Primitive roots and quadratic non-residues

by

A. SCHINZEL (Warszawa)

C. Hooley [1] deduced Artin’s conjecture on primitive roots from the Riemann hypothesis for the Dedekind zeta function of a certain class of fields. His investigations have been taken further by K. R. Matthews [4], who has deduced from a similar hypothesis a formula for the natural density of the primes for which finitely many given numbers are primitive roots. We shall prove

**Theorem.** Let $\mathcal{A}, \mathcal{B}$ be two finite disjoint sets of primes of cardinalities $n > 0$ and $m$, respectively, with $2 \notin \mathcal{A} \cup \mathcal{B}$. Under the Riemann hypothesis for the Dedekind zeta functions of Kummer extensions the natural density of the primes $p$ such that

$$ (1) \quad (2 \mid p) = 1 = (b \mid p) \quad \text{for all } b \in \mathcal{B} $$

and all $a \in \mathcal{A}$ are primitive roots modulo $p$ equals

$$ d(\mathcal{A}, \mathcal{B}) = \frac{\Delta_n}{2^{m+2}} \prod_{a \in \mathcal{A}} (1 + (-1 \mid a)d_{n,a}) \prod_{b \in \mathcal{B}} (1 - (-1 \mid b)d_{n,b}) $$

$$ + \frac{\Delta_n}{2^{m+2}} \prod_{a \in \mathcal{A}} (1 + d_{n,a}) \prod_{b \in \mathcal{B}} (1 - d_{n,b}), $$

where

$$ d_{n,p} = \frac{c_n(p)}{1-c_n(p)}, \quad c_n(p) = \frac{1}{p-1} \left( \frac{1}{p} - \left( \frac{1}{p} \right)^n \right), \quad \Delta_n = \prod_{p \text{ prime}} (1 - c_n(p)). $$

**Corollary 1.** Let $p_i$ be the $i$th prime. Under the extended Riemann hypothesis for Kummer extensions, the natural density of the primes $p$ such that $p_k (k > 1)$ is for $p$ the least quadratic non-residue and $p_i$ is the least

2010 Mathematics Subject Classification: Primary 11N99.

Key words and phrases: primitive roots, quadratic residues.
prime primitive root equals
\[ D(p_k, p_l) = \sum_{N \subset \{p_k, \ldots, p_l\}} (-1)^{|N|-1} (d(N, \{p_1, \ldots, p_{k-1}\}) - d(N, \{p_1, \ldots, p_k\})) \]

**Corollary 2.** In the notation of Corollary 1,
\[ D(p_k, p_k) = \frac{\Delta_k}{2^k} (1 + (-1 | p_k) d_{1,p_k}) \prod_{i=2}^{k-1} (1 - (-1 | p_i) d_{1,p_i}) \]
\[ + \frac{\Delta_k}{2^k} (1 + d_{1,p_k}) \prod_{i=2}^{k-1} (1 - d_{1,p_i}) \]

Corollaries 1 and 2 answer questions proposed orally by Dr. A. Paszkiewicz. From a numerical calculation he has obtained heuristic values of \( D(p_k, p_l) \) for small \( k, l \) and communicated them to the author. This is gratefully acknowledged.

**Notation.** We put
\[ \mathcal{A} = \{a_1, \ldots, a_n\}, \quad A = \prod_{i=1}^{n} a_i, \quad A_1 = \prod_{i=1}^{n} a_i, \quad a_i \equiv 1 \pmod{4} \]
\[ \mathcal{B} = \{b_1, \ldots, b_m\}, \quad B = \prod_{j=1}^{m} b_j, \quad B_1 = \prod_{j=1}^{m} b_j, \quad b_j \equiv 1 \pmod{4} \]

\( b_0 = 2, \langle l_1, \ldots, l_n \rangle \) is the l.c.m. of \( l_1, \ldots, l_n \), \( \omega(k) \) is the number of distinct prime factors of \( k \), and \( \pi(x) \) the number of primes \( \leq x \).

**Lemma 1.** Let \( K \) be a number field, and \( \pi(x, K) \) the number of prime ideals of \( K \) with norm \( \leq x \). Then
\[ \pi(x, K) = \text{li} x + O(x e^{-c(K) \sqrt{\log x}}) \]
and under the extended Riemann hypothesis
\[ \pi(x, K) = \text{li} x + O(N(K)x^{1/2} \log(\Delta(K)^{1/N(K)}x)) \]
where \( N(K) \) and \( \Delta(K) \) are the degree and the discriminant of \( K \), respectively.

**Proof.** See Landau [3, Satz 191] and Hooley [1, §5].

**Lemma 2.** Suppose \( \langle l_1, \ldots, l_n \rangle \) divides \( k \) and let \( P(x, l_1, \ldots, l_n, k; \mathcal{A}, \mathcal{B}) \) be the number of primes \( p \leq x, p \equiv 1 \pmod{k}, p \notin \mathcal{A} \cup \mathcal{B} \), such that each of the congruences
\[ x^{l_i} \equiv a_i \pmod{p} \quad (1 \leq i \leq n), \quad x^2 \equiv b_j \pmod{p} \quad (0 \leq j \leq m) \]
is soluble. Then

\[ (4) \quad N(K_1)P(x, l, k; A, B) = \pi(x, K_1) + O(N(K_1)\omega(k)) + O(N(K_1)x^{1/2}) \]

where \( K_1 = \mathbb{Q}(\sqrt[1]{l}, i\sqrt[1]{a_1}, \ldots, i\sqrt[1]{a_n}, \sqrt[1]{b_0}, \ldots, \sqrt[1]{b_m}) \), \( N(K_1) = \langle K_1 : \mathbb{Q} \rangle \).

**Proof.** See \([1\text{, formula (5.7)}]\), where we may suppose that \( k \) is even.

**Lemma 3.** For every positive integer \( k \) the set \( S(k; A, B) \) of primes \( p \equiv 1 \) (mod \( k \)) such that \([1]\) holds and for every prime \( q | k \) at least one of the numbers \( a_i \) is a \( q \)th power residue modulo \( p \) has natural density

\[ (5) \quad c_0(k) = \mu(k) \sum_{l_1|k} \cdots \sum_{l_n|k} \frac{\mu(l_1) \cdots \mu(l_n)}{N(K_1)}. \]

**Proof.** Let \( P(x, k; A, B) \) be the number of primes \( p \in S(k; A, B), p \leq x \). We have (see \([1\text{, Lemma 4.1]}\))

\[ P(x, k; A, B) = \mu(k) \sum_{l_1|k} \cdots \sum_{l_n|k} \frac{\mu(l_1) \cdots \mu(l_n)}{N(K_1)}P(x, l, k; A, B). \]

Using the formulae \([2]\) and \([4]\) we obtain

\[ P(x, k; A, B) = \frac{\mu(k)x}{\log x} \sum_{l_1|k} \cdots \sum_{l_n|k} \frac{\mu(l_1) \cdots \mu(l_n)}{N(K_1)} + O \left( \frac{x}{\log^2 x} \right), \]

which gives the existence of \( c_0(k) \) and formula \([5]\).

**Lemma 4.** The discriminant \( \Delta(K_1) \) of \( K_1 \) satisfies

\[ \Delta(K_1) \leq (k 2^m l_1 \ldots l_n a_1 \ldots a_n b_1 \ldots b_m)^{N(K_1)} \leq k^{cN(K_1)} \]

where \( c \) depends only on \( A \) and \( B \).

**Proof.** See Lemma 7.3 of \([1]\).

**Lemma 5.** We have

\[ \sum_{k>x} c_0(k) \ll x^{-1}(\log x)^{2n-1}. \]

**Proof.** Clearly we have

\[ c_0(k) \leq c(k), \]

where \( c(k) \) is the natural density of the primes \( p \equiv 1 \) (mod \( k \)) such that for each prime \( q | k \) at least one of the numbers \( a_i \) is a \( q \)th power residue modulo \( p \). Now, Lemma \([5]\) follows from \([1\text{, formula (8.9)}\) and Lemma 8.4.]

**Lemma 6.** Let \( R(q, p) \) denote the statement: \((1)\) holds, \( p \nmid A, q \mid p - 1 \) and at least one of the numbers \( a_i \) is a \( q \)th power residue modulo \( p \). Let \( M(x, \eta_1, \eta_2; A, B) \) be the number of primes \( p \leq x \) such that \( R(q, p) \) is true
for at least one prime \( q, \eta_1 < q \leq \eta_2 \). Then under the extended Riemann hypothesis

\[
M\left(x, \frac{1}{6} \log x, x - 1; \mathcal{A}, \mathcal{B}\right) = O\left(\frac{\log \log x}{\log^2 x}\right).
\]

Proof. We have

\[
M\left(x, \frac{1}{6} \log x, x - 1; \mathcal{A}, \mathcal{B}\right) \leq M\left(x, \frac{1}{6} \log x, x - 1; \mathcal{A}, \emptyset\right)
\]
\[
\leq M\left(x, \frac{1}{6} \log x, x^{1/2} \log^{-2} x; \mathcal{A}, \emptyset\right) + M\left(x, x^{1/2} \log^{-2} x, x - 1; \mathcal{A}, \emptyset\right)
\]

and it suffices to apply [4, formulae (3.3) and (8.15)].

Lemma 7. Let \( N(x; \mathcal{A}, \mathcal{B}) \) be the number of primes \( p \leq x \) such that all \( a \in \mathcal{A} \) are primitive roots modulo \( p \) and (1) holds. Then under the assumption of the extended Riemann hypothesis,

\[
N(x; \mathcal{A}, \mathcal{B}) = \frac{x}{\log x} \sum_{k=1}^{\infty} \mu(k) c_0(k) + O\left(\frac{x}{\log^2 x}(\log \log x)^{2n-1}\right).
\]

Proof. \( N(x; \mathcal{A}, \mathcal{B}) \) is the number of primes \( p \leq x, p \nmid A \) such that (1) holds and \( R(q, p) \) is false for all primes \( q \). Let \( N(x, \eta; \mathcal{A}, \mathcal{B}) \) be the number of primes \( p \leq x, p \nmid A \) such that (1) holds and \( R(q, p) \) is false for all primes \( q \leq \eta \). We let \( P(x, k; \mathcal{A}, \mathcal{B}) \) be the number of primes \( p \leq x, p \nmid A \) such that \( R(q, p) \) is true for all \( q | k \).

By the exclusion principle

\[
M\left(x, \frac{1}{6} \log x; \mathcal{A}, \mathcal{B}\right) = \sum_{k=1}^{\infty} \mu(k) P(x, k; \mathcal{A}, \mathcal{B}),
\]

where \( \sum_0 \) is over the squarefree numbers \( k \) composed entirely of primes \( q \leq \frac{1}{6} \log x \). The relevant \( k \) satisfy

\[
k \leq \prod_{q \leq \frac{1}{6} \log x} q \leq e^{\frac{1}{3} \log x} = x^{1/3}.
\]

Now, using formulae (3) and (4) we obtain

\[
P(x, k; \mathcal{A}, \mathcal{B}) = c_0(k) \text{li} x + O(d(k)^n x^{1/2} \log(\Delta(K_1)^{1/N(K_1)} x)),
\]

which, by the formula

\[
\sum_{k \leq x} d(k)^n = O(x(\log x)^{2n-1})
\]

(see [2, Theorem 5.3]), by Lemma 4 and by formulae (6) and (7) gives

\[
N\left(x, \frac{1}{6} \log x; \mathcal{A}, \mathcal{B}\right) = (\text{li} x) \sum_{k=1}^{\infty} \mu(k) c_0(k) + O(x^{5/6}(\log x)^{2n}).
\]
Now, by Lemma 5,
\[
\sum_0 \mu(k)c_0(k) = \sum_{k=1}^{\infty} \mu(k)c_0(k) + O\left( \sum_{k > \frac{1}{6} \log x} c_0(k) \right)
= \sum_{k=1}^{\infty} \mu(k)c_0(k) + O\left( \frac{\left(\log \log x\right)^{2n-1}}{\log x} \right),
\]
and by Lemma 6 and (8),
\[
N(x; \mathcal{A}, \mathcal{B}) = N\left( x, \frac{1}{6} \log x; \mathcal{A}, \mathcal{B} \right) + O\left( M\left( x, \frac{1}{6} \log x, x-1; \mathcal{A}, \mathcal{B} \right) \right)
= \frac{x}{\log x} \sum_{k=1}^{\infty} \mu(k)c_0(k) + O\left( \frac{x(\log \log x)^{2n-1}}{\log^2 x} \right) + O\left( \frac{x \log \log x}{\log^2 x} \right),
\]
Lemma 8. We have
\[
N(K) = 2^{m+1} \varphi(k) \prod_{i=1}^{n} l_i / \sum_{i=1}^{1} 1,
\]
where the sum \( \sum_1 \) is taken over all vectors \( [\nu_1, \ldots, \nu_n, q_0, \ldots, q_m] \) such that \( 1 \leq \nu_i \leq l_i \) \( (1 \leq i \leq n) \), \( 1 \leq q_j \leq 2 \) \( (0 \leq j \leq m) \) and
\[
\prod_{i=1}^{n} a_i^{(k,2)\nu_i l_i} \prod_{j=0}^{m} b_j^{(k,2)\nu_j l_j} = \beta^{(k,2)}, \quad \beta \in \mathbb{Q}(\sqrt{1}).
\]
Proof. This follows from [4, Lemma 9.1] on replacing, for \( k \) odd, \( k \) by \( \langle k, 2 \rangle \).

Lemma 9. For \( a \in \mathbb{Z} \setminus \{0\} \) and \( k \) even squarefree we have \( a = \beta^k \), \( \beta \in \mathbb{Q}(\sqrt{1}) \) if and only if \( a = b^{k/2}, \ b \in \mathbb{Z}, \sqrt{b} \in \mathbb{Q}(\sqrt{1}) \). Moreover, for \( b \) squarefree, \( \sqrt{b} \in \mathbb{Q}(\sqrt{1}) \) if and only if \( b \equiv 1 \pmod{4}, \ b \mid k \).

Proof. See [4, Lemma 10.1].

Lemma 10. For \( k \) squarefree we have
\[
c_0(k) = \frac{\mu(\langle k, 2 \rangle)}{2^{m+1}} \prod_{p \mid k} c_n(p) \sum_{m_1 \mid 2} \sum_{m_n \mid 2} \frac{\mu(m_1) \ldots \mu(m_n)}{m_1 \ldots m_n} D(m_1, \ldots, m_n, k, B),
\]
where
\[
D(m_1, \ldots, m_n, k, B) = \sum_{\mu_1 = 1}^{m_1} \ldots \sum_{\mu_n = 1}^{m_n} \sum_{2}^{1} 1
\]
and $\sum_2$ is over all divisors of $2B$ such that

$$\prod_{i=1}^n a_i^{2\mu_i/m_i} d = \beta^2, \quad \beta \in \mathbb{Q}(\sqrt{1}).$$

**Proof.** By formula (5) and Lemma 8 we have

$$c_0(k) = \frac{\mu(k)}{2^{m+1} \varphi(k)} \sum_{l_1|k} \cdots \sum_{l_n|k} \frac{\mu(l_1) \cdots \mu(l_n)}{l_1 \cdots l_n} \sum_1 1.$$ 

Now, let $l_i = m_i l'_i$, where $m_i | 2$ and $l'_i$ is odd, $(m_1, \ldots, m_n) = (k, 2)$. Since $a_i, b_j$ are distinct primes, $\varphi$ is equivalent by virtue of Lemma 9 to the conditions $\nu_i = l'_i \mu_i$, $1 \leq \mu_i \leq m_i$,

$$\prod_{i=1}^m a_i^{2\mu_i/m_i} \prod_{j=0}^m b_j^{\varphi_j} = \beta^2, \quad \beta \in \mathbb{Q}(\sqrt{1}).$$

The last condition is satisfied by $\varphi_0, \ldots, \varphi_m$ if and only if it is satisfied by $2 - \varphi_0, \ldots, 2 - \varphi_m$, but when $[\varphi_0, \ldots, \varphi_m]$ runs through $\{1, 2\}^{m+1}, \prod_{j=0}^m b_j^{2 - \varphi_j}$ runs through all positive divisors of $2B$. Thus

$$c_0(k) = \frac{\mu(k)}{2^{m+1} \varphi(k)} \sum_{l_1'|k/(k,2)} \cdots \sum_{l_n'|k/(k,2)} \sum_{m_1|2} \cdots \sum_{m_n|2} \frac{\mu(l'_1) \mu(m_1) \cdots \mu(l'_n) \mu(m_n)}{l_1' \cdots l_n' m_1 \cdots m_n} \sum_{\mu_1=1}^m \cdots \sum_{\mu_n=1}^m \sum_{2} 1.$$

Now, however,

$$S_1(k) = \sum_{l_1'|k/(k,2)} \cdots \sum_{l_n'|k/(k,2)} \frac{\mu(l'_1) \cdots \mu(l'_n)}{l_1' \cdots l_n'}$$

is independent of $m_1, \ldots, m_n$. Moreover, by Lemma 10.4 of [4] the function $S_1(k)$ is multiplicative. If $p$ is a prime we have

$$S_1(p) = \sum_{l_1'|p} \cdots \sum_{l_n'|p} \frac{\mu(l'_1) \cdots \mu(l'_n)}{l_1' \cdots l_n'} = \left( \sum_{l|p} \frac{\mu(l)}{l} \right)^n - 1$$

$$= \left( 1 - \frac{1}{p} \right)^n - 1 = -(p-1)c_n(p),$$
thus by (11),
\[ c_0(k) = \frac{\mu((k, 2))}{2^{m+1}} \prod_{p | k} c_n(p) \sum_{m_1 | 2} \sum_{m_n | 2} \mu(m_1) \ldots \mu(m_n) D(m_1, \ldots, m_n, k, B). \]

**Lemma 11.** Let \( F \) be a field and \( d \) a non-zero integer. For \( 1 \leq i_1 < \ldots < i_j \leq n \) let
\[ \tau(i_1, \ldots, i_j; d) = \sum_{\nu_1 = 1}^{2} \ldots \sum_{\nu_j = 1}^{2} 1. \]
Also let
\[ \sigma_j(d) = \sum_{1 \leq i_1 < \ldots < i_j \leq n} \tau(i_1, \ldots, i_j; d), \quad \sigma_0(d) = \begin{cases} 1 & \text{if } d = \beta^2, \beta \in F, \\ 0 & \text{otherwise}. \end{cases} \]
Then if \( \tau^*(i_1, \ldots, i_j; d) \) and \( \sigma_j^*(d) \) are defined similarly, but with all \( \nu_i \) equal to 1, we have
\[ \sum_{j=0}^{n} (-1)^j 2^{n-j} \sigma_j(d) = \sum_{j=0}^{n} (-1)^j \sigma_j^*(d). \]

**Proof.** For \( d = \beta^2, \beta \in F \) the lemma is contained in [4, Lemma 10.7], where one takes \( p = 2 \). If \( d \neq \beta^2, \beta \in F \), then a similar argument applies, only 1 disappears in the formula for \( \tau(i_1, \ldots, i_j) \) and \( \binom{n}{j} \) disappears in the formula for \( \sigma_j \). Since, however, \( \sigma_0^* = 0 \) we obtain, in analogy with (10.14) of [4],
\[ \sigma_j^*(d) = \binom{n}{j} \sigma_0^*(d) + \sum_{r=1}^{j} \binom{n-r}{j-r} \sigma_r^*(d) = \binom{n}{j} \sigma_0^*(d) + \sum_{r=1}^{n} \binom{n-r}{j-r} \sigma_r^*(d) \]
and the final argument is the same as in [4].

**Lemma 12.** For every squarefree \( k \) we have
\[ S_2(k) = \sum_{m_1 | 2} \ldots \sum_{m_n | 2} \mu(m_1) \ldots \mu(m_n) D(m_1, \ldots, m_n, k, B) = 2^{-n} \sum_{\delta} \mu(\delta) \]
where the sum \( \sum_{\delta} \) is taken over all pairs \( \delta, d \) such that \( \delta | A, d | B, \delta d \equiv 1 \pmod{4} \) and \( d \delta | k \).
Proof. By Lemma 11 we have, in the notation of that lemma,

\[ S_2(k) = \sum_{j=0}^{n} (-1)^j 2^{-j} \sum_{d | 2B} \sigma_j(d) = 2^{-n} \sum_{j=0}^{n} \sum_{d | 2B} (-1)^j \sigma_j^*(d) = 2^{-n} \sum_{\delta | A} \mu(\delta) \sum_{d \mid 2B} \sigma_j(d), \]

where the sum \( \sum_{d \mid 2B} \) is taken over all \( d \mid 2B \) such that \( d\delta = \beta^2, \beta \in \mathbb{Q}(\sqrt[4]{1}) \). By Lemma 9 the last condition is equivalent to \( \delta d \equiv 1 \pmod{4}, \delta d \mid k \). Hence

\[ S_2(k) = 2^{-n} \sum_{\delta \mid 3} \mu(\delta). \]

Proof of the Theorem. By Lemmas 10 and 12 we have, for every square-free odd \( k \),

\[
(12) \quad c_0(k) - c_0(2k) = 2^{-m-1} \prod_{\substack{p \mid k \\quad \text{p} > 2 \quad \text{p} \mid k}} c_n(p) \sum_{m_1 \mid 2} \cdots \sum_{m_n \mid 2} \frac{\mu(m_1) \cdots \mu(m_n)}{m_1 \cdots m_n} D(m_1, \ldots, m_n, k, B)
\]

\[ = 2^{-m-n-1} \prod_{\substack{p \mid k \\quad \text{p} > 2 \quad \text{p} \mid k}} c_n(p) \sum_{\delta \mid 3} \mu(\delta). \]

Now, we have

\[
(13) \quad S_3 = \sum_{k=1}^{\infty} \mu(k) c_0(k) = S_4 + S_5,
\]

where

\[ S_i = \sum_{k=1}^{\infty} \mu(k) (c_0(k) - c_0(2k)) \quad (i = 4, 5) \]

and \( S_4, S_5 \) are taken over all squarefree odd \( k \) such that \( (k, B) \mid B_1 \) and \( (k, B) \nmid B_1 \), respectively. Now, by (12),

\[ S_4 = 2^{-m-n-1} \sum_{\delta \mid 4} \mu(k) \prod_{\substack{p \mid k \\quad \text{p} > 2 \quad \text{p} \mid k}} c_n(p) \sum_{\delta \mid 3} \mu(\delta) \]

\[ = 2^{-m-n-1} \sum_{\delta \mid 4} \mu(k) \prod_{\substack{p \mid k \\quad \text{p} > 2 \quad \text{p} \mid k}} c_n(p) 2^{\omega((k, B))} \sum_{\delta \mid (A, k) \\quad \delta \equiv 1 \pmod{4}} \mu(\delta) \]

and

\[ \sum_{\delta \mid (A, k) \\quad \delta \equiv 1 \pmod{4}} \mu(\delta) = \begin{cases} 1 & \text{if } (A, k) = 1, \\ 2^{\omega((k, A))} - 1 & \text{if } (A, k) \neq 1, (A_1, k) = 1, \\ 0 & \text{otherwise}. \end{cases} \]

Hence
\[ S_4 = 2^{-m-n-1} \sum_6 \mu(k)2^{\omega((k,B))} \prod_{p|k, p>2} c_n(p) \]
\[ + 2^{-m-n-2} \sum_7 \mu(k)2^{\omega((k,B)) + \omega((k,A))} \prod_{p|k, p>2} c_n(p) \]

where \( \sum_6 \) and \( \sum_7 \) are taken over all squarefree odd \( k \) with \( (k, B)|B_1 \) such that \( (A, k) = 1 \) and \( (A, k) \neq 1 \), \( (A_1, k) = 1 \), respectively. Since the functions under the summation sign are multiplicative we obtain

\[ S_4 = 2^{-m-n-1} \prod_{p|B_1} (1 - 2c_n(p)) \prod_{p|AB, p>2} (1 - c_n(p)) \]
\[ + 2^{-m-n-2} \prod_{p|B_1} (1 - 2c_n(p)) \prod_{p|A_1, p>2} (1 - 2c_n(p)) \prod_{p|AB, p>2} (1 - c_n(p)) \]
\[ - 2^{-m-n-2} \prod_{p|B_1} (1 - 2c_n(p)) \prod_{p|AB, p>2} (1 - c_n(p)) \]
\[ = 2^{-m-2} \Delta_n \prod_{p|B} (1 - (-1 | p)d_{n,p}) \prod_{p|A} (1 + d_{n,p}) \]
\[ + 2^{-m-2} \Delta_n \prod_{p|B} (1 - (-1 | p)d_{n,p}) \prod_{p|A} (1 + (-1 | p)d_{n,p}). \]

Similarly, by (12),

\[ S_5 = 2^{-m-n-1} \sum_5 \mu(k) \prod_{p|k, p>2} c_n(p) \sum_3 \mu(\delta) \]
\[ = 2^{-m-n-1} \sum_5 \mu(k)2^{\omega((k,B)) - 1} \prod_{p|k, p>2} c_n(p) \cdot \left\{ 1 \text{ if } (k, A) = 1, \right. \]
\[ \left. 0 \text{ otherwise,} \right\} \]

hence

\[ S_5 = 2^{-m-n-2} \prod_{p|B} (1 - 2c(p)) \prod_{p|AB} (1 - c(p)) \]
\[ - 2^{-m-n-2} \prod_{p|B_1} (1 - 2c(p)) \prod_{p|AB} (1 - c(p)) \]
\[ = 2^{-m-2} \Delta_n \prod_{p|B} (1 - d_{n,p}) \prod_{p|A} (1 + d_{n,p}) \]
\[ - 2^{-m-2} \Delta_n \prod_{p|B} (1 - (-1 | p)d_{n,p}) \prod_{p|A} (1 + d_{n,p}). \]

The Theorem follows on combining (13)–(15) and Lemma 7.
Proof of Corollary 1. Let $P_k$ be the set of primes for which $p_k$ is the least quadratic non-residue, and let for a given $g$, and $p \in P_k$,

$$\chi_g(p) = \begin{cases} 1 & \text{if } g \text{ is a primitive root modulo } p, \\ 0 & \text{otherwise.} \end{cases}$$

We have

$$D(p_k, p_l) = \lim_{x \to \infty} \pi(x)^{-1} \sum_{p \in P_k} \chi_{p_k}(p) \prod_{g=p_k}^{p_l-1} (1 - \chi_g(p))$$

$$= \lim_{x \to \infty} \pi(x)^{-1} \sum_{N \subseteq \{p_k, \ldots, p_l\}, p_l \in N} (-1)^{|N|-1} \sum_{p \in P_k, g \in N} \chi_g(p)$$

$$= \sum_{N \subseteq \{p_k, \ldots, p_l\}, p_l \in N} (-1)^{|N|-1} \lim_{x \to \infty} \pi(x)^{-1} \sum_{p \in P_k, g \in N} \chi_g(p)$$

$$= \sum_{N \subseteq \{p_k, \ldots, p_l\}, p_l \in N} (-1)^{|N|-1} (d(N, \{p_1, \ldots, p_{k-1}\}) - d(N, \{p_1, \ldots, p_k\})).$$

Proof of Corollary 2. For $k = l$ we have only one term in the sum occurring in Corollary 1 corresponding to $N = \{p_k\}$. Since $p_k$ cannot be simultaneously modulo $p > 2$ a primitive root and a quadratic residue we have

$$d(N, \{p_1, \ldots, p_k\}) = 0$$

and Corollary 1 gives

$$D(p_k, p_k) = d(\{p_k\}, \{p_1, \ldots, p_{k-1}\}).$$

Now Corollary 2 follows from the Theorem.

References


A. Schinzel
Institute of Mathematics
Polish Academy of Sciences
Sniadeckich 8
00-956 Warszawa, Poland
E-mail: schinzel@impan.pl

Received on 11.5.2010
and in revised form on 31.12.2010