ON THE IRREGULAR PRIMES WITH RESPECT TO
EULER POLYNOMIALS

SU HU, MIN-SOO KIM, AND MIN SHA

Abstract. An odd prime $p$ is called irregular with respect to
Euler polynomials if it divides the numerator of one of the numbers
$E_1(0), E_3(0), \ldots, E_{p-2}(0)$,
where $E_n(x)$ is the $n$-th Euler polynomial. As in the classical case,
we link the regularity of primes to the divisibility of some class
numbers. Besides, we obtain some results on the distribution of
such irregular primes.

1. Introduction

1.1. The classical case. The Bernoulli numbers $B_0, B_1, B_2, \ldots$ are
given by $B_0 = 1$ and the recursion relation

\begin{equation}
B_n = -\frac{1}{n+1} \sum_{k=0}^{n-1} \binom{n+1}{k} B_k, \quad n = 1, 2, 3, \ldots.
\end{equation}

They are exactly the values at the zero of the Bernoulli polynomials
$B_n(x)$ ($n = 0, 1, 2, \ldots$), which are defined by the generating function

\begin{equation}
\frac{te^tx}{e^t-1} = \sum_{n=0}^{\infty} B_n(x) \frac{t^n}{n!}.
\end{equation}

That is, $B_n = B_n(0), n = 0, 1, 2, \ldots$; see [6, p. 230, Lemma 1]. It is
well-known that $B_n = 0$ for any odd $n > 1$. Throughout the paper,
every rational number is assumed to be in lowest terms.

Inspired by Fermat’s Last Theorem, Kummer introduced the notion
of regular prime as follows. An odd prime $p$ is said to be regular (with
respect to Bernoulli numbers) if $p$ does not divide the numerator of
any of the Bernoulli numbers $B_2, B_4, \ldots, B_{p-3}$. If $p$ is not regular, it is
called irregular. Kummer proved that Fermat’s Last Theorem is true
for a prime exponent $p$ if $p$ is regular. This raised attention in irregular
primes.

2010 Mathematics Subject Classification. 11B68, 11A07,11R29.

Key words and phrases. Irregular prime, Bernoulli number and polynomial, Eu-
er number and polynomial, refined class number.
The notion of irregular prime has an important application in algebraic number theory. Let \( \mathbb{Q}(\zeta_p) \) be the \( p \)-th cyclotomic field, and \( h_p \) the class number of \( \mathbb{Q}(\zeta_p) \), where \( \zeta_p \) is a \( p \)-th root of unity. Denote by \( h_p^+ \) the class number of \( \mathbb{Q}(\zeta_p + \zeta_p^{-1}) \), and define \( h_p^- = h_p / h_p^+ \), which indeed is a positive integer and called the relative class number of \( \mathbb{Q}(\zeta_p) \). Kummer proved the following result.

**Theorem 1.1** (Kummer, [21, Theorem 5.16]). *Let \( p \) be an odd prime. Then, \( p \) is irregular if and only if \( p \mid h_p^- \).*

For the distribution of irregular primes, Jensen [8] first proved that there are infinitely many irregular primes not of the form \( 4n + 1 \), then Montgomery [15] generalized this by replacing 4 with any integer greater than 2. The following result, given by Metsänkylä [14] is currently the best up to our knowledge; see [9, 13, 22] for the previous results.

**Theorem 1.2.** *Given an integer \( m > 2 \), let \( \mathbb{Z}_m^* \) be the multiplicative group of the residue classes modulo \( m \), and let \( H \) be a proper subgroup of \( \mathbb{Z}_m^* \). Then, there exist infinitely many irregular primes not lying in the residue classes in \( H \).*

Besides, Carlitz [2] gave a simple proof of the weaker result that there are infinitely many irregular primes, and recently Luca, Pizarro-Madariaga and Pomerance [12, Theorem 1] gave the following quantitative version:

\[
\# \{ \text{prime } p \leq x : p \text{ is irregular} \} \geq (1 + o(1)) \frac{\log \log x}{\log \log \log \log x}
\]

as \( x \to \infty \). Note that Siegel [17] conjectured that the proportion of regular primes in the asymptotic sense is about

\[ \exp(-1/2) = 0.6065 \ldots \]

which is consistent with numerical data. However, it is still not known whether or not there are infinitely many regular primes.

1.2. **Regularity with respect to Euler numbers.** In [2] Carlitz also gave a similar notion of irregular prime with respect to Euler numbers.

The Euler numbers \( E_0, E_1, E_2, \ldots \) are given by \( E_0 = 1 \) and the recursion relation

\[
E_n = - \sum_{k=0}^{n-1} \binom{n}{k} E_k, \quad n = 1, 2, \ldots .
\]

Moreover, \( E_n = 0 \) for any odd \( n \geq 1 \). As Bernoulli numbers, Euler numbers also can be defined via special values of some polynomials.
The Euler polynomials $E_n(x) (n = 0, 1, 2, \ldots)$ are defined by the generating function

\begin{equation}
\frac{2e^{xt}}{e^t + 1} = \sum_{n=0}^{\infty} E_n(x) \frac{t^n}{n!}.
\end{equation}

Then, $E_n = 2^n E_n(1/2), n = 0, 1, 2, \ldots$. Different from Bernoulli polynomials, the numbers $E_n(0) (n = 0, 1, 2, \ldots)$ are not named Euler numbers in the literature.

Now, a prime $p$ is said to be irregular with respect to Euler numbers if it divides at least one of the numbers $E_2, E_4, \ldots, E_{p-3}$. Vandiver in [19] indeed proved that Fermat’s Last Theorem is true for a prime exponent $p$ if $p$ is regular with respect to Euler numbers.

In [2] Carlitz showed that there are infinitely many irregular primes with respect to Euler numbers. Luca, Pizarro-Madariaga and Pomerance in [12, Theorem 2] also gave the same quantitative result about these irregular primes as in (1.3). About the distribution, currently we only know that there are infinitely many irregular primes with respect to Euler numbers not lying in the residue classes $\pm 1 \pmod{8}$, which was proven by Ernvall [3].

We remark that we still don’t know whether or not the regularity with respect to Euler numbers depends on the divisibility of some class numbers of number fields.

1.3. Regularity with respect to Euler polynomials. It is well-known that for any integer $n \geq 0$,

\begin{equation}
E_n(0) = 2(1 - 2^{n+1})B_{n+1}/(n + 1);
\end{equation}

for example see [18, Equation (2.1)]. So, for any even integer $n > 1$, we have $E_n(0) = 0$. Moreover, $2^n E_n(0) \in \mathbb{Z}$ for any integer $n \geq 1$; see [10, Lemma 2.1].

Analogy with Kummer and Carlitz, we here define an odd prime $p$ to be irregular with respect to Euler polynomials if it divides the numerator of one of the numbers $E_1(0), E_3(0), \ldots, E_{p-2}(0)$. For simplicity, we call such prime $p$ $E$-irregular.

Based on (1.6), we first prove that

**Theorem 1.3.** For any odd prime $p$, if $p$ is irregular with respect to Bernoulli numbers, then it is also $E$-irregular.

In other words, if an odd prime is $E$-regular, then it is also regular with respect to Bernoulli numbers. Then, in view of Theorem 1.2 we directly have
**Corollary 1.4.** Given an integer $m > 2$, let $H$ be a proper subgroup of $\mathbb{Z}_m^*$. Then, there exist infinitely many $E$-irregular primes not lying in the residue classes in $H$.

From Corollary 1.4 we can get a direct consequence.

**Corollary 1.5.** For each residue class of $3 \pmod{4}$ and $5 \pmod{6}$, it contains infinitely many $E$-irregular primes.

Compared with (1.3), one much better result can be obtained about the number of $E$-irregular primes up to a fixed number $x$. Let $\mathcal{P}_E(x)$ be the number of $E$-irregular primes not greater than $x$.

**Theorem 1.6.** For any sufficiently large $x$, we have

\begin{equation}
\#\mathcal{P}_E(x) \geq (0.875 - A) \frac{x}{\log x} + O\left(\frac{x(\log \log x)^2}{\log^{5/4} x}\right),
\end{equation}

where $A$ is the Artin constant

$$A = \prod_{\text{prime } p} \left(1 - \frac{1}{p(p-1)}\right) = 0.373955 \ldots .$$

Since $0.875 - A > 0.5$, there are more $E$-irregular primes than $E$-regular primes. Using Theorem 1.6 and Dirichlet’s theorem on arithmetic progressions, we directly get a new result about the distribution of $E$-irregular primes compared with Corollary 1.4.

**Corollary 1.7.** Given an integer $m > 2$, let $H$ be a proper subgroup of $\mathbb{Z}_m^*$. If

$$\frac{\#H}{\varphi(m)} \geq A + 0.125,$$

where $\varphi$ is Euler’s totient function and $A$ has been defined in Theorem 1.6, then there exist infinitely many $E$-irregular primes lying in the residue classes in $H$.

Notice that $A + 0.125 < 0.5$, from Corollary 1.7 we further have

**Corollary 1.8.** For each residue class of $1 \pmod{4}$ and $1 \pmod{6}$, it contains infinitely many $E$-irregular primes.

Finally, as in the classical case, we indeed can link the $E$-regularity of primes to the divisibility of some class numbers of cyclotomic fields. Let $S$ be the set of infinite places of $\mathbb{Q}(\zeta_p)$ and $T$ the set of places above the prime 2. Denote by $h_{p,2}$ the $(S,T)$-refined class number of $\mathbb{Q}(\zeta_p)$. Similarly, let $h_{p,2}^+$ be the refined class number of $\mathbb{Q}(\zeta_p + \zeta_p^{-1})$ with respect to its infinite places and places above the prime 2. For
the definition of the refined class number of global fields, we refer to Gross [4, Section 1], Aoki [1, Section 7] or [5, Section 2]. Define
\[ h_{p,2}^- = h_{p,2}^- \cdot h_{p,2}^+ \]
which is indeed an integer (see [5, Proof of Proposition 3.4]).

**Theorem 1.9.** Let \( p \) be an odd prime. Then, \( p \) is \( E \)-irregular if and only if \( p \mid h_{p,2}^- \).

## 2. Preliminaries

In this section, we gather some results which are used later on and obtain some new properties about the values \( E_n(0) \).

We first recall two classical results about Bernoulli numbers; for instance see [14]. Given an integer \( k \geq 1 \), let \( N_{2k} \) and \( D_{2k} \) be the numerator and denominator of the Bernoulli number \( B_{2k} \), respectively. That is,
\[ B_{2k} = \frac{N_{2k}}{D_{2k}}, \quad \gcd(N_{2k}, D_{2k}) = 1, \]
\( D_{2k} > 0 \) and the sign of \( N_{2k} \) is \((-1)^{k-1}\).

**Lemma 2.1.** For each integer \( k \geq 1 \), \( D_{2k} \) is the product of those distinct primes \( p \) for which \( p - 1 \) divides \( 2k \).

**Lemma 2.2.** For every integer \( k \geq 1 \), there is a unique decomposition \( k = k_1k_2 \) such that \( k_1 \geq 1, k_2 \geq 1, \gcd(k_1, k_2) = 1, k_1 \mid N_{2k}, \) and every prime in \( k_2 \) divides \( D_{2k} \).

We have known that \( 2^n E_n(0) \in \mathbb{Z} \) for any integer \( n \geq 1 \). So, the denominator of \( E_n(0) \) is some power of 2 for each \( n \geq 1 \). We actually can determine such denominators. Since \( E_n(0) = 0 \) when \( n \) is even, we only need to consider the case when \( n \) is odd.

**Lemma 2.3.** For any odd integer \( n \geq 1 \), let \( m \) be the integer satisfying \( 2^m \mid (n + 1) \) and \( 2^{m+1} \nmid (n + 1) \). Then, the denominator of \( E_n(0) \) is \( 2^m \).

**Proof.** We write \( n + 1 = 2k \). Then, by (1.6) we have
\[ E_n(0) = 2(1 - 2^{2k}) \frac{B_{2k}}{2k} = (1 - 2^{2k}) \frac{N_{2k}/k_1}{k_2D_{2k}}, \]
where \( k_1 \) and \( k_2 \) are defined as in Lemma 2.2. From Lemma 2.1, we know that \( D_{2k} \) is an even and square-free integer, and so \( |N_{2k}| \) is an odd integer (and so is \( k_1 \)). Thus, we have \( 2^m \mid k_2D_{2k} \) and \( 2^{m+1} \nmid k_2D_{2k} \). Noticing \( 2^n E_n(0) \in \mathbb{Z} \), we conclude the proof. \( \square \)

For any prime \( p \) and two rational numbers \( a, b \), “\( a \equiv b \pmod{p} \)” means that \( p \) divides the numerator of \( b - a \).
Lemma 2.4. For any odd prime $p$, assume that $m, n$ are two positive integers satisfying $m + 1 \equiv n + 1 \not\equiv 0 \pmod{p - 1}$. Then
\[ E_m(0) \equiv E_n(0) \pmod{p}. \]

Proof. If $m$ is even, then $n$ is also even, and so $E_m(0) = E_n(0) = 0$. Now, we suppose that both $m$ and $n$ are odd.

We first recall a basic property of Bernoulli numbers due to Kummer. Suppose that $2^k \equiv 2^l \not\equiv 0 \pmod{p - 1}$, then
\[ B_{2^k} \equiv B_{2^l} \pmod{p}; \]
see [21, Corollary 5.14].

Write $m = (p - 1)k + n$ for some integer $k$. Using (1.6) and (2.1), we deduce that
\[
E_m(0) = 2(1 - 2^{m+1}) \frac{B_{m+1}}{m+1} = 2(1 - 2^{(p-1)k+n+1}) \frac{B_{m+1}}{m+1} \\
\equiv 2(1 - 2^{n+1}) \frac{B_{m+1}}{m+1} \equiv 2(1 - 2^{n+1}) \frac{B_{n+1}}{n+1} = E_n(0) \pmod{p}.
\]
This completes the proof. \qed

For a primitive Dirichlet character $\chi$ with an odd conductor $f$, the generalized Euler numbers $E_{n,\chi}$ are defined by
\[
2 \sum_{a=1}^{f} \frac{(-1)^a \chi(a)e^{at}}{e^{ft} + 1} = 2 \sum_{n=0}^{\infty} E_{n,\chi} \frac{t^n}{n!};
\]
see [11, Section 5.1].

For any odd prime $p$, let $\omega_p$ be the Teichmüller character of $\mathbb{Z}/p\mathbb{Z}$, and then any multiplicative character of $\mathbb{Z}/p\mathbb{Z}$ is of the form $\omega_p^k$ for some $1 \leq k \leq p - 1$. In particular, the odd characters are $\omega_p^k$, $k = 1, 3, \ldots, p - 2$.

We have the following result.

Lemma 2.5. Suppose that $p$ is an odd prime and $n$ is an odd integer. Then
\[ E_{0,\omega_p^n} \equiv E_n(0) \pmod{p}. \]

Proof. Here we use some notation in [11]. By [11, Proposition 5.4], for any integers $k, n \geq 0$, we have
\[
E_{k,\omega_p^n \cdot -k} = \int_{\mathbb{Z}_p} \omega_p^{n-k}(a)a^k d\mu_{-1}(a).
\]
Besides, by [11, Proposition 2.1 (1)] we have

\begin{equation}
E_n(0) = \int_{\mathbb{Z}/p} a^n d\mu_{-1}(a).
\end{equation}

Since \( \omega_p(a) \equiv a \pmod{p} \), we have

\begin{equation}
\omega_p^{n-k}(a) \equiv a^{n-k} \pmod{p} \quad \text{and} \quad \omega_p^{n-k}(a)a^k \equiv a^n \pmod{p}.
\end{equation}

From (2.3) and (2.4), we have

\begin{equation*}
E_{k,\omega_p^{n-k}} - E_n(0) = \int_{\mathbb{Z}/p} (\omega_p^{n-k}(a)a^k - a^n) d\mu_{-1}(a).
\end{equation*}

By (2.5), the integral function is congruent to zero modulo \( p \). So, the desired result follows by choosing \( k = 0 \).

We remark that Lemma 2.5 is an analogue of a well-known result for the generalized Bernoulli numbers; see [21, Corollary 5.15].

3. Proofs

We only need to prove Theorems 1.3, 1.6 and 1.9.

3.1. Proof of Theorem 1.3. Given an odd prime \( p \), if it is irregular with respect to Bernoulli numbers, then \( p \) divides the numerator of some Bernoulli number \( B_{2k} \) with \( 1 \leq k \leq (p-3)/2 \). Since \( \gcd(p, 2k) = 1 \), \( p \) divides the numerator of \( B_{2k}/(2k) \). So, \( p \) divides the numerator of

\begin{equation*}
2(1 - 2^{2k}) \frac{B_{2k}}{2k} = E_{2k-1}(0),
\end{equation*}

where the identity follows from (1.6). Hence, \( p \) is also irregular with respect to Euler polynomials.

3.2. Proof of Theorem 1.6. Given \( x \geq 3 \), we first define two sets of primes: the set \( \mathcal{P}_1(x) \) consists of primes \( p \leq x \) such that \( p \equiv 3 \pmod{4} \) and the multiplicative order of 2 modulo \( p \) is \( (p-1)/2 \), and

\[ \mathcal{P}_2(x) = \{ \text{prime } p \leq x : 2 \text{ is a primitive root modulo } p \}. \]

Let \( p \) be an odd prime not contained in \( \mathcal{P}_1(x) \cup \mathcal{P}_2(x) \). Then, the multiplicative order \( r \) of 2 modulo \( p \) satisfies \( r < p-1 \) and \( r \mid p-1 \). Let \( m = r \) if \( r \) is even, and otherwise put \( m = 2r \). So, \( m \) is an even integer such that \( p \mid 2^m - 1 \) and \( m \leq p-1 \). We write \( m = 2k \). Notice that

\begin{equation*}
E_{2k-1}(0) = (1 - 2^{2k}) \frac{B_{2k}}{k} = \frac{1 - 2^{2k}}{k_2D_{2k}} \cdot \frac{N_{2k}}{k_1},
\end{equation*}

where \( k_1 \) and \( k_2 \) are defined as in Lemma 2.2. If \( 2k = p-1 \), then we must have that \( r = (p-1)/2 \) and moreover it is an odd integer, and
so \( p \equiv 3 \pmod{4} \), this contradict with \( p \not\in \mathcal{P}_1(x) \). So, we must have \( 2k < p - 1 \). Then, by Lemma 2.1 we have \( p \nmid D_{2k} \). Combining the fact \( p \mid 2^{2k} - 1 \) with Lemma 2.2, we get that \( p \mid E_{2k-1}(0) \), which implies that \( p \) is \( E \)-irregular.

Hence, for any prime \( p \not\in \mathcal{P}_1(x) \cup \mathcal{P}_2(x) \), \( p \) is \( E \)-irregular. As a result, we have

\[
\tag{3.1} \# \mathcal{P}_E(x) \geq \pi(x) - \# \mathcal{P}_1(x) - \# \mathcal{P}_2(x),
\]

where \( \pi(x) \) is the number of primes \( p \leq x \). Now, to complete the proof we only need to estimate the sizes of \( \mathcal{P}_1(x) \) and \( \mathcal{P}_2(x) \).

Let \( p \) be a prime in \( \mathcal{P}_1(x) \). Since \( 2^{(p-1)/2} \equiv 1 \pmod{p} \), we see that 2 is a quadratic residue modulo \( p \). Noticing \( p \equiv 3 \pmod{4} \), we must have \( p \equiv 7 \pmod{8} \). Then, \( p \) is of the form either \( 24n + 7 \) or \( 24n + 23 \). If \( p \) is of the form \( 24n + 23 \), then \( p \equiv 2 \pmod{3} \), and thus 2 is a cubic residue modulo \( p \) (actually any integer is a cubic residue modulo \( p \)). So, we have

\[ 2^{(p-1)/3} \equiv 1 \pmod{p}, \]

which contradicts with the assumption that the multiplicative order of 2 modulo \( p \) is \( (p - 1)/2 \). Hence, \( p \) must be of the form \( 24n + 7 \). So,

\[
\# \mathcal{P}_1(x) \leq \# \{ \text{prime } p \leq x : p \equiv 7 \pmod{24} \} = \frac{x}{8 \log x} + O\left( \frac{x}{\log^2 x} \right), \tag{3.2}
\]

where the asymptotic identity follows from the Siegel-Walfisz theorem (for instance see [7, Corollary 5.29]).

Using a result of Vinogradov [20] related to Artin’s conjecture on primitive roots (see also [16, Equation (12)]), we directly obtain

\[
\# \mathcal{P}_2(x) \leq \frac{Ax}{\log x} + O\left( \frac{x(\log \log x)^2}{\log^{5/4} x} \right). \tag{3.3}
\]

Finally, the desired result follows from (3.1), (3.2) and (3.3).

### 3.3. Proof of Theorem 1.9.

By [5, Proposition 3.4], we obtain

\[
h_{p,2} = (-1)^{\frac{\omega_p-1}{2}}2^{2-p} \prod_{1 \leq k < p \atop k \text{ odd}} E_{0,\omega_p^k}
\]

\[= (-1)^{\frac{\omega_p-1}{2}}2^{2-p}E_{0,\omega_p}E_{0,\omega_p^3} \cdots E_{0,\omega_p^{p-2}}.\]

Using Lemma 2.5, we have

\[
h_{p,2} \equiv (-1)^{\frac{\omega_p-1}{2}}2^{2-p}E_{1}(0)E_{3}(0) \cdots E_{p-2}(0) \pmod{p}.
\]

So, we conclude the proof.
Acknowledgement

This work was supported by the National Natural Science Foundation of China, Grant No. 11501212. The research of Min-Soo Kim was also supported by the Kyungnam University Foundation Grant, 2017. The research of Min Sha was also supported by the Macquarie University Research Fellowship.

References

[1] N. Aoki, *On Tate’s refinement for a conjecture of Gross and its generalization*, J. Théor. Nombres Bordeaux **16** (2004), 457–486.
[2] L. Carlitz, *Note on irregular primes*, Proc. Amer. Math. Soc. **5** (1954), 329–331.
[3] R. Ernvall, *On the distribution mod 8 of the E-irregular primes*, Ann. Acad. Sci. Fenn. Ser. A I, **1** (1975), 195–198.
[4] B. Gross, *On the values of abelian L-functions at s = 0*, J. Fac. Sci. Univ. Tokyo **35** (1988), 177–197.
[5] S. Hu and M.-S. Kim, *The (S, {2})-Iwasawa theory*, J. Number Theory **158** (2016), 73–89.
[6] K. Ireland and M. Rosen, *A classical introduction to modern number theory*, 2nd ed., Graduate Texts in Mathematics **84**, Springer-Verlag, New York, 1990.
[7] H. Iwaniec and E. Kowalski, *Analytic Number Theory*, Amer. Math. Soc., Providence, RI, 2004.
[8] K. L. Jensen, *Om talteoretiske Egenskaber ved de Bernoulliske Tal*, Nyt Tidsskr. Mat. **26**, Afd. B (1915), 73–83.
[9] J. Johnsen, *On the distribution of irregular primes*, J. Number Theory **8** (1976), 434–437.
[10] M.-S. Kim, *On Euler numbers, polynomials and related p-adic integrals*, J. Number Theory **129** (2009), 2166–2179.
[11] M.-S. Kim and S. Hu, *On p-adic Hurwitz-type Euler zeta functions*, J. Number Theory **132** (2012), 2977–3015.
[12] F. Luca, A. Pizarro-Madariaga and C. Pomerance, *On the counting function of irregular primes*, Indag. Math. **26** (2015), 147–161.
[13] T. Metsänkylä, *Note on the distribution of irregular primes*, Ann. Acad. Sci. Fenn. Ser. A I, **492** (1971), 1–7.
[14] T. Metsänkylä, *Distribution of irregular prime numbers*, J. Reine Angew. Math. **282** (1976), 126–130.
[15] H. L. Montgomery, *Distribution of irregular primes*, Illinois J. Math. **9** (1965), 553–558.
[16] P. Moree, *Artin’s primitive root conjecture – a survey*, Integers **12A** (2012), #A13.
[17] C. L. Siegel, *Zu zwei Bemerkungen Kummers*, Nachr. Akad. d. Wiss. Goettingen, Math. Phys. K1. **11** (1964), 51–62.
[18] Z.-W. Sun, *On Euler numbers modulo powers of two*, J. Number Theory **115** (2005), 371–380.
[19] H. S. Vandiver, *Note on Euler number criteria for the first case of Fermat’s last theorem*, Amer. J. Math. **62** (1940), 79–82.
[20] A. I. Vinogradov, *Artin’s L-series and his conjectures*, Trudy Mat. Inst. Steklov. 122 (1971), 123–140.
[21] L. C. Washington, *Introduction to Cyclotomic Fields*, 2nd ed., Springer-Verlag, New York, 1997.
[22] H. Yokoi, *On the distribution of irregular primes*, J. Number Theory 7 (1975), 71–76.

Department of Mathematics, South China University of Technology, Guangzhou 510640, China
E-mail address: mahusu@scut.edu.cn

Center for General Education, Kyungnam University, 7(Woryeong-dong) kyungnamdaehak-ro, Masanhappo-gu, Changwon-si, Gyeongsangnam-do 631-701, Republic of Korea
E-mail address: mskim@kyungnam.ac.kr

Department of Computing, Macquarie University, Sydney, NSW 2109, Australia
E-mail address: shamin2010@gmail.com