Euclid Prime Sequences over Unique Factorization Domains

Nobushige Kurokawa and Takakazu Satoh

CONTENTS

2000 AMS Subject Classification: Primary 11T55, 11A51, 13F15, 13P05

Keywords: Prime sequences, polynomial factorization, the Shanks conjecture

The proof by Euclid that there exist infinitely many prime numbers is well known. The proof involves generating prime numbers that do not belong to a given finite set of primes, and one may ask whether all prime numbers can be obtained by this method. Daniel Shanks gave a heuristic argument that suggests that the answer is affirmative. Despite recent advances in computational number theory, numerical examples do not seem to make this conjecture convincing. We reformulate the problem in polynomial rings over finite fields and prove that in some explicitly characterized cases, Shanks's argument does not hold. On the other hand, we have performed numerical computations that suggest that except for the above cases, Shanks's conjecture is true.

1. INTRODUCTION

Proposition 20 in Book IX of Euclid's *Elements* essentially states that there are infinitely many prime numbers. Let $X := \{ p_1, \ldots, p_m \}$ be an arbitrary finite set of primes. Then the minimal (or the maximal) prime divisor of $p_1 \cdots p_m + 1$ does not belong to X. By this method we can generate an infinite sequence consisting of primes, beginning with 2. Although there are several papers on such sequences (see [Narkiewicz 2000, Section 1.1] and references cited there), the authors of these papers work only over $\mathbb{Z}$. However, the above method can be straightforwardly generalized to unique factorization domains.

Definition 1.1. Let R be a unique factorization domain. The group $R^\times$ of the units of R acts on the set P of all irreducible elements. Let $\mathcal{P}$ be a complete system of representatives of $P/R^\times$. We assume that a total order is defined over $\mathcal{P}$ and fix the total order once and for all. Let $c \in R$ and $l \in \mathcal{P}$.

Assume that c and l satisfy the following condition: for any $n \geq 0$ and $p_1, p_2, \ldots, p_n$, we have that $lp_1 \cdots p_n + c \notin R^\times \cup \{0\}$ (we understand that the empty product is 1).

The *minimal Euclid prime sequence* $E_{\min}(l,c)_R$ with initial term $l \in \mathcal{P}$ and offset $c \in R - \{0\}$ is a sequence $\{l_n\}_{n=-1}^{\infty}$ defined by $l_{-1} := l$ and

$$l_{n+1} = \min\{x \in \mathcal{P} : x \mid (l_{-1}l_0 \cdots l_n + c)\}$$

for $n \geq -1$.

Under the given condition, this generates an infinite sequence. Similarly, the *maximal Euclid prime sequence* $E_{\max}(l,c)_R$ with initial term l and offset c is a sequence $\{l_n\}_{n=-1}^{\infty}$ defined by $l_{-1} := l$ and

$$l_{n+1} = \max\{x \in \mathcal{P} : x \mid (l_{-1}l_0 \cdots l_n + c)\}$$

for $n \geq -1$. (It is convenient to begin the sequence with the (-1)th term in order to simplify notation in Section 3.) When there is no danger of confusion, the subscript R will be omitted.

Throughout the paper, we assume that l and c satisfy the condition of Definition 1.1. In most cases, $c \in R^{\times}$. However, we do not exclude the case of a nonunit c. If $l \nmid c$, the above sequences have no repeated term (Proposition 2.1).

If we have $R = \mathbb{Z}$ we take $\mathcal{P}$ to be the set of positive rational primes, while if $R = \mathbb{F}_p[X]$, we take $\mathcal{P}$ to be the set of all monic irreducible polynomials. For example, the first few terms of the Euclid prime sequences with initial value 2 and an offset 1 are

$$E_{\min}(2,1)_{\mathbb{Z}} = \{2, 3, 7, 43, 13, 53, 5, 6221671, \ldots\},$$
$$E_{\max}(2,1)_{\mathbb{Z}} = \{2, 3, 7, 43, 139, 50207, 340999, \ldots\}.$$

It is easily proved that $5 \notin E_{\max}(2,1)_{\mathbb{Z}}$ (see, for example, [Narkiewicz 2000, p. 2]). On the other hand, Shanks [Shanks 91] conjectured that $E_{\min}(2,1)_{\mathbb{Z}}$ would coincide with $\mathcal{P}$, the set of all (positive rational) primes. We formulate the Shanks conjecture for R as follows:

$$E_{\min}(l,c)_R = \{p \in \mathcal{P} : p \nmid c\}.$$

For example, is

$$E_{\min}(3,2)_{\mathbb{Z}} = \{3, 5, 17, 257, 65537, 641, 7, 318811, 19, \ldots\}$$

equal to the set of all odd primes?

For some rings (e.g., $\mathbb{C}[X]$), the conjecture is trivially false. However, we can still ask, for example, whether $E_{\min}(X,c)_{\mathbb{Z}[X]}$ coincides with the set of monic irreducible polynomials in $\mathbb{Z}[X]$ (cf. Section 4).

The main result of this paper, Corollary 3.6, is that in $\mathbb{F}_p[X]$, the analogue of the Shanks conjecture is false for infinitely many primes p and $c \in \mathbb{F}_p$ (which depends on p). More precisely, let $\mathcal{P}$ be the set of all monic irreducible polynomials in $\mathbb{F}_p[X]$. Then there are infinitely many primes p and $c \in \mathbb{F}_p$ such that $E_{\min}(X,c)_{\mathbb{F}_p[X]} \subsetneq \mathcal{P}$ for any order of $\mathcal{P}$.

The rest of the paper is organized as follows: In Section 2, we prove some basic properties of the Euclid prime sequence. Section 3 is devoted to a proof of our main result. We use the biquadratic reciprocity law and the Čebotarev density theorem in the proof. Some related topics are discussed in Section 4.

In Section 5, we give numerical support for the truth of the Shanks conjecture over $\mathbb{F}_p[X]$ by computing $E_{\min}(X,c)_{\mathbb{F}_p[X]}$ for $p \leq 5$ except for $(p,c) = (5,1)$, for which the Shanks conjecture is proved to be false in Example 3.4. Note that such a computation for $E_{\min}(p,c)_{\mathbb{Z}}$ is hard, due to difficulty of integer factorization.

Wagstaff [Wagstaff 93] computed such sequences to about fifty terms. Thanks to an efficient polynomial factorization algorithm (together with an asymptotically fast GCD algorithm and FFT-based multiplication over $\mathbb{F}_p[X]$), we can compute several hundred terms of $E_{\min}(X,c)_{\mathbb{F}_p[X]}$.

2. BASIC PROPERTIES OF THE EUCLID SEQUENCES OVER UNIQUE FACTORIZATION DOMAINS

In this section, we observe some basic properties of the Euclid sequences.

Proposition 2.1. *Assume $l \nmid c$. Then $E_{\min}(l,c)_R$ and $E_{\max}(l,c)_R$ have no repeated terms.*

Proof: Because a proof for $E_{\max}(l,c)_R$ is the same as one for $E_{\min}(l,c)$, we give a proof only for $E_{\min}(l,c)$. Let l_n be the nth term of $E_{\min}(l,c)_R$. Assume that there exists $m > n \geq -1$ such that $l_m = l_n$. Then $l_m \mid l_{-1} \cdots l_n \cdots l_{m-1} + c$, which means that $l_m \mid c$. Hence $l_n \mid c$. Let ν be the minimal integer such that $\nu \geq -1$ and $l_\nu \mid c$. Then $\nu \geq 0$ because of the assumption $l_{-1} \nmid c$. Hence $l_\nu \mid l_{-1} \cdots l_{\nu-1}$. So there exists $-1 \leq n < \nu$ satisfying $l_n = l_\nu$. Then $l_n \mid c$, which contradicts the minimality of ν. □

Theorem 2.2. *Let $c \in R$ and $l \in \mathcal{P}$. Assume $l \nmid c$. Let p be the mth minimal element of $\mathcal{P}$. Assume $p \nmid c$ and $\#R/\langle p \rangle = 2$. Then p appears in one of the first $(m-1)$ terms of $E_{\min}(l,c)$.*

Proof: Denote the nth term of $E_{\min}(l,c)$ by l_n. Suppose that $l_{-1},\dots,l_{m-1}$ are distinct from p. We denote by $\overline{a}\in R/\langle p\rangle$ the residue modulo p for each element $a\in R$. Then we have

$$\begin{aligned} l_{-1}+c &= l_0\times d_0,\\ l_{-1}l_0+c &= l_1\times d_1,\\ &\cdots\\ l_{-1}\cdots l_{m-2}+c &= l_{m-1}\times d_{m-1}, \end{aligned}$$

with $\overline{l_0d_0}=\overline{l_1d_1}=\cdots=\overline{l_{m-1}d_{m-1}}=\overline{0}$. In fact, from $\overline{l_{-1}}\neq\overline{0}$, we know that $\overline{l_{-1}+c}=\overline{l_{-1}}+\overline{c}=\overline{0}$, since $\overline{c}\neq\overline{0}$ and $R/\langle p\rangle=\{\overline{0},\overline{1}\}$.

Hence $\overline{l_0d_0}=\overline{0}$, i.e., $p\mid l_0d_0$, and the minimality of l_0 implies $l_0<p$. Similarly, we see that $l_k<p$ for $k=1,\dots,m-1$. Moreover, $l_{-1},\dots,l_{m-1}$ are distinct by Proposition 2.1. This contradicts the assumption that p is the mth minimal element in $\mathcal{P}$. □

Remark 2.3. An example (other than $\mathbb{Z}$) for which Theorem 2.2 is applicable can be given as follows: Let $d\in\mathbb{Z}$ be an integer such that $d\equiv 1 \bmod 8$ and such that the class number of $\mathbb{Q}(\sqrt{d})$ is 1, i.e., $d\in\{-7,17,33,41,57,\dots\}$. Let R be the ring of integers of $\mathbb{Q}(\sqrt{d})$. Then 2 splits into two prime principal ideals with norm 2. Note that Theorem 2.2 holds for any order on $\mathcal{P}$. Even for the case of $R=\mathbb{Z}$ and $p=2$, the assertion is nontrivial for an order for which 2 is not the minimal element.

Let p be a rational prime. We introduce a total order of $\mathbb{F}_p[X]$.

Definition 2.4. For $f(X):=\sum_{k=0}^{m}a_kX^k\in\mathbb{F}_p[X]$, we put $I(f):=\sum_{k=0}^{m}\alpha_kp^k\in\mathbb{Z}$, where $\alpha_k\in\{0,1,\dots,p-1\}$ and $a_k=\alpha_k \bmod p$.

We define an order on $\mathbb{F}_p[X]$ by $f_1\le f_2$ if $I(f_1)\le I(f_2)$. We use this order on $\mathbb{F}_p[X]$ unless otherwise noted.

The following proposition is a straightforward analogue of the fact that 5 does not appear in $E_{\max}(2,1)_{\mathbb{Z}}$.

Proposition 2.5. *The polynomial X^3+X+1 does not appear in $E_{\max}(X,1)_{\mathbb{F}_2[X]}$.*

Proof: The sequence begins $X, X+1, X^2+X+1$. Denote by $f_n(X)$ the nth term of $E_{\max}(X,1)_{\mathbb{F}_2[X]}$ and assume $f_m(X)=X^3+X+1$ with some $m\ge 2$. Note that all irreducible polynomials less than X^3+X+1 have already appeared in $E_{\max}(X,1)_{\mathbb{F}_2[X]}$. This implies $f_{-1}(X)\cdots f_{m-1}(X)+1=(X^3+X+1)^s$ with $s\ge 2$.

Therefore, $f_{-1}(X)\cdots f_{m-1}(X)$ is divisible by $X^3+X=X(X+1)^2$. This contradicts the fact that $f_{-1}(X)\cdots f_{m-1}(X)$ is square-free. □

Although we are mainly interested in rings finitely generated over $\mathbb{Z}$, the next theorem (with a somewhat tricky proof) is of independent interest.

Theorem 2.6. *Let $\mathcal{P}$ be the set of monic irreducible polynomials in $\mathbb{R}[X]$. Choose an order on $\mathcal{P}$ such that a monic irreducible quadratic polynomial is greater than a monic polynomial of degree one and such that $X-t$ is greater than $X-t'$ if and only if $t<t'$. Let $a\in\mathbb{R}$ and $c>0$. Denote the nth term of $E_{\min}(X-a,-c)_{\mathbb{R}[X]}$ by l_n (so $l_{-1}(X)=X-a$). Put $f_n(X)=l_{-1}(X)\cdots l_n(X)-c$ and $\alpha_{-1}=a$. Then the following assertions hold:*

(1) *For all $n\ge 0$, the equation $f_n(X)=0$ has a unique real root α_{n+1} satisfying $\alpha_{n+1}>\alpha_n$. In other words, $l_{n+1}(X)=X-\alpha_{n+1}$.*

(2) *We have*

$$\alpha_n\ge\min(c,1)\log(n+2)+a \qquad (2\text{–}1)$$

for all $n\ge -1$. In particular, $\lim_{n\to\infty}\alpha_n=\infty$.

Proof: (1) It is easy to see that $f_n'(X)>0$ for $X>\alpha_n$. Hence the assertion follows from $f_n(\alpha_n)=-c<0$ and $\lim_{X\to\infty}f_n(X)=\infty$.

(2) First, we show that

$$\alpha_n\ge\beta_n \text{ where } \beta_n:=\frac{1}{n+1}\sum_{i=-1}^{n-1}\alpha_i+c^{\frac{1}{n+1}} \qquad (2\text{–}2)$$

for $n\ge 0$. By (1), this is obvious in the case $\beta_n\le\alpha_{n-1}$. Otherwise, $\beta_n>\alpha_i$ for $-1\le i\le n-1$ (again by (1)). Then

$$\begin{aligned} f_{n-1}(\beta_n) &= \prod_{i=-1}^{n-1}(\beta_n-\alpha_i)-c\\ &\le \Big(\beta_n-\frac{1}{n+1}\sum_{i=-1}^{n-1}\alpha_i\Big)^{n+1}-c\\ &= 0. \end{aligned}$$

(Recall that a geometric mean is less than or equal to an arithmetic mean.) This implies that $\beta_n\le\alpha_n$.

We now prove (2–1) by induction on n. For simplicity, put $b:=\min(c,1)$. For $n=-1$, this is trivial. Assume

that (2–1) holds for all n less than m. By (2–2), we obtain

$$\begin{aligned}\alpha_m &\geq \frac{1}{m+1}\sum_{i=-1}^{m-1}\alpha_i + c^{\frac{1}{m+1}}\\ &\geq \frac{1}{m+1}\sum_{i=-1}^{m-1}(b\log(i+2)+a) + c^{\frac{1}{m+1}}\\ &= b\log(m+2)+a+\frac{b}{m+1}\log\left(\frac{(m+1)!}{(m+2)^{m+1}}\right)\\ &\quad + c^{\frac{1}{m+1}}.\end{aligned}$$

Note that $\log\left(\frac{(m+1)!}{(m+2)^{m+1}}\right) \geq -(m+1)$ for all $m \geq 0$. This is obvious for $m = 0$. For $m \geq 1$, this follows from

$$\begin{aligned}\frac{(m+1)!}{(m+2)^{m+1}} &= \frac{m!}{(m+1)^m}\cdot\frac{1}{\left(1+\frac{1}{m+1}\right)^{m+1}}\\ &\geq \frac{m!}{(m+1)^m}\cdot\frac{1}{e},\end{aligned}$$

that is,

$$\log\left(\frac{(m+1)!}{(m+2)^{m+1}}\right) \geq \log\left(\frac{m!}{(m+1)^m}\right) - 1.$$

Therefore

$$\alpha_m \geq b\log(m+2)+a-b+c^{\frac{1}{m+1}} \geq b\log(m+2)+a,$$

since $c \geq b \geq b^{m+1}$.

Thus (2–1) holds for $n = m$. □

Remark 2.7. Numerical computations suggest that $\log\alpha_n = \log\log n + o(\log\log n)$, where the little-$o$ constant may depend on c. But this conjecture is open.

3. EUCLID SEQUENCES OVER POLYNOMIAL RINGS

In this section, we consider a polynomial analogue of the Shanks conjecture. In order to describe our result, the following terminology is useful.

Definition 3.1. Let R be a unique factorization domain and let $\mathcal{P}$, l, and c be as in Definition 1.1. Denote the mth term of $E_{\min}(l,c)$ by l_m. The sequence $E_{\min}(l,c)_R$ is called *totally irreducible* if $\prod_{m=-1}^{n} l_m + c \in \mathcal{P}$ for all $n \in \mathbb{N}$. (In this case, $E_{\min}(l,c)_R$ coincides with $E_{\max}(l,c)_R$, and they are independent of the order of R. However, total irreducibility depends on the choice of $\mathcal{P}$.)

In the rest of the paper, we put $g_c(X) := X(X+c)$ for $c \in R$. We define $g_c^0(X) := X$ and $g_c^{n+1}(X) := g_c(g_c^n(X))$ for $n \geq 0$. If $R = \mathbb{F}_p[X]$, recall that $\mathcal{P}$ is the set of all monic irreducible polynomials in $\mathbb{F}_p[X]$. What we shall actually do in this section is construct a rational prime p and $c \in \mathbb{F}_p$ such that $E_{\min}(X,c)_{\mathbb{F}_p[X]}$ is totally irreducible. The next lemma implies that the Shanks conjecture for $E_{\min}(X,c)_{\mathbb{F}_p[X]}$ is false if it is totally irreducible.

Lemma 3.2. *Let l_m be the mth term of $E_{\min}(l,c)_R$. Assume that $\prod_{m=-1}^{n} l_m + c \in \mathcal{P}$ for all $-1 \leq n \leq N$. Then $l_n = g_c^n(l) + c$ for all $0 \leq n \leq N+1$. Assume, moreover, that $E_{\min}(l,c)_R$ is totally irreducible. Then $l_n = g_c^n(l)+c$ for all $n \geq 0$.*

Proof: The case $N = 0$ is trivial. Assume that the assertion holds for $n \leq N$. Then

$$\begin{aligned}l_{N+1} &= l_{-1}\cdots l_{N-1}l_N + c\\ &= (l_N - c)l_N + c\\ &= g_c^N(l)(g_c^N(l)+c)+c\\ &= g_c^{N+1}(l)+c\end{aligned}$$

which completes the proof. □

Theorem 3.3. *Let q be an odd prime power and $c \in \mathbb{F}_q^\times$. Take an integer m (in practice, the minimal such number) satisfying $g_c^m(-c^2/4) = g_c^\nu(-c^2/4)$ for some $\nu \in \mathbb{N}$ satisfying $\nu < m$. Assume*

$$\left(-c+\frac{c^2}{4}\right)^{(q-1)/2} = -1$$

and

$$\left(c+g_c^n\left(-\frac{c^2}{4}\right)\right)^{(q-1)/2} = -1$$

for $n \in \mathbb{N}$ less than or equal to m. Then $E_{\min}(X,c)_{\mathbb{F}_q[X]}$ is totally irreducible.

Proof: Let $A_{-1}(X) := X$ and

$$A_n(X) := A_{-1}(X)A_0(X)\cdots A_{n-1}(X) + c$$

for $n \geq 0$. It is enough to show that $A_n(X)$ is monic and irreducible over $\mathbb{F}_q$ for all $n \geq 0$. By a similar argument to the proof of Lemma 3.2, we see that $A_n(X) = g_c^n(X) + c$ for $n \geq 0$. Note that the existence of m in the assumptions implies that

$$\left(-c+g_c^n\left(-\frac{c^2}{4}\right)\right)^{(q-1)/2} = -1$$

for all $n \in \mathbb{N}$.

Put $\gamma_0 := -c$ and let γ_n be one of roots of $g_c(X) = \gamma_{n-1}$ for $n \geq 1$. We see that $A_n(\gamma_n) = 0$. Since $\deg A_n = 2^n$, it is enough to show that $[\mathbb{F}_q(\gamma_{n+1}) : \mathbb{F}_q(\gamma_n)] = 2$, or equivalently, $g_c(X) - \gamma_n$ is irreducible over $\mathbb{F}_q(\gamma_n)$ for all $n \geq 0$.

We use induction on n. For $n = 0$, this is again obvious, since

$$g_c(X) - \gamma_0 = X^2 + cX + c = \left(X + \frac{c}{2}\right)^2 - \frac{c^2}{4} + c.$$

For $n \geq 1$, assume that $g_c(X) - \gamma_k$ is irreducible over $\mathbb{F}_q(\gamma_k)$ for all $0 \leq k < n$. In particular, $[\mathbb{F}_q(\gamma_k) : \mathbb{F}_q] = 2^k$ for all $k \leq n$ (note that the case $k = n$ is also valid). We compute $(\gamma_n - t)^{(q^{2^n}-1)/2}$ for any $t \in \mathbb{F}_q$. Let σ_n be the $q^{2^{n-1}}$th power map, which is the unique nontrivial element of $\mathrm{Gal}(\mathbb{F}_q(\gamma_n)/\mathbb{F}_q(\gamma_{n-1}))$. We note that $\sigma_n(\gamma_n) = -\gamma_n - c$.

Therefore

$$\begin{aligned}
(\gamma_n - t)^{(q^{2^n}-1)/2} &= (\gamma_n - t)^{q^{2^{n-1}} \frac{q^{2^{n-1}}-1}{2} + \frac{q^{2^{n-1}}-1}{2}} \\
&= (-\gamma_n - c - t)^{(q^{2^{n-1}}-1)/2} (\gamma_n - t)^{(q^{2^{n-1}}-1)/2} \\
&= (-1)^{(q^{2^{n-1}}-1)/2} \left((\gamma_n + c + t)(\gamma_n - t)\right)^{(q^{2^{n-1}}-1)/2} \\
&= (-1)^{(q^{2^{n-1}}-1)/2} (\gamma_n^2 + c\gamma_n - ct - t^2)^{(q^{2^{n-1}}-1)/2} \\
&= (-1)^{(q^{2^{n-1}}-1)/2} (\gamma_{n-1} - g_c(t))^{(q^{2^{n-1}}-1)/2}.
\end{aligned}$$

Note that $(-1)^{(q^{2^{n-1}}-1)/2} = -1$ if and only if $q \equiv 3 \bmod 4$ and $n = 1$. Thus we see that

$$\begin{aligned}
(\gamma_n - t)^{(q^{2^n}-1)/2} &= (\gamma_{n-1} - g_c(t))^{(q^{2^{n-1}}-1)/2} \\
&= (\gamma_{n-2} - g_c^2(t))^{(q^{2^{n-2}}-1)/2} \\
&= \cdots = (\gamma_1 - g_c^{n-1}(t))^{(q^2-1)/2} \\
&= (-1)^{(q-1)/2} (\gamma_0 - g_c^n(t))^{(q-1)/2} \\
&= (g_c^n(t) + c)^{(q-1)/2},
\end{aligned}$$

and in particular,

$$\left(\gamma_n + \frac{c^2}{4}\right)^{(q^{2^n}-1)/2} = \left(g_c^n(-c^2/4) + c\right)^{(q-1)/2} = -1.$$

This implies that

$$g_c(X) - \gamma_n = \left(X + \frac{c}{2}\right)^2 - \left(\frac{c^2}{4} + \gamma_n\right)$$

is irreducible over $\mathbb{F}_q(\gamma_n)$. □

Example 3.4. Take $q := 5$ and $c := 1$. Then $-c^2/4 = 1$, and we have $g_1^0(1) = 1$, $g_1^1(1) = 2$, and $g_1^2(1) = 1$. Hence $1 + g_1^n(1)$ is 2 for even n and 3 for odd n. In either case, it is a quadratic nonresidue. Therefore $E_{\min}(X, 1)_{\mathbb{F}_5[X]}$ is totally irreducible.

The same is true for the case $q := 13$ and $c := 10$. It might be interesting to observe the case $q := 83$ and $c := 28$. In this case, $c + g_c^n(-c^2/4)$ are quadratic nonresidues for $1 \leq n \leq 8$, but $c + g_c^9(-c^2/4)$ is a quadratic residue. Indeed, $A_9(X)$ is an irreducible polynomial of degree 512 over $\mathbb{F}_{83}$, but $A_{10}(X)$ is reducible over $\mathbb{F}_{83}$.

Before proving that there are infinitely many pairs (p, c) for which $E_{\min}(X, c)_{\mathbb{F}_p[X]}$ is totally irreducible, we recall some basic facts about the biquadratic reciprocity law over $\mathbb{Z}[\sqrt{-1}]$. For details, see, for example, [Ireland and Rosen 82, Chapter 9]. A nonunit $a + bi$, $a, b \in \mathbb{Z}$, is called *primary* if either $a \equiv 1 \bmod 4$ and $4 \mid b$ or $a \equiv 3 \bmod 4$ and $b \equiv 2 \bmod 4$. Let π be an irreducible element of $\mathbb{Z}[\sqrt{-1}]$ that does not divide 2.

Then $N(\pi) \equiv 1 \bmod 4$, where $N(\pi)$ is the norm of the principal ideal $\langle \pi \rangle$. For α not divisible by π, there exists a unique element $z \in \{\pm 1, \pm i\}$ satisfying $\alpha^{(N(\pi)-1)/4} \equiv z \bmod \langle \pi \rangle$. We call the value z the *biquadratic residue symbol* of α for π and denote it by $\left(\frac{\alpha}{\pi}\right)_4$.

Note that the quadratic equation $x^2 = \overline{\alpha}$ in $\mathbb{Z}[\sqrt{-1}]/\langle \pi \rangle$ has a solution if and only if $\left(\frac{\alpha}{\pi}\right)_4 = \pm 1$. The biquadratic reciprocity law is the formula

$$\left(\frac{\lambda}{\pi}\right)_4 = \left(\frac{\pi}{\lambda}\right)_4 (-1)^{(N(\lambda)-1)(N(\pi)-1)/16} \tag{3–1}$$

for relatively prime primary elements π and λ.

Theorem 3.5. *Let π be an irreducible primary element of $\mathbb{Z}[\sqrt{-1}]$ that is not a rational integer. Assume that $\pi \equiv \pm i \bmod 5$ or $\pi \equiv \pm 2 \bmod 5$. Put $p := N(\pi)$. Then 5 is a quadratic residue modulo p and*

$$E_{\min}\left(p, \frac{1 + \sqrt{5}}{2}\right)_{\mathbb{F}_p[X]}$$

is totally irreducible. (Here $\sqrt{5}$ stands for an element of $\mathbb{F}_p$ satisfying $\left(\sqrt{5}\right)^2 = 5$.)

Proof: First, we observe that π does not divide 2 under the assumption. Let $\gamma \in \mathbb{Q}(\sqrt{5})$ be one of roots of $\gamma^2 - 2\gamma - 4 = 0$. Thus $-\frac{\gamma^2}{4} = -1 - \frac{\gamma}{2}$. Hence $g_\gamma(-\gamma^2/4) = -\gamma/2$ and $g_\gamma(-\gamma/2) = -\gamma^2/4$.

Note that $N(\pi)$ is a rational prime, since π is not a rational integer. Let $\mathfrak{P}$ be a prime ideal of $\mathbb{Q}\left(\sqrt{-1}, \sqrt{5}\right)$ lying above $\langle \pi \rangle$. Put $k := \mathbb{Z}[\sqrt{-1}]/\langle \pi \rangle \cong \mathbb{F}_p$. By the assumption, $p = N(\pi) = \pm 1 \bmod 5$. This proves that 5 is a quadratic residue modulo p. Therefore, the residue

class field of $\mathfrak{P}$ is k, and the reduction of $X^2-2X-4 \in \mathbb{Z}[X]$ modulo $\langle\pi\rangle$ splits in $k[X]$. Let $c \in k$ be the residue class of γ modulo $\mathfrak{P}$.

We need to show that

$$-c+\frac{c^2}{4} \quad \left(=1-\frac{c}{2}\right),$$

$$c+g_c\left(-\frac{c^2}{4}\right) \quad \left(=\frac{c}{2}\right),$$

and

$$c+g_c^2\left(-\frac{c^2}{4}\right) \quad \left(=-1+\frac{c}{2}\right)$$

are all quadratic nonresidues in k. Since π is not a rational integer, -1 is a square in k. Moreover, $\left(1-\frac{c}{2}\right)\frac{c}{2} = -1$ is a square in k. Therefore we have only to show that $\frac{c}{2}$ is not a square in k by Theorem 3.3.

The minimal polynomial of $\sqrt{\gamma/2}$ is

$$X^4-X^2-1=(X^2-\sqrt{1-2i}X-i)(X^2+\sqrt{1-2i}X-i),$$

and its roots are

$$\frac{\pm\sqrt{1-2i}\pm\sqrt{1+2i}}{2}.$$

We show that both $1-2i$ and $1+2i$ are quadratic nonresidues modulo π.

By the biquadratic reciprocity law (3–1), we have

$$\left(\frac{-1+2i}{\pi}\right)_4 = \pm\left(\frac{\pi}{-1+2i}\right)_4$$

and

$$\left(\frac{-1-2i}{\pi}\right)_4 = \pm\left(\frac{\pi}{-1-2i}\right)_4.$$

Note that

$$\frac{N(-1+2i)-1}{4}=\frac{N(-1-2i)-1}{4}=1.$$

Thus $\left(\frac{\pi}{-1\pm 2i}\right)_4 = c$ is simply equivalent to $\pi \equiv c \bmod (-1\pm 2i)$.

Using the Chinese remainder theorem, we see that the condition $\pi \equiv \pm i \bmod (-1+2i)$ and $\pi \equiv \pm i \bmod (-1-2i)$ is equivalent to $\pi \equiv \pm i \bmod 5$. Similarly, the condition

$$\pi \equiv \pm i \bmod (-1+2i) \quad \text{and} \quad \pi \equiv \mp i \bmod (-1-2i)$$

is equivalent to $\pi \equiv \mp 2 \bmod 5$. In either case, the pth-power map changes signs of $\alpha^{1/2}$, $\beta^{1/2} \in \mathbb{F}_{p^2}$, where α is the class of $1+2i$ in k, and β is the class of $1-2i$ in k.

Clearly, $\alpha^{1/2} \pm \beta^{1/2} \neq 0$. Thus, $c/2$ is a nonsquare in k. This completes the proof. □

Corollary 3.6. *There are infinitely many pairs of a rational prime p and an element c of $\mathbb{F}_p$ such that $E_{\min}(X,c)_{\mathbb{F}_p[X]}$ is totally irreducible.*

Proof: By the Čebotarev density theorem, there are infinitely many irreducible elements $\pi \in \mathbb{Z}[\sqrt{-1}]$ that satisfy $\pi \equiv -5+6\sqrt{-1} \bmod 20$, or equivalently, $\pi \equiv \sqrt{-1} \bmod 5$ and $\pi \equiv 3+2\sqrt{-1} \bmod 4$. Hence π is a primary element that is not a rational integer. Our assertion follows from Theorem 3.5. □

4. TOTAL IRREDUCIBILITY OVER INTEGER RINGS

In the previous section, we proved existence of totally irreducible Euclid prime sequences over $\mathbb{F}_p[X]$ for infinitely many primes p. A natural question arises: can $E_{\min}(l,c)_{\mathbb{Z}}$ be totally irreducible for some l and c? In this section, we consider problems related to this question.

It is easy to observe that $E_{\min}(l,1)_{\mathbb{Z}}$ is never totally irreducible. For an odd l, this is trivial, and it is an easy computation to verify that $E_{\min}(2,1)_{\mathbb{Z}}$ is not totally irreducible. Another example is that $E_{\min}(X,4)_{\mathbb{Z}[X]}$ is not totally irreducible, for the first two terms are X and $X+4$, and $X(X+4)+4=(X+2)^2$. Therefore, $E_{\min}(l,4)_{\mathbb{Z}}$ is not totally irreducible for any prime l.

Theorem 4.1. *Put $F_k := 2^{2^k}+1$ for $k \geq 0$. Assume that k is an integer such that F_k is a prime. Let l be a prime. Assume that $l \neq F_k$ and that $l \not\equiv -1 \bmod F_k$. Then $E_{\min}(l,2)_{\mathbb{Z}}$ is not totally irreducible.*

Proof: Clearly, $E_{\min}(2,2)_{\mathbb{Z}}$ is not totally irreducible. In the rest of the proof, we assume that l is an odd prime. Suppose $E_{\min}(l,2)_{\mathbb{Z}}$ is totally irreducible. For $n \geq 0$, denote its nth term by l_n. Then we see that

$$l_n=(l+1)^{2^n}+1$$

by induction on n.

Observe that $\mathbb{F}_{F_k}^{\times}$ is a cyclic group of order 2^{2^k}. Thus there exists $m \in \mathbb{N}$ such that

$$(l+1)^{2^m}=1 \quad \text{and} \quad (l+1)^{2^{m-1}} \neq 1$$

in $\mathbb{F}_{F_k}$, i.e., $(l+1)^{2^{m-1}} \equiv -1 \bmod F_k$. Therefore, $F_k \mid l_{m-1}$. However, both F_k and l_{m-1} are prime numbers. Thus $F_k = l_{m-1}$ and

$$2^{2^k}=(l+1)^{2^{m-1}}. \tag{4–1}$$

This implies $l+1=2^s$ with some $s \in \mathbb{N}$. Thus, l must be a Mersenne prime, and s must be prime. On the

other hand, substituting $l+1$ by 2^s in (4–1), we obtain $2^k = s2^{m-1}$. Hence s is a power of 2. Therefore, $s = 2$ and $l = 3$.

Straightforward computation of $E_{\min}(3,2)_{\mathbb{Z}}$ shows that its fourth term is divisible by 641. (Recall that $E_{\min}(3,2)$ begins with the (-1)th term. Actually, the nth term of $E_{\min}(3,2)$ is F_{n+1} for $-1 \le n \le 3$.) Thus, $E_{\min}(3,2)_{\mathbb{Z}}$ is not totally irreducible. □

Remark 4.2. If there exist infinitely many Fermat primes, we can conclude that $E_{\min}(l,2)_{\mathbb{Z}}$ is never totally irreducible for a prime l. However, it is open whether there are infinitely many Fermat primes.

On the other hand, for arbitrarily large k, we can show that there exist infinitely many $c \in \mathbb{N}$ and a prime l such that $\prod_{m=-1}^{n} l_n + c$ is prime for all $n \le k$ under "Hypothesis H" proposed in [Schinzel and Sierpiński 58]. This hypothesis is as follows.

Hypothesis H. Let $f_1(X), \dots, f_k(X) \in \mathbb{Z}[X]$ be irreducible polynomials with positive leading coefficients. Assume that for any p there exists $t_p \in \mathbb{Z}$ (depending on p) satisfying

$$f_1(t_p) \cdots f_k(t_p) \not\equiv 0 \bmod p.$$

Then there are infinitely many integers n such that $f_1(n), \dots, f_k(n)$ are all prime numbers.

Recall that $E_{\min}(X,1)_{\mathbb{F}_5[X]}$ is totally irreducible (cf. Example 3.4). Hence for any $k \in \mathbb{Z}$, the sequence $E_{\min}(X, 5k+1)_{\mathbb{Z}[X]}$ is totally irreducible. There are many other $c \in \mathbb{Z}$ for which $E_{\min}(X,c)_{\mathbb{Z}[X]}$ is totally irreducible. For example, $E_{\min}(X,2)_{\mathbb{Z}[X]}$ is totally irreducible because its nth term is $(X+1)^{2^n}+1$ for $n \ge 0$, which is irreducible by Eisenstein's criterion.

Theorem 4.3. *Let $c \in \mathbb{Z}$ be even. Assume that $E_{\min}(X,c)_{\mathbb{Z}[X]}$ is totally irreducible and that all prime factors of $c-1$ are congruent to* 1 mod 4. *Suppose that Hypothesis H is true.*

Then for an arbitrary $k \in \mathbb{N}$, there exist infinitely many primes l such that $\prod_{m=-1}^{n} l_m + c$ is prime for all $-1 \le n \le k$, where l_n is the nth term of $E_{\min}(l,c)_{\mathbb{Z}}$.

Proof: Let $A_n(X) \in \mathbb{Z}[X]$ be the nth term of $E_{\min}(X,c)_{\mathbb{Z}[X]}$. Then $A_n(X)$ is a monic irreducible polynomial.

Total irreducibility implies

$$A_{n+1}(X) = (A_n(X) - c)A_n(X) + c,$$

or equivalently,

$$A_{n+1}(X) - 1 = (A_n(X) - c + 1)(A_n(X) - 1) \qquad (4\text{–}2)$$

for $n \ge 0$. Assume that p is a prime not dividing $c-1$. Then we have $A_{-1}(-c+1) = -c+1 \not\equiv 0 \bmod p$ and $A_0(-c+1) = 1$.

By (4–2), we see that

$$\begin{aligned} A_{-1}(-c+1)\cdots A_{k+1}(-c+1) &= (-c+1)\cdot 1 \cdots 1 \\ &= -c+1 \\ &\not\equiv 0 \bmod p. \end{aligned}$$

On the other hand, let p be a prime dividing $c-1$. Since $p \equiv 1 \bmod 4$, there exists $t_p \in \mathbb{N}$ such that $t_p^2 \equiv -1 \bmod p$.

Note that $t_p \not\equiv 1 \bmod p$ because $p \ne 2$. Therefore $A_{-1}(t_p - 1) \not\equiv 0 \bmod p$ and $A_0(t_p) \equiv t_p \not\equiv 0 \bmod p$. Using (4–2) and $t_p^2 \equiv -1 \bmod p$, we obtain $A_n(t_p) \equiv (-1)^n t_p$ for $n \ge 0$ by induction on n. Thus $A_{-1}(t_p)A_0(t_p)\cdots A_{k+1}(t_p) \not\equiv 0 \bmod p$. Our assertion follows from the Schinzel–Sierpiński conjecture. □

5. SOME NUMERICAL COMPUTATIONS

Unlike integer factorization, factorization of polynomials over finite fields is computationally feasible. With the order defined in Definition 2.4, we computed $E_{\min}(X,c)_{\mathbb{F}_p[X]}$ up to the 2600th term for $p \le 5$ and $c \in \mathbb{F}_p^{\times}$ except for the case $p = 5$ and $c = 1$, in which $E_{\min}(X,c)_{\mathbb{F}_p[X]}$ is totally irreducible (cf. Example 3.4).

These numerical computations strongly suggest that the Shanks conjecture over $\mathbb{F}_p[X]$ with initial term X is true unless $E_{\min}(X,c)_{\mathbb{F}_p[X]}$ is totally irreducible.

In Table 1, the columns labeled $*$ show the number of irreducible polynomials in $\mathbb{F}_p[X]$ of degrees indicated by the first column. In the columns labeled with c, an entry m/n implies that m irreducible polynomials appeared and the last occurrence was the nth term. We can confirm that all irreducible polynomials of small degree (less than or equal to 9 for $p = 2$, 5 for $p = 3$, 3 for $p = 5$) appear.

Put $d_{p,c}(m) := \deg \prod_{n=-1}^{m} l_n$ in $E_{\min}(X,c)_{\mathbb{F}_p[X]}$. In Table 2, we list values of $d_{p,c}(m)$ for the above cases. We observe that $d_{3,1}(m)$ and $d_{3,2}(m)$ grow at similar rates as m increases (for $m \le 2600$). However, $d_{5,4}(m)$ seems to grow faster than $d_{5,2}(m)$ and $d_{5,3}(m)$. Whether this holds is open.

	$p=2$		$p=3$			$p=5$			
	$*$	$c=1$	$*$	$c=1$	$c=2$	$*$	$c=2$	$c=3$	$c=4$
1	2	2/0	3	3/1	3/3	5	5/4	5/9	5/7
2	1	1/1	3	3/13	3/19	10	10/72	10/56	10/70
3	2	2/6	8	8/25	8/89	40	40/630	40/469	40/458
4	3	3/13	18	18/304	18/255	150	146/2559	145/1974	148/2531
5	6	6/32	48	48/1565	48/1366	624	329/2586	311/2591	315/2599
6	9	9/329	116	115/2556	109/2519	2580	299/2600	317/2600	306/2600
7	18	18/519	312	204/2559	195/2586	11160	236/2584	241/2589	240/2588
8	30	30/783	810	184/2587	209/2561	48750	195/2596	178/2579	187/2571
9	56	56/2217	2184	200/2579	201/2582	217000	170/2597	149/2590	137/2598
10	99	87/2587	5880	186/2578	167/2595	976248	119/2577	111/2592	107/2476

TABLE 1. Numbers of irreducible polynomials appearing up to the 2600th term.

	$p=2$	$p=3$		$p=5$		
m	$c=1$	$c=1$	$c=2$	$c=2$	$c=3$	$c=4$
200	6762	5722	4834	2367	2156	22028
400	28312	13810	27943	9411	5281	30590
600	37103	37116	37192	15793	11289	37469
800	89437	44428	50156	25421	18466	41959
1000	100796	50080	77096	30727	25675	49376
1200	114843	82763	87850	36089	32026	52761
1400	141105	88415	101411	43831	36729	56438
1600	155845	98577	109257	49034	42783	62857
1800	168181	116547	119540	54461	48103	154931
2000	178069	124213	125698	58440	52914	160861
2200	216659	131377	138323	65993	61101	172040
2400	232173	144763	146836	73600	75916	182809
2600	246567	152216	156042	80044	80257	188120

TABLE 2. Degrees of products $\prod_{n=-1}^{m} l_n$

ACKNOWLEDGMENTS

The authors would like to thank the Department of Mathematics, Saitama University, Japan, for providing computer resources to perform some of computations described in Section 5, and Professor Igor Shparlinski for valuable comments on an earlier version of the paper.

REFERENCES

[Ireland and Rosen 82] K. Ireland and M. Rosen. *A Classical Introduction to Modern Number Theory*. New York: Springer, 1982.

[Narkiewicz 2000] W. Narkiewicz. *The Development of Prime Number Theory: From Euclid to Hardy and Littlewood*, Springer Monographs in Mathematics. New York: Springer, 2000.

[Schinzel and Sierpiński 58] A. Schinzel and W. Sierpiński. "Sur certaines hypotheses concernant les nombres premiers." *Acta Arith.* 4 (1958), 185–208 (erratum ibid. 5 (1958), 259).

[Shanks 91] D. Shanks. "Euclid's Primes." *Bull. Inst. Combin. Appl.* 1 (1991), 33–36.

[Wagstaff 93] S. Wagstaff, Jr. "Computing Euclid's Primes." *Bull. Inst. Combin. Appl.* 8 (1993), 23–32.

Nobushige Kurokawa,Department of Mathematics,Tokyo Institute of Technology, Tokyo, 152-8551, Japan (kurokawa@math.titech.ac.jp)

Takakazu Satoh, Department of Mathematics, Tokyo Institute of Technology, Tokyo, 152-8551, Japan (satohaar@mathpc-satoh.math.titech.ac.jp)

Received November 30, 2006; accepted in revised form October 19, 2007.