ACTA ARITHMETICA
149.2 (2011)

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*

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

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

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

Corollary 1. *Let p_i be the ith 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_l is the least*

2010 *Mathematics Subject Classification*: Primary 11N99.
Key words and phrases: primitive roots, quadratic residues.

DOI: 10.4064/aa149-2-5

prime primitive root equals

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

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

$$\mathcal{A}=\{a_1,\ldots,a_n\},\quad A=\prod_{i=1}^{n}a_i,\quad A_1=\prod_{\substack{i=1\\ a_i\equiv1\ (\mathrm{mod}\ 4)}}^{n}a_i,$$

$$\mathcal{B}=\{b_1,\ldots,b_m\},\quad B=\prod_{j=1}^{m}b_j,\quad B_1=\prod_{\substack{j=1\\ b_j\equiv1\ (\mathrm{mod}\ 4)}}^{m}b_j,$$

$b_0=2$, $\langle l_1,\ldots,l_n\rangle$ 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 $\le x$.

Lemma 1. *Let K be a number field, and $\pi(x,K)$ the number of prime ideals of K with norm $\le x$. Then*

$$\pi(x,K)=\mathrm{li}\,x+O(xe^{-c(K)\sqrt{\log x}})\tag{2}$$

and under the extended Riemann hypothesis

$$\pi(x,K)=\mathrm{li}\,x+O(N(K)x^{1/2}\log(\Delta(K)^{1/N(K)}x))\tag{3}$$

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 $p\le x$, $p\equiv1\pmod{k}$, $p\notin\mathcal{A}\cup\mathcal{B}$, such that each of the congruences*

$$x^{l_i}\equiv a_i\ (\mathrm{mod}\ p)\ (1\le i\le n),\qquad x^2\equiv b_j\ (\mathrm{mod}\ p)\ (0\le j\le m)$$

is soluble. Then

$$N(K_{\boldsymbol{l}})P(x,\boldsymbol{l},k;\mathcal{A},\mathcal{B}) = \pi(x,K_{\boldsymbol{l}}) + O(N(K_{\boldsymbol{l}})\omega(k)) + O(N(K_{\boldsymbol{l}})x^{1/2}) \tag{4}$$

where $K_{\boldsymbol{l}} = \mathbb{Q}(\sqrt[k]{1}, \sqrt[l_1]{a_1}, \ldots, \sqrt[l_n]{a_n}, \sqrt{b_0}, \ldots, \sqrt{b_m})$, $N(K_{\boldsymbol{l}}) = [K_{\boldsymbol{l}} : \mathbb{Q}]$.

Proof. See [4, formula (5.7)], where we may suppose that k is even.

LEMMA 3. *For every positive integer k the set $S(k;\mathcal{A},\mathcal{B})$ of primes $p \equiv 1$* (mod k) *such that* (1) *holds and for every prime $q \mid k$ at least one of the numbers a_i is a qth power residue modulo p has natural density*

$$c_0(k) = \mu(k) \sum_{l_1|k} \ldots \sum_{\substack{l_n|k \\ \langle l_1,\ldots,l_n\rangle = k}} \frac{\mu(l_1)\ldots\mu(l_n)}{N(K_{\boldsymbol{l}})}. \tag{5}$$

Proof. Let $P(x,k;\mathcal{A},\mathcal{B})$ be the number of primes $p \in S(k;\mathcal{A},\mathcal{B})$, $p \le x$. We have (see [4, Lemma 4.1])

$$P(x,k;\mathcal{A},\mathcal{B}) = \mu(k) \sum_{l_1|k} \ldots \sum_{\substack{l_n|k \\ \langle l_1,\ldots,l_n\rangle = k}} \mu(l_1)\ldots\mu(l_n)P(x,\boldsymbol{l},k;\mathcal{A},\mathcal{B}).$$

Using the formulae (2) and (4) we obtain

$$P(x,k;\mathcal{A},\mathcal{B}) = \frac{\mu(k)x}{\log x} \sum_{l_1|k} \ldots \sum_{\substack{l_n|k \\ \langle l_1,\ldots,l_n\rangle = k}} \frac{\mu(l_1)\ldots\mu(l_n)}{N(K_{\boldsymbol{l}})} + O\Big(\frac{x}{\log^2 x}\Big),$$

which gives the existence of $c_0(k)$ and formula (5).

LEMMA 4. *The discriminant $\Delta(K_{\boldsymbol{l}})$ of $K_{\boldsymbol{l}}$ satisfies*

$$\Delta(K_{\boldsymbol{l}}) \le (k\, 2^m\, l_1 \ldots l_n\, a_1 \ldots a_n\, b_1 \ldots b_m)^{N(K_{\boldsymbol{l}})} \le k^{cN(K_{\boldsymbol{l}})}$$

where c depends only on $\mathcal{A}$ and $\mathcal{B}$.

Proof. See Lemma 7.3 of [4].

LEMMA 5. *We have*

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

Proof. Clearly we have

$$c_0(k) \le c(k),$$

where $c(k)$ is the natural density of the primes $p \equiv 1$ (mod k) such that for each prime $q \mid k$ at least one of the numbers a_i is a qth power residue modulo p. Now, Lemma 5 follows from [4, 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 qth power residue modulo p. Let $M(x,\eta_1,\eta_2;\mathcal{A},\mathcal{B})$ be the number of primes $p \le x$ such that $R(q,p)$ is true* *for at least one prime q, $\eta_1 < q \le \eta_2$. Then under the extended Riemann hypothesis*

$$M\Big(x, \frac{1}{6}\log x, x-1; \mathcal{A}, \mathcal{B}\Big) = O\Big(\frac{\log\log x}{\log^2 x}\Big).$$

Proof. We have

$$\begin{aligned} &M\Big(x, \frac{1}{6}\log x, x-1; \mathcal{A}, \mathcal{B}\Big) \le M\Big(x, \frac{1}{6}\log x, x-1; \mathcal{A}, \emptyset\Big) \\ &\le M\Big(x, \frac{1}{6}\log x, x^{1/2}\log^{-2} x; \mathcal{A}, \emptyset\Big) + M(x, x^{1/2}\log^{-2} x, x-1; \mathcal{A}, \emptyset) \end{aligned}$$

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 $p \le x$ such that all $a \in \mathcal{A}$ are primitive roots modulo p and* (1) *holds. Then under the assumption of the extended Riemann hypothesis,*

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

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

By the exclusion principle

$$M\Big(x, \frac{1}{6}\log x; \mathcal{A}, \mathcal{B}\Big) = \sum\nolimits_0 \mu(k)P(x, k; \mathcal{A}, \mathcal{B}), \tag{6}$$

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

$$k \le \prod_{q \le \frac{1}{6}\log x} q \le e^{\frac{1}{3}\log x} = x^{1/3}. \tag{7}$$

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

$$P(x, k; \mathcal{A}, \mathcal{B}) = c_0(k)\,\mathrm{li}\,x + O(d(k)^n x^{1/2}\log(\varDelta(K_{\boldsymbol{l}})^{1/N(K_{\boldsymbol{l}})}x)),$$

which, by the formula

$$\sum_{k \le x} d(k)^n = O(x(\log x)^{2^n-1})$$

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

$$N\Big(x, \frac{1}{6}\log x; \mathcal{A}, \mathcal{B}\Big) = (\mathrm{li}\,x)\sum\nolimits_0 \mu(k)c_0(k) + O(x^{5/6}(\log x)^{2^n}). \tag{8}$$

Now, by Lemma 5,

$$\sum\nolimits_0 \mu(k)c_0(k) = \sum_{k=1}^{\infty} \mu(k)c_0(k) + O\Big(\sum_{k>\frac{1}{6}\log x} c_0(k)\Big)$$
$$= \sum_{k=1}^{\infty} \mu(k)c_0(k) + O\Big(\frac{(\log\log x)^{2^n-1}}{\log x}\Big),$$

and by Lemma 6 and (8),

$$N(x;\mathcal{A},\mathcal{B}) = N\Big(x, \frac{1}{6}\log x; \mathcal{A},\mathcal{B}\Big) + O\Big(M\Big(x, \frac{1}{6}\log x, x-1; \mathcal{A},\mathcal{B}\Big)\Big)$$
$$= \frac{x}{\log x}\sum_{k=1}^{\infty} \mu(k)c_0(k) + O\Big(\frac{x(\log\log x)^{2^n-1}}{\log^2 x}\Big) + O\Big(\frac{x\log\log x}{\log^2 x}\Big)$$
$$= \frac{x}{\log x}\sum_{k=1}^{\infty} \mu(k)c_0(k) + O\Big(\frac{x}{\log^2 x}(\log\log x)^{2^n-1}\Big).$$

LEMMA 8. *We have*

$$N(K_{\boldsymbol{l}}) = 2^{m+1}\varphi(k)\prod_{i=1}^{n} l_i \Big/ \sum\nolimits_1 1,$$

where the sum $\sum_1$ *is taken over all vectors* $[\nu_1,\ldots,\nu_n,\varrho_0,\ldots,\varrho_m]$ *such that* $1 \le \nu_i \le l_i$ $(1 \le i \le n)$, $1 \le \varrho_j \le 2$ $(0 \le j \le m)$ *and*

$$\prod_{i=1}^{n} a_i^{\langle k,2\rangle \nu_i/l_i} \prod_{j=0}^{m} b_j^{\langle k,2\rangle \varrho_j/2} = \beta^{\langle k,2\rangle}, \qquad \beta \in \mathbb{Q}(\sqrt[k]{1}). \tag{9}$$

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* $a = \beta^k$, $\beta \in \mathbb{Q}(\sqrt[k]{1})$ *if and only if* $a = b^{k/2}$, $b \in \mathbb{Z}$, $\sqrt{b} \in \mathbb{Q}(\sqrt[k]{1})$. *Moreover, for* b *squarefree,* $\sqrt{b} \in \mathbb{Q}(\sqrt[k]{1})$ *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*

$$c_0(k) = \frac{\mu((k,2))}{2^{m+1}} \prod_{\substack{p\mid k\\ p>2}} c_n(p) \sum_{\substack{m_1\mid 2 \\ \langle m_1,\ldots,m_n\rangle=(k,2)}} \cdots \sum_{m_n\mid 2} \frac{\mu(m_1)\ldots\mu(m_n)}{m_1\ldots m_n} D(m_1,\ldots,m_n,k,B),$$

where

$$D(m_1,\ldots,m_n,k,B) = \sum_{\mu_1=1}^{m_1} \cdots \sum_{\mu_n=1}^{m_n} \sum\nolimits_2 1 \tag{10}$$

and $\sum_2$ *is over all divisors of* $2B$ *such that*

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

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

$$c_0(k) = \frac{\mu(k)}{2^{m+1}\varphi(k)} \sum_{\substack{l_1|k \\ \langle l_1,\ldots,l_n\rangle = k}} \ldots \sum_{l_n|k} \frac{\mu(l_1)\ldots\mu(l_n)}{l_1\ldots l_n} \sum\nolimits_1 1.$$

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

$$\prod_{i=1}^{m} a_i^{2\mu_i/m_i} \prod_{j=0}^{m} b_j^{\varrho_j} = \beta^2, \qquad \beta \in \mathbb{Q}(\sqrt[k]{1}).$$

The last condition is satisfied by $\varrho_0,\ldots,\varrho_m$ if and only if it is satisfied by $2-\varrho_0,\ldots,2-\varrho_m$, but when $[\varrho_0,\ldots,\varrho_m]$ runs through $\{1,2\}^{m+1}$, $\prod_{j=0}^{m} b_j^{2-\varrho_j}$ runs through all positive divisors of $2B$. Thus

$$(11) \qquad c_0(k) = \frac{\mu(k)}{2^{m+1}\varphi(k)} \sum_{\substack{l_1'|k/(k,2) \\ \langle l_1',\ldots,l_n'\rangle = k/(k,2)}} \cdots \sum_{l_n'|k/(k,2)} \sum_{\substack{m_1|2 \\ \langle m_1,\ldots,m_n\rangle = (k,2)}} \cdots \sum_{m_n|2} \frac{\mu(l_1')\mu(m_1)\ldots\mu(l_n')\mu(m_n)}{l_1'\ldots l_n' m_1\ldots m_n} \sum_{\mu_1=1}^{m_1} \cdots \sum_{\mu_n=1}^{m_n} \sum\nolimits_2 1.$$

Now, however,

$$S_1(k) = \sum_{\substack{l_1'|k/(k,2) \\ \langle l_1',\ldots,l_n'\rangle = k/(k,2)}} \cdots \sum_{l_n'|k/(k,2)} \frac{\mu(l_1')\ldots\mu(l_n')}{l_1'\ldots l_n'}$$

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

$$S_1(p) = \sum_{\substack{l_1'|p \\ \langle l_1',\ldots,l_n'\rangle = p}} \ldots \sum_{l_n'|p} \frac{\mu(l_1')\ldots\mu(l_n')}{l_1'\ldots l_n'} = \Big(\sum_{l|p} \frac{\mu(l)}{l}\Big)^n - 1$$
$$= \Big(1 - \frac{1}{p}\Big)^n - 1 = -(p-1)c_n(p),$$

thus by (11),

$$c_0(k)=\frac{\mu((k,2))}{2^{m+1}}\prod_{\substack{p\mid k\\ p>2}}c_n(p)\sum_{\substack{m_1\mid 2\\ \langle m_1,\ldots,m_n\rangle=(k,2)}}\ldots\sum_{m_n\mid 2}\frac{\mu(m_1)\ldots\mu(m_n)}{m_1\ldots m_n}D(m_1,\ldots,m_n,k,B).$$

Lemma 11. *Let F be a field and d a non-zero integer. For $1\le i_1<\ldots<i_j\le n$ let*

$$\tau(i_1,\ldots,i_j;d)=\sum_{\substack{\nu_{i_1}=1\\ a_{i_1}^{\nu_{i_1}}\ldots a_{i_j}^{\nu_{i_j}}d=\beta^2,\,\beta\in F}}^{2}\ldots\sum_{\nu_{i_j}=1}^{2}1.$$

Also let

$$\sigma_j(d)=\sum_{1\le i_1<\cdots<i_j\le n}\tau(i_1,\ldots,i_j;d),\qquad \sigma_0(d)=\begin{cases}1 & \text{if } d=\beta^2,\ \beta\in F,\\ 0 & \text{otherwise.}\end{cases}$$

Then if $\tau^*(i_1,\ldots,i_j;d)$ and $\sigma_j^*(d)$ are defined similarly, but with all ν_i equal to 1, we have

$$\sum_{j=0}^{n}(-1)^j2^{n-j}\sigma_j(d)=\sum_{j=0}^{n}(-1)^j\sigma_j^*(d).$$

Proof. For $d=\beta^2$, $\beta\in F$ the lemma is contained in [4, Lemma 10.7], where one takes $p=2$. If $d\ne\beta^2$, $\beta\in F$, 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 σ_j. Since, however, $\sigma_0^*=0$ we obtain, in analogy with (10.14) of [4],

$$\sigma_j^*(d)=\binom{n}{j}\sigma_0^*(d)+\sum_{r=1}^{j}\binom{n-r}{j-r}\sigma_r^*(d)=\binom{n}{j}\sigma_0^*(d)+\sum_{r=1}^{n}\binom{n-r}{j-r}\sigma_r^*(d)$$
$$=\sum_{r=0}^{n}\binom{n-r}{j-r}\sigma_r^*(d)$$

and the final argument is the same as in [4].

Lemma 12. *For every squarefree k we have*

$$S_2(k)=\sum_{m_1\mid 2}\ldots\sum_{m_n\mid 2}\frac{\mu(m_1)\ldots\mu(m_n)}{m_1\ldots m_n}D(m_1,\ldots,m_n,k,B)=2^{-n}\sum\nolimits_3\mu(\delta)$$

where the sum $\sum_3$ is taken over all pairs δ,d such that $\delta\mid A$, $d\mid B$, $\delta d\equiv 1 \pmod 4$ and $d\delta\mid k$.

Proof. By Lemma 11 we have, in the notation of that lemma,

$$S_2(k)=\sum_{j=0}^{n}(-1)^j 2^{-j}\sum_{d\mid 2B}\sigma_j(d)=2^{-n}\sum_{j=0}^{n}\sum_{d\mid 2B}(-1)^j\sigma_j^*(d)=2^{-n}\sum_{\delta\mid A}\mu(\delta)\sum\nolimits_4 1,$$

where the sum $\sum_4$ is taken over all $d\mid 2B$ such that $d\delta=\beta^2$, $\beta\in\mathbb{Q}(\sqrt[k]{1})$. By Lemma 9 the last condition is equivalent to $\delta d\equiv 1 \pmod 4$, $\delta d\mid k$. Hence

$$S_2(k)=2^{-n}\sum\nolimits_3 \mu(\delta).$$

Proof of the Theorem. By Lemmas 10 and 12 we have, for every squarefree odd k,

$$\begin{aligned}(12)\qquad & c_0(k)-c_0(2k)\\ &=2^{-m-1}\prod_{\substack{p\mid k\\ p>2}}c_n(p)\sum_{m_1\mid 2}\dots\sum_{m_n\mid 2}\frac{\mu(m_1)\dots\mu(m_n)}{m_1\dots m_n}D(m_1,\dots,m_n,k,B)\\ &=2^{-m-n-1}\prod_{\substack{p\mid k\\ p>2}}c_n(p)\sum\nolimits_3 \mu(\delta).\end{aligned}$$

Now, we have

$$S_3=\sum_{k=1}^{\infty}\mu(k)c_0(k)=S_4+S_5, \tag{13}$$

where

$$S_i=\sum\nolimits_i \mu(k)(c_0(k)-c_0(2k))\qquad (i=4,5)$$

and $\sum_4,\sum_5$ are taken over all squarefree odd k such that $(k,B)\mid B_1$ and $(k,B)\nmid B_1$, respectively. Now, by (12),

$$\begin{aligned}S_4&=2^{-m-n-1}\sum\nolimits_4 \mu(k)\prod_{\substack{p\mid k\\ p>2}}c_n(p)\sum\nolimits_3\mu(\delta)\\ &=2^{-m-n-1}\sum\nolimits_4 \mu(k)\prod_{\substack{p\mid k\\ p>2}}c_n(p)2^{\omega((k,B))}\sum_{\substack{\delta\mid (A,k)\\ \delta\equiv 1 \,(\mathrm{mod}\, 4)}}\mu(\delta)\end{aligned}$$

and

$$\sum_{\substack{\delta\mid (A,k)\\ \delta\equiv 1 \,(\mathrm{mod}\, 4)}}\mu(\delta)=\begin{cases}1 & \text{if } (A,k)=1,\\ 2^{\omega((k,A))-1} & \text{if } (A,k)\neq 1,\ (A_1,k)=1,\\ 0 & \text{otherwise.}\end{cases}$$

Hence

$$S_4 = 2^{-m-n-1} \sum\nolimits_6 \mu(k) 2^{\omega((k,B))} \prod_{\substack{p \mid k \\ p>2}} c_n(p)$$
$$+ 2^{-m-n-2} \sum\nolimits_7 \mu(k) 2^{\omega((k,B))+\omega((k,A))} \prod_{\substack{p \mid k \\ p>2}} c_n(p)$$

where $\sum_6$ and $\sum_7$ are taken over all squarefree odd k with $(k, B) \mid B_1$ 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

$$S_4 = 2^{-m-n-1} \prod_{p \mid B_1} (1 - 2c_n(p)) \prod_{\substack{p \nmid AB \\ p>2}} (1 - c_n(p)) \tag{14}$$
$$+ 2^{-m-n-2} \prod_{p \mid B_1} (1 - 2c_n(p)) \prod_{p \mid A_1} (1 - 2c_n(p)) \prod_{\substack{p \nmid AB \\ p>2}} (1 - c_n(p))$$
$$- 2^{-m-n-2} \prod_{p \mid B_1} (1 - 2c_n(p)) \prod_{\substack{p \nmid AB \\ p>2}} (1 - c_n(p))$$
$$= 2^{-m-2} \Delta_n \prod_{p \mid B} (1 - (-1 \mid p) d_{n,p}) \prod_{p \mid A} (1 + d_{n,p})$$
$$+ 2^{-m-2} \Delta_n \prod_{p \mid B} (1 - (-1 \mid p) d_{n,p}) \prod_{p \mid A} (1 + (-1 \mid p) d_{n,p}).$$

Similarly, by (12),

$$S_5 = 2^{-m-n-1} \sum\nolimits_5 \mu(k) \prod_{\substack{p \mid k \\ p>2}} c_n(p) \sum\nolimits_3 \mu(\delta)$$
$$= 2^{-m-n-1} \sum\nolimits_5 \mu(k) 2^{\omega((k,B))-1} \prod_{\substack{p \mid k \\ p>2}} c_n(p) \cdot \begin{cases} 1 & \text{if } (k, A) = 1, \\ 0 & \text{otherwise,} \end{cases}$$

hence

$$S_5 = 2^{-m-n-2} \prod_{p \mid B} (1 - 2c(p)) \prod_{p \nmid AB} (1 - c(p)) \tag{15}$$
$$- 2^{-m-n-2} \prod_{p \mid B_1} (1 - 2c(p)) \prod_{p \nmid AB} (1 - c(p))$$
$$= 2^{-m-2} \Delta_n \prod_{p \mid B} (1 - d_{n,p}) \prod_{p \mid A} (1 + d_{n,p})$$
$$- 2^{-m-2} \Delta_n \prod_{p \mid B} (1 - (-1 \mid p) d_{n,p}) \prod_{p \mid A} (1 + d_{n,p}).$$

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

$$\begin{aligned} D(p_k, p_l) &= \lim_{x\to\infty} \pi(x)^{-1} \sum_{p\in P_k} \chi_{p_l}(p) \prod_{g=p_k}^{p_{l-1}} (1-\chi_g(p)) \\ &= \lim_{x\to\infty} \pi(x)^{-1} \sum_{\substack{N\subset\{p_k,\dots,p_l\} \\ p_l\in N}} (-1)^{|N|-1} \sum_{p\in P_k} \prod_{g\in N} \chi_g(p) \\ &= \sum_{\substack{N\subset\{p_k,\dots,p_l\} \\ p_l\in N}} (-1)^{|N|-1} \lim_{x\to\infty} \pi(x)^{-1} \sum_{p\in P_k} \prod_{g\in N} \chi_g(p) \\ &= \sum_{\substack{N\subset\{p_k,\dots,p_l\} \\ p_l\in N}} (-1)^{|N|-1} \big(d(N, \{p_1,\dots,p_{k-1}\}) - d(N, \{p_1,\dots,p_k\})\big). \end{aligned}$$

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

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

and Corollary 1 gives

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

Now Corollary 2 follows from the Theorem.

References

[1] C. Hooley, *On Artin's conjecture*, J. Reine Angew. Math. 225 (1967), 209–220.
[2] L. K. Hua, *Introduction to Number Theory*, Springer, 1982.
[3] E. Landau, *Einführung in die elementare und analytische Theorie der algebraischen Zahlen und Ideale*, B. G. Teubner, 1918.
[4] K. R. Matthews, *A generalization of Artin's conjecture*, Acta Arith. 29 (1976), 113–146.

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

Received on 11.5.2010
and in revised form on 31.12.2010 (6379)