\alpha}{\pi_1}\right]^{e_1} \cdots \left[\frac{\alpha}{\pi_n}\right]^{e_n}.$$

- An element $\alpha = a + bi$ in $\mathbb{Z}$[i] is primary if and only if either $a \equiv 1 \pmod 4$ and $b \equiv 0 \pmod 4$ or $a \equiv 3 \pmod 4$ and $b \equiv 2 \pmod 4$.

- If $\alpha$ and $\beta$ are primary, then $\alpha\beta$ is primary.

- If $\alpha$ and $\beta$ are primary and relatively prime non-units, then $\left[\frac{\alpha}{\beta}\right] = \left[\frac{\beta}{\alpha}\right] \cdot (-1)^{\frac{N(\alpha)-1}{4}\frac{N(\beta)-1}{4}}$.

- If $\theta$ and $\pi$ are primary primes, then $\left[\frac{\theta}{\pi}\right] = \left[\frac{\pi}{\theta}\right]$ whenever $\theta$ or $\pi$ is $\equiv 1 \pmod 4$.

- If $\beta$ is a primary integer, then $\left[\frac{1+i}{\beta}\right] = i^{(Re(\beta)-Im(\beta)-Im(\beta)^2-1)/4}$.

## 5.2 Conditional case of Euclid-Mullin-like Sequences in the Gaussian Integers

**Definition 5.1.** (*EML for $\mathbb{Z}[i]$*) *Let $\omega_1 = 1+i$. Supposing $\omega_j$ has been defined for $1 \leq j \leq n$, continue the sequence by choosing $\omega_{n+1}$ such that $\omega_n$ is a primary prime of largest norm dividing $1 + 2\omega_1 \cdots \omega_{n-1}$. We will call the sequence $\{\omega_n\}_{n=1}^{\infty}$ the Euclid-Mullin-like (EML) sequence.*

**Remark 5.2.** *Throughout, we concern ourselves only with primary primes. We multiply $\omega_1 \cdots \omega_{n-1}$ by 2 to ensure that $1 + 2\omega_1 \cdots \omega_{n-1}$ will be primary.*

In both [1] and [6] a key fact used is that intervals of length small relative to $p$ must contain both integers which are quadratic residues modulo $p$ and integers which are non-quadratic residues modulo $p$. When working over $\mathbb{Z}[i]$ one might hope to prove that balls of small radius (small relative to the norm of a prime $\pi$) contain both biquadratic residues and non-residues. Rausch [7] provides a theorem that implies a result in this direction. His bounds on character sums in algebraic number fields can be used to prove that for any $\epsilon \in \{\pm 1 \pm i\}$, for a prime $\pi \in \mathbb{Z}[i]$, and for given $\alpha \in \mathbb{Z}[i]$, there is some $\gamma \in \mathbb{Z}[i]$ in a ball of not-too-large radius about $\alpha$ such that $\left[\frac{\gamma}{\pi}\right] = \epsilon$. To prove that certain Euclid-Mullin-like sequences in the Gaussian integers miss infinitely many prime elements, a slightly stronger result is needed due to the possibility that

Table 1: First terms in the Euclid-Mullin-like sequence for the Gaussian integers

| | |
|---|---|
| $\omega_1$ | $1+i$ |
| $\omega_2$ | $3+2i$ |
| $\omega_3$ | $3+10i$ |
| $\omega_4$ | $-93+50i$ |
| $\omega_5$ | $-827+120i$ |
| $\omega_6$ | $477839-760062i$ |
| $\omega_7$ | $22662669-40258594i$ |
| $\omega_8$ | $-3085230919875999-807504660092300i$ |

there may be *two* primes of largest norm dividing $1+2\omega_1\cdots\omega_{n-1}$. To ensure that a contradiction can be achieved regardless of the choice of a prime of largest norm, the following unproven hypothesis is needed.

[**The Strong Close-By Hypothesis**] *There is a constant $C$ such that for any prime $\pi_1\in\mathbb{Z}[i]$, for any $\alpha\in\mathbb{Z}[i]$, and for any fixed $\epsilon_1,\epsilon_2\in\{\pm1,\pm i\}$, there is a $\gamma\in\mathbb{Z}[i]$ with $N(\gamma-\alpha)<CN(\pi_1)^{1/2}$, $\left[\frac{\gamma}{\pi_1}\right]=\epsilon_1$, and $\left[\frac{\gamma}{\pi_2}\right]=\epsilon_2$ (where $\pi_2=\overline{\pi}_1$).*

The Strong Close-by Hypothesis is only slightly stronger than a result implied by Rausch which gives a bound of $N(\gamma-\alpha)<CN(\pi_1)^{1/2+\delta}$ for each $\delta>0$. Assuming the hypothesis, we prove the following proposition.

**Proposition 5.3.** *Let $Q_1,\ldots,Q_r$ be the smallest (in norm) $r$ primes omitted from the sequence $\{\omega_n\}_{n=1}^{\infty}$, where $r\geq 0$ and let $X=(32C)\cdot N(Q_1\cdots Q_r)$. Then there is another omitted prime $\Omega$ such that $N(\Omega)<X$ and no associate of $\Omega$ is contained in $\{\omega_n\}_{n=1}^{\infty}$ .*

**Proof of the proposition:** Suppose by way of contradiction that every prime $\pi$ with $N(\pi)\leq X$ except $Q_1,\ldots,Q_r$ has an associate appearing in the EML sequence above. Let $\pi$ be last prime to appear in the sequence with $N(\pi)\in[2,X]$, say $\pi=\omega_n$. Then $\pi$ is a prime of largest norm dividing $\beta=1+2\omega_1\cdots\omega_{n-1}$. If there is another prime of norm $N(\pi)$ which is not associate to $\pi$, we denote it by $\pi_2$ (note that in such a case we have $\pi_2=\overline{\pi}$). Since any prime with norm smaller than $N(\pi)$ that is not one of the $Q_j$ is one of $\omega_1,\ldots,\omega_{n-1}$, the only possible factors of $\beta$ are $Q_1,\ldots,Q_r,\pi_2,\pi$, so $\beta=Q_1^{e_1}\cdots Q_r^{e_r}\pi_2^{e_{r+1}}\pi^e$, where $e_1,\ldots,e_r,e_{r+1}\geq 0$ and $e\geq 1$.

We claim we can choose $\lambda\in\mathbb{Z}[i]$ with $N(\lambda)\leq X$ such that :

$$\lambda \text{ is primary} \tag{11}$$

$$\lambda\equiv 1+i \pmod{Q_1\cdots Q_r} \tag{12}$$

and

$$\left[\frac{\lambda}{\pi}\right]=\left[\frac{1+i}{\pi}\right] \text{ and } \left[\frac{\lambda}{\pi_2}\right]=\left[\frac{1+i}{\pi_2}\right]. \tag{13}$$

Supposing for the moment this has been proved, since $N(\lambda)\leq X$, and $\lambda$ is coprime to $Q_1,\ldots,Q_r,\overline{\pi},\pi$, every prime dividing $\lambda$ is among the primes $\omega_1,\ldots,\omega_{n-1}$ (or an associate of one of the $\omega_j$'s). Thus, if we

write $\lambda = \lambda_0 \lambda_1^2$, with $\lambda_0$ square free, then $\lambda_0 | \omega_1 \cdots \omega_{n-1}$, so Biquadratic Reciprocity gives

$$\begin{aligned}\left[\frac{\lambda}{\beta}\right] &= \left[\frac{\beta}{\lambda}\right] \cdot (-1)^{\frac{N(\lambda)-1}{4}\frac{N(\beta)-1}{4}} \\ &= \left[\frac{\beta}{\lambda_0}\right] \cdot \left[\frac{\beta}{\lambda_1^2}\right] \cdot (-1)^{\frac{N(\lambda)-1}{4}\frac{N(\beta)-1}{4}} \\ &= \left[\frac{1}{\lambda_0}\right] \cdot \left[\frac{\beta}{\lambda_1}\right]^2 \\ &= (1) \cdot (\pm 1) \cdot (-1)^{\frac{N(\lambda)-1}{4}\frac{N(\beta)-1}{4}} \in \{\pm 1\}.\end{aligned}$$

On the other hand, for each $j = 1, 2, \ldots, r$, $\left[\frac{\lambda}{Q_j}\right] = \left[\frac{1+i}{Q_j}\right]$, $\left[\frac{\lambda}{\pi}\right] = \left[\frac{1+i}{\pi}\right]$ and $\left[\frac{\lambda}{\pi_2}\right] = \left[\frac{1+i}{\pi_2}\right]$, so

$$\left[\frac{\lambda}{\beta}\right] = \left(\prod_{j=1}^{r} \left[\frac{\lambda}{Q_j}\right]^{e_j}\right) \cdot \left[\frac{\lambda}{\pi_2}\right]^{e_{r+1}} \left[\frac{\lambda}{\pi}\right]^{e} = \left(\prod_{j=1}^{r} \left[\frac{1+i}{Q_j}\right]^{e_j}\right) \cdot \left[\frac{1+i}{\pi_2}\right]^{e_{r+1}} \left[\frac{1+i}{\pi}\right]^{e} = \left[\frac{1+i}{\beta}\right].$$

Since $\omega_2 \cdots \omega_{n-1} = a + bi$ is primary, we have that $a$ is odd, $b$ is even; then for $\beta = 1 + 2\omega_1 \cdots \omega_{n-1}$ (recalling that $\omega_1 = 1 + i$), we have $\beta = 1 + 2(1+i)(a+bi) = (1 + 2a - 2b) + i(2a + 2b)$, so

$$\frac{Re(\beta) - Im(\beta) - Im(\beta)^2 - 1}{4} = \frac{1 + 2a - 2b - (2a + 2b) - (4a^2 + 8ab + 4b^2) - 1}{4} = -b - a^2 - 2ab - b^2,$$

which is odd, thus

$$\left[\frac{1+i}{\beta}\right] = i^{(Re(\beta) - Im(\beta) - Im(\beta)^2 - 1)/4} \in \{\pm i\}.$$

This is a contradiction.

It remains to show there is such $\lambda \in \mathbb{Z}[i]$ with $N(\lambda) \leq X$ satisfying (11), (12), and (13). By the Chinese Remainder Theorem, we know there exists some $A$ satisfying conditions (11) and (12). Then the conditions are also satisfied by any $\lambda = \delta M + A$, where $M = Q_1 \cdots Q_r \cdot (1+i)^3$ (where no $Q_i$ or associate of $Q_1$ is equal to $1 + i$). Then finding a $\lambda$ of sufficiently small norm relative to $X$ satisfying condition (13) is equvialent to finding $\delta$ of sufficiently small norm such that $\left[\frac{\delta + AM'}{\pi}\right] = \left[\frac{(1+i)M'}{\pi}\right]$, $\left[\frac{\delta + AM'}{\pi_2}\right] = \left[\frac{(1+i)M'}{\pi}\right]$, where $MM' \equiv 1 \pmod{\pi}$ and $MM' \equiv 1 \pmod{\pi_2}$ . By the hypothesis, there exists $\gamma \in \mathbb{Z}[i]$ such that $\left[\frac{\gamma}{\pi}\right] = \left[\frac{(1+i)M'}{\pi}\right]$, $\left[\frac{\gamma}{\pi_2}\right] = \left[\frac{(1+i)M'}{\pi_2}\right]$and $N(\gamma - AM') \leq CN(\pi)^{1/2}$. Letting $\delta \coloneqq \gamma - AM'$, we have $\left[\frac{\delta + AM'}{\pi}\right] = \left[\frac{(1+i)M'}{\pi}\right]$; then setting $\lambda \coloneqq \delta M + A$ (and noting that we can choose $A$ with $|A| < |M|$), we have

$$\begin{aligned}\sqrt{N(\lambda)} = |\lambda| = |\delta M + A| \leq |\delta M| + |A| < |\delta M| + |M| < |M|(|\delta| + 1) = (\sqrt{8} \cdot |Q_1 \cdots Q_r|) \cdot (|\delta| + 1) \\ \leq (\sqrt{8} \cdot |Q_1 \cdots Q_r|)(2|\delta|) \leq (2\sqrt{8} \cdot |Q_1 \cdots Q_r|) \cdot (C^{1/2}|\pi|^{1/2}) \leq \sqrt{X^{\frac{1}{2}}}\sqrt{X^{\frac{1}{2}}} = X^{1/2},\end{aligned}$$

for $X$ chosen to be large relative to $N(Q_1 \cdots Q_r)$. Thus $N(\lambda) < X$, proving the claim. □

## References


[1] A. Booker. On Mullin's second sequence of primes. *Integers*, 12A, 2012.

[2] P. L. Clark. The Euclidean criterion for irreducibles. `https://arxiv.org/abs/1605.01298`, May 2016.

[3] C.D. Cox and A.J. van der Poorten. On a sequence of prime numbers. *Journal of the Australian Mathematical Society*, 8:571–574, 1968.

[4] F. Lemmermeyer. *Reciprocity laws, from Euler to Eisenstein*. Springer-Verlag, New York, NY, 2000.

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

[6] P. Pollack and E. Treviño. The primes that Euclid forgot. *American Mathematical Monthly*, 121, no.5: 433–437, 2014.

[7] U. Rausch. Character sums in algebraic number fields. *Journal of Number Theory*, 46(2):179 – 195, 1994.