„Опасными" с точки зрения оценки величины типа (6.2) в случае $k = 3$ являются кубические характеры $\chi_1(a_1)$. Но L-ряды с кубическими характерами не имеют зигелевских нулей. Поэтому в случае $k = 3$ достаточно теоремы Линника–Галлахера [1] без эффекта Линника–Дейринга–Хейльбронна [3], [4].

Все эти замечания характерны для любого нечетного k.

Уравнение (0.7) отличается от уравнения (0.5) с точки зрения кругового метода, тем, что на малых дугах надо использовать оценки тригонометрических сумм И. М. Виноградова для полиномов от простых чисел.

К этому же кругу идей относятся уравнения

$$n = p_1^2+p_2^2+p_3^2 \quad \text{и} \quad n = p_1^2+p_2^2+p_3^2+p_4^2$$

потому что два простых квадрата ведут себя как одно простое число с точки зрения метода большого решета.

Литература

[1] P. X. Gallagher, *A large sieve density estimate near* $\sigma = 1$, Invent. Math. 11 (1970), pp. 320–339.

[2] G. H. Hardy and J. E. Littlewood, *Some problems of 'Partitio Numerorum' (V) A further contribution to the study of Goldbach's problem*, Proc. London Math. Soc. (2) 22 (1924), pp. 46–56.

[3] M. Jutila, *On Linnik's constant*, Math. Scand. 41 (1977), pp. 45–62.

[4] Yu. V. Linnik, *On the least prime in an arithmetic progression, I, II*, Mat. Sb. (N. S.) 15 (1944), pp. 139–178, 347–367.

[5] H. L. Montgomery and R. C. Vaughan, *The exceptional set in Goldbach's problem*, Acta Arith. 27 (1975), pp. 353–370.

[6] H. L. Montgomery, *Topics in Multiplicative Number Theory*, Lecture Notes in Mathematics 227, Springer-Verlag, Berlin 1971.

[7] L. A. Takhtajan and A. I. Vinogradov, *The Gauss–Hasse hypothesis on real quadratic fields with class number one*, J. Reine Angew. Math. 335 (1982), pp. 40–87.

[8] А. И. Виноградов, *Об одной почти бинарной задаче*, Изв. АН СССР, серия матем., 20(1956), стр. 713–750.

[9] — *О числе классов идеалов и группе классов дивизоров*, Изв. АН СССР, серия матем., 27(3)(1963), стр. 561–576.

[10] Ю. В. Линник, *Некоторые условные теоремы, касающиеся бинарной проблемы Гольдбаха*, Изв. АН СССР, серия матем., 16(1952), стр. 347–368.

[11] И. В. Поляков, *Об исключительном множестве суммы простого и квадрата целого*, Изв. АН СССР, серия матем., 45(6)(1981), стр. 1391–1423.

Поступило 26.01.1984
и в исправленной форме 7.12.1984 (1395)

ACTA ARITHMETICA
XLVI (1985)

A congruence for the index of a unit of a real abelian number field

by

KENNETH S. WILLIAMS* and KENNETH HARDY** (Ottawa, Ont., Canada)

1. Introduction. Let K be a real abelian extension of the rational number field Q. As K is abelian, by the Kronecker–Weber theorem, K is contained in a cyclotomic field $Q(\zeta_n)$, where $\zeta_n = \exp(2\pi i/n)$, $n \not\equiv 2 \pmod 4$. We let $Q(\zeta_n)$ be the smallest such field containing K, so that n is the conductor of K. The ring of integers of $Q(\zeta_n)$ is

$$R = \Big\{ \sum_{j=0}^{\varphi(n)-1} a_j \zeta_n^j \colon a_j \in Z \ (0 \leqslant j \leqslant \varphi(n)-1) \Big\},$$

where φ denotes Euler's totient function and Z denotes the domain of rational integers.

Now let p be a prime $\equiv 1 \pmod n$, say, $p = nf+1$. Let g be a fixed primitive root modulo p. The cyclotomic polynomial of index n has $\varphi(n)$ distinct roots modulo p. One of these roots is g^f. Thus, by Kummer's theorem, the ideal

$$P = pR + (\zeta_n - g^f) R$$

of R is a prime ideal of norm p which divides pR. Thus the canonical homomorphism

$$(1.1) \qquad \lambda\colon\ R \to R/p \xrightarrow{\sim} Z/pZ$$

maps ζ_n onto $g^f \pmod p$. We have thus shown that for any given primitive root $g \pmod p$ there is a unique homomorphism $\lambda\colon R \to Z/pZ$ satisfying $\lambda(\zeta_n) \equiv g^f \pmod p$. This homomorphism is central to the rest of this paper.

For any integer a not divisible by p, the least non-negative integer b such that $a \equiv g^b \pmod p$ is called the *index of a with respect to g* and is denoted by $\operatorname{ind} a$. (We re-emphasize that g is regarded as fixed.) The purpose

---

* Research supported by Natural Sciences and Engineering Research Council Canada Grant A-7233.

** Research supported by Natural Sciences and Engineering Research Council Canada Grant A-8049.

of this paper is to obtain a congruence modulo a certain divisor of n for $\tilde{\varepsilon} = \operatorname{ind}\lambda(\varepsilon)$, where ε is a unit of K (see Theorem 1).

Taking K to be the real quadratic field $Q(\sqrt{D})$ of discriminant D, we obtain, as a special case of Theorem 1, a congruence for $\tilde{\varepsilon}_D = \lambda(\varepsilon_D)$ modulo $\mathrm{GCD}(D, h_D)$, where ε_D denotes the fundamental unit (>1) of $Q(\sqrt{D})$ and h_D denotes the class number of $Q(\sqrt{D})$ (see Theorem 2).

The congruences in Theorems 1 and 2 are given in terms of the cyclotomic numbers $(h, k)_n$ of order n, where for any integers h and k the cyclotomic number $(h, k)_n$ is defined to be the number of solutions (r, s) of

$$\begin{cases} 1+g^{nr+h} \equiv g^{ns+k} \pmod{p}, \\ 1 \leqslant r \leqslant f-1,\ 1 \leqslant s \leqslant f-1. \end{cases}$$

The basic properties of cyclotomic numbers are given for example in [14].

Finally, as explicit expressions are known for the cyclotomic numbers of orders 8, 12, 5 (see [6], [16], [15] respectively), Theorem 2 can be applied to the real quadratic fields $Q(\sqrt{2})$ (of conductor 8), $Q(\sqrt{3})$ (of conductor 12), $Q(\sqrt{5})$ (of conductor 5), to obtain explicit congruences for $\operatorname{ind}(1+\sqrt{2}) \pmod 8$, $\operatorname{ind}(2+\sqrt{3}) \pmod{12}$, $\operatorname{ind}\left(\frac{1}{2}(1+\sqrt{5})\right) \pmod 5$. This is done in Sections 4,5 and 6 respectively. Theorem 2 can also be applied to $Q(\sqrt{6})$ (of conductor 24) as the cyclotomic numbers of order 24 are known explicitly [5]. However, in this case the amount of elementary algebra needed to compute the right-hand side of Theorem 2 is extremely onerous so this was not done. For $D \neq 5, 8, 12, 24$ explicit expressions are not known for the cyclotomic numbers of order D and so are not available for use in Theorem 2. For example for $K = Q(\sqrt{7})$, we have $D = 28$, and although the cyclotomic numbers of orders 7 and 14 have been evaluated ([10], [11]) this is not the case for those of order 28.

2. Proof of Theorem 1. Let $U(K)$ denote the group of units of K and let $C(K)$ denote the group of cyclotomic units of K. $C(K)$ is a subgroup of $U(K)$ of finite index and we set $i(K) = [U(K):C(K)]$. It is known that $i(K)$ is related to the class number $h(K)$ of K (see for example [13]).

Let ε be a unit of K. Then we have $\varepsilon^{i(K)} \in C(K)$, and so there exist integers a $(=0, 1)$, b $(=0, 1, \ldots, n-1)$, c_j and d_j $(=0, 1, \ldots, n-1)$, $j = 1, 2, \ldots, k$, such that

$$(2.1)\qquad \varepsilon^{i(K)} = (-1)^a \zeta_n^b \prod_{j=1}^{k} (\zeta_n^{d_j}-1)^{c_j}.$$

Applying the homomorphism $\lambda\colon R \to Z/pZ$ to (2.1), we obtain

$$(2.2)\qquad \tilde{\varepsilon}^{i(K)} \equiv (-1)^a g^{bf} \prod_{j=1}^{k} (g^{d_j f}-1)^{c_j} \pmod{p}.$$

Taking the index of both sides of the congruence (2.2), we obtain, as $\operatorname{ind}(-1) = nf/2$,

$$(2.3)\qquad i(K)\operatorname{ind}\tilde{\varepsilon} \equiv \tfrac{1}{2}naf + bf + \sum_{j=1}^{k} c_j \operatorname{ind}(g^{d_j f}-1) \pmod{p-1}.$$

Now by a result of Muskat ([12], p. 499), we have

$$\operatorname{ind}(g^{df}-1) \equiv \sum_{l=1}^{n-1} l(l, d)_n \pmod{n},$$

so that

$$i(K)\operatorname{ind}\tilde{\varepsilon} \equiv \tfrac{1}{2}naf + bf + \sum_{j=1}^{k} c_j \sum_{l=1}^{n-1} l(l, d_j)_n \pmod{n}.$$

We have thus proved the following congruence for $\operatorname{ind}\tilde{\varepsilon}$ modulo $n/\mathrm{GCD}(n, i(K))$.

THEOREM 1.

$$\frac{i(K)}{\mathrm{GCD}(n, i(K))} \operatorname{ind}\tilde{\varepsilon} \equiv (\tfrac{1}{2}na+b)f + \sum_{j=1}^{k} c_j \sum_{l=1}^{n-1} l(l, d_j)_n \left(\bmod \frac{n}{\mathrm{GCD}(n, i(K))}\right).$$

3. Proof of Theorem 2. We take K to be the real quadratic field $Q(\sqrt{D})$ of discriminant D. It is well-known that the conductor n of $Q(\sqrt{D})$ is D and that $i(Q(\sqrt{D})) = h(Q(\sqrt{D})) = h_D$. The character χ_D of the field $Q(\sqrt{D})$ is given by $\chi_D(j) = \left(\frac{D}{j}\right)$, where $\left(\frac{D}{j}\right)$ is the Kronecker symbol.

Dirichlet's class number formula (see for example [4], p. 344) for h_D can be written in the form

$$(3.1)\qquad \varepsilon_D^{h_D} = \prod_{0<j<D/2} (\sin \pi j/D)^{-\chi_D(j)}.$$

We note that there are $\frac{1}{4}\varphi(D)$ values of j in the range $0 < j < D/2$ for which $\chi_D(j) = 1$, and $\frac{1}{4}\varphi(D)$ values for which $\chi_D(j) = -1$. The remaining values of j, namely those for which $\mathrm{GCD}(j, D) > 1$, are such that $\chi_D(j) = 0$. Replacing $\sin \pi j/D$ by $-i\zeta_D^{-j/2}(\zeta_D^j - 1)$ in (3.1), we obtain

$$(3.2)\qquad \varepsilon_D^{h_D} = \zeta_D^{\Sigma_D/2} \prod_{0<j<D/2} (\zeta_D^j - 1)^{-\chi_D(j)},$$

where

$$(3.3)\qquad \Sigma_D = \sum_{0<j<D/2} j\chi_d(j).$$

If $D \equiv 0 \pmod 4$, it is easily shown that $\Sigma_D \equiv 0 \pmod 2$ so that the exponent $\Sigma_D/2$ in (3.2) is an integer. If $D \equiv 1 \pmod 4$, Σ_D can be either even or odd, so in this case we write $\zeta_D^{\Sigma_D/2}$ in (3.2) in the form

$$\zeta_D^{\Sigma_D/2} = (\zeta_D^{1/2})^{\Sigma_D} = -(\zeta_D^{(D+1)/2})^{\Sigma_D} = (-1)^{\Sigma_D}\zeta_D^{((D+1)/2)\Sigma_D}. \tag{3.4}$$

Then (3.2) has the form (2.1) with

$$n = D, \quad i(K) = h_D, \quad \varepsilon = \varepsilon_D, \tag{3.5}$$

$$a = \begin{cases} 0, & \text{if} \quad D \equiv 0 \pmod 4, \\ \Sigma_D, & \text{if} \quad D \equiv 1 \pmod 4, \end{cases} \tag{3.6}$$

$$b = \begin{cases} \tfrac{1}{2}\Sigma_D, & \text{if} \quad D \equiv 0 \pmod 4, \\ \tfrac{1}{2}(D+1)\Sigma_D, & \text{if} \quad D \equiv 1 \pmod 4, \end{cases} \tag{3.7}$$

$$k = \begin{cases} D/2, & \text{if} \quad D \equiv 0 \pmod 4, \\ (D-1)/2, & \text{if} \quad D \equiv 1 \pmod 4, \end{cases} \tag{3.8}$$

and for $j = 1, 2, \ldots, k$

$$c_j = -\chi_D(j), \quad d_j = j. \tag{3.9}$$

Appealing to Theorem 1 we obtain the following congruence for ind $\tilde{\varepsilon}_D$ modulo $D/\mathrm{GCD}(D, h_D)$.

THEOREM 2.

$$\frac{h_D}{\mathrm{GCD}(D, h_D)} \operatorname{ind} \tilde{\varepsilon}_D \equiv \sum_{0<j<D/2} \chi_D(j)\left(\tfrac{1}{2}fj - \sum_{l=1}^{D-1} l(l, j)_D\right) \left(\operatorname{mod} \frac{D}{\mathrm{GCD}(D, h_D)}\right).$$

We remark that in Theorem 2 if we set

$$\varepsilon_D = \tfrac{1}{2}(T + U\sqrt{D}), \quad T \equiv U \pmod 2, \tag{3.10}$$

then appealing to the result [1]; p. 319

$$\sqrt{D} = \sum_{\substack{r=1 \\ (r,D)=1}}^{D-1} \chi_D(r)\zeta_D^r, \tag{3.11}$$

we have

$$\lambda(\sqrt{D}) \equiv \sum_{\substack{r=1 \\ (r,D)=1}}^{D-1} \chi_D(r) g^{rf} \pmod p, \tag{3.12}$$

and

$$\tilde{\varepsilon}_D \equiv \lambda(\varepsilon_D) \equiv \tfrac{1}{2}T + \tfrac{1}{2}U \sum_{\substack{r=1 \\ (r,D)=1}}^{D-1} \chi_D(r) g^{rf} \pmod p. \tag{3.13}$$

4. $K = Q(\sqrt{2})$. In this case $n = D = 8$, $\varepsilon_D = 1+\sqrt{2}$, $h_D = 1$, and for k odd

$$\chi_D(k) = \left(\frac{8}{k}\right) = \left(\frac{2}{k}\right) = \begin{cases} +1, & \text{if} \quad k \equiv 1, 7 \pmod 8, \\ -1, & \text{if} \quad k \equiv 3, 5 \pmod 8). \end{cases}$$

Let $p = 8f+1$ be a prime with primitive root g. Interpreting $\sqrt{2} = \frac{1}{2}\sqrt{8}$ modulo p as $\lambda(\sqrt{2}) \equiv \frac{1}{2}\lambda(\sqrt{8}) \equiv \frac{1}{2}(g^f - g^{3f} - g^{5f} + g^{7f}) \pmod p$, Theorem 2 gives

$$\operatorname{ind}(1+\sqrt{2}) \equiv -f + \sum_{l=1}^{7} l((l, 3)_8 - (l, 1)_8) \pmod 8. \tag{4.1}$$

Next we define integers x and y by

$$\sum_{m=2}^{p-1} \exp\left\{\frac{2\pi i}{4}(\operatorname{ind} m + \operatorname{ind}(1-m))\right\} = -x + 2y\sqrt{-1} \tag{4.2}$$

and integers a and b by

$$\sum_{m=2}^{p-1} \exp\left\{\frac{2\pi i}{8}(\operatorname{ind} m + 3\operatorname{ind}(1-m))\right\} = -a + b\sqrt{-2}. \tag{4.3}$$

It is known (see for example [3]) that

$$p = x^2 + 4y^2, \quad x \equiv 1 \pmod 4, \tag{4.4}$$

$$p = a^2 + 2b^2, \quad a \equiv (-1)^{(p-1)/8} \pmod 4. \tag{4.5}$$

Emma Lehmer ([6], pp. 115–117) has expressed the values of the cyclotomic numbers $(l, m)_8$ in terms of p, x, y, a and b. It should be noted that in order to make her formulae conform to the definitions of x, y, a, b given in (4.2) and (4.3), it is necessary to change the sign of a in her tables for the case $p \equiv 9 \pmod{16}$. Making use of her tables we obtain

$$4\sum_{l=1}^{7} l((l, 3)_8 - (l, 1)_8) \tag{4.6}$$

$$= \begin{cases} -1+3x+4y-2a-2b, & \text{if} \quad p \equiv 1 \pmod{16}, \operatorname{ind} 2 \equiv 0 \pmod 4, \\ -1-x+4y+2a-2b, & \text{if} \quad p \equiv 1 \pmod{16}, \operatorname{ind} 2 \equiv 2 \pmod 4, \\ -1+3x+12y+2a+2b, & \text{if} \quad p \equiv 9 \pmod{16}, \operatorname{ind} 2 \equiv 0 \pmod 4, \\ -1-x-4y-2a+2b, & \text{if} \quad p \equiv 9 \pmod{16}, \operatorname{ind} 2 \equiv 2 \pmod 4. \end{cases}$$

As

$$
(4.7)\quad \begin{cases}
x \equiv 4f+1 \pmod{32}, & a \equiv 4f+1 \pmod{16}, \\
y \equiv 0 \pmod 4, & b \equiv 0 \pmod 4, \\
 & \qquad \text{if } p \equiv 1 \pmod{16},\ \operatorname{ind} 2 \equiv 0 \pmod 4, \\
x \equiv 4f+25 \pmod{32}, & a \equiv 4f+5 \pmod{16}, \\
y \equiv 2 \pmod 4, & b \equiv 2 \pmod 4, \\
 & \qquad \text{if } p \equiv 1 \pmod{16},\ \operatorname{ind} 2 \equiv 2 \pmod 4, \\
x \equiv 4f+25 \pmod{32}, & a \equiv 12f+3 \pmod{16}, \\
y \equiv 0 \pmod 4, & b \equiv 2 \pmod 4, \\
 & \qquad \text{if } p \equiv 9 \pmod{16},\ \operatorname{ind} 2 \equiv 0 \pmod 4, \\
x \equiv 4f+17 \pmod{32}, & a \equiv 12f+7 \pmod{16}, \\
y \equiv 2 \pmod 4, & b \equiv 0 \pmod 4, \\
 & \qquad \text{if } p \equiv 9 \pmod{16},\ \operatorname{ind} 2 \equiv 2 \pmod 4,
\end{cases}
$$

we obtain

$$
(4.8)\quad 4\sum_{l=1}^{7} l\big((l,3)_8-(l,1)_8\big) \equiv \begin{cases} 4f-4y-2b \pmod{32}, & \text{if} \quad p \equiv 1 \pmod{16}, \\ 16+4f+4y+2b \pmod{32}, & \text{if} \quad p \equiv 9 \pmod{16}, \end{cases}
$$

and so by (4.1) we obtain

$$
(4.9)\quad \operatorname{ind}(1+\sqrt{2}) \equiv \begin{cases} -y-\tfrac{1}{2}b \pmod 8, & \text{if} \quad p \equiv 1 \pmod{16}, \\ 4+y+\tfrac{1}{2}b \pmod 8, & \text{if} \quad p \equiv 9 \pmod{16}. \end{cases}
$$

We have thus proved

THEOREM 3. *Let $p = 8f+1$ be a prime. Let g be a primitive root* (mod p). *Define $\sqrt{2}$ modulo p by*

$$2\sqrt{2} \equiv g^{f}-g^{3f}-g^{5f}+g^{7f} \pmod p.$$

Let (x, y) be the solution of

$$p = x^2+4y^2, \quad x \equiv 1 \pmod 4,$$

given by (4.2), *and let (a, b) be the solution of*

$$p = a^2+2b^2, \quad a \equiv (-1)^{(p-1)/8} \pmod 4,$$

given by (4.3). *Then we have*

$$
\operatorname{ind}(1+\sqrt{2}) \equiv \begin{cases} -y-\tfrac{1}{2}b \pmod 8, & \textit{if} \quad p \equiv 1 \pmod{16}, \\ 4+y+\tfrac{1}{2}b \pmod 8, & \textit{if} \quad p \equiv 9 \pmod{16}, \end{cases}
$$

A few values of p, g, a, b, x, y are given in Table 1 to illustrate Theorem 3.

Table 1

$p \equiv 1 \pmod 8$ $p < 500$	p (mod 16)	g	x	y	a	b	$\operatorname{ind}(1+\sqrt{2})$ (mod 8)	$-y-\frac{1}{2}b \pmod 8$ if $p \equiv 1 \pmod{16}$ $4+y+\frac{1}{2}b \pmod 8$ if $p \equiv 9 \pmod{16}$
17	1	3	1	2	−3	2	5	5
41	9	6	5	2	3	−4	4	4
73	9	5	−3	4	−1	−6	5	5
89	9	3	5	4	−9	−2	7	7
97	1	5	9	−2	5	6	7	7
113	1	3	−7	4	9	4	2	2
137	9	3	−11	2	3	8	2	2
193	1	5	−7	6	−11	−6	5	5
233	9	3	13	−4	15	2	1	1
241	1	7	−15	2	13	−6	1	1
257	1	3	1	8	−15	−4	2	2
281	9	3	5	−8	−9	10	1	1
313	9	10	13	−6	−5	12	4	4
337	1	10	9	8	−7	12	2	2
353	1	3	17	4	−15	−8	0	0
401	1	3	1	−10	−3	14	3	3
409	9	21	−3	10	11	−12	0	0
433	1	5	17	−6	−19	6	3	3
449	1	3	−7	10	21	−2	7	7
457	9	13	21	2	−13	12	4	4

Remark 1. As $y \equiv 0 \pmod 2$, by Theorem 3, we have

$$(4.10)\quad \operatorname{ind}(1+\sqrt{2}) \equiv 0 \pmod 2 \Leftrightarrow b \equiv 0 \pmod 4,$$

which is a result of Barrucand and Cohn [2]. From (4.7) we see that

$$(4.11)\quad y \equiv b+2f \pmod 4,$$

so that (4.10) can also be formulated

$$(4.12)\quad \operatorname{ind}(1+\sqrt{2}) \equiv 0 \pmod 2 \Leftrightarrow y \equiv \tfrac{1}{4}(p-1) \pmod 4.$$

Remark 2. If $b \equiv 0 \pmod 4$, by Theorem 3, we have

$$
\begin{aligned}
\operatorname{ind}(1+\sqrt{2}) \equiv 0 \pmod 4 &\Leftrightarrow y+\tfrac{1}{2}b \equiv 0 \pmod 4 \\
&\Leftrightarrow y \equiv \tfrac{1}{2}b \pmod 4 \\
&\Leftrightarrow \tfrac{1}{2}b+2f \equiv 0 \pmod 4,
\end{aligned}
$$

that is

$$\text{(4.13)} \qquad \operatorname{ind}(1+\sqrt{2}) \equiv 0 \pmod 4 \;\Leftrightarrow\; \tfrac{1}{4}b+f \equiv 0 \pmod 2,$$

which is Theorem 1 of [9].

Remark 3. By Theorem 3 we have

$$\text{(4.14)} \qquad \operatorname{ind}(1+\sqrt{2}) \equiv 0 \pmod 8$$

$$\Leftrightarrow \begin{cases} y+\tfrac{1}{2}b \equiv 0 \pmod 8, & \text{if} \quad p \equiv 1 \pmod{16}, \\ y+\tfrac{1}{2}b \equiv 4 \pmod 8, & \text{if} \quad p \equiv 9 \pmod{16}. \end{cases}$$

The case $p \equiv 1 \pmod{16}$ of (4.14) is Theorem 2 of [9].

5. $K = Q(\sqrt{3})$. In this case $n = D = 12$, $\varepsilon_D = 2+\sqrt{3}$, $h_D = 1$, and for k satisfying $(k, 12) = 1$

$$\chi_D(k) = \left(\frac{12}{k}\right) = \left(\frac{3}{k}\right) = \begin{cases} +1, & \text{if} \quad k \equiv 1, 11 \pmod{12}, \\ -1, & \text{if} \quad k \equiv 5, 7 \pmod{12}. \end{cases}$$

Let $p = 12f+1$ be a prime with primitive root g. Interpreting $\sqrt{3} = \frac{1}{2}\sqrt{12}$ modulo p as $\lambda(\sqrt{3}) \equiv \frac{1}{2}\lambda(\sqrt{12}) \equiv \frac{1}{2}(g^f - g^{5f} - g^{7f} + g^{11f}) \pmod p$, Theorem 2 gives

$$\text{(5.1)} \qquad \operatorname{ind}(2+\sqrt{3}) \equiv -2f + \sum_{l=1}^{11} l\big((l, 5)_{12} - (l, 1)_{12}\big) \pmod{12}.$$

Next we define integers x and y by

$$\text{(5.2)} \qquad \sum_{m=2}^{p-1} \exp\left\{\frac{2\pi i}{4}\big(\operatorname{ind} m + \operatorname{ind}(1-m)\big)\right\} = -x+2yi$$

and integers A and B by

$$\text{(5.3)} \qquad \sum_{m=2}^{p-1} \exp\left\{\frac{2\pi i}{6}\big(2\operatorname{ind} m + \operatorname{ind}(1-m)\big)\right\} = -A+B\sqrt{-3}$$

(see for example [16], p. 61). It is known that

$$\text{(5.4)} \qquad p = x^2+4y^2, \quad x \equiv 1 \pmod 4,$$

$$\text{(5.5)} \qquad p = A^2+3B^2, \quad A \equiv 1 \pmod 6.$$

Whiteman [16] has expressed the values of the cyclotomic numbers of order twelve in terms of p, A, B, x and y. There are twenty-four different sets of formulae depending upon $p \pmod{24}$, $\operatorname{ind} 2 \pmod 6$, $\operatorname{ind} 3 \pmod 4$, and the value of a certain quantity c, whose precise definition is not needed in this paper ([16], eqn. (5.7), p. 64). Using these formulae we obtain the following

table of values for $6\sum_{l=1}^{11} l\big((l, 5)_{12} - (l, 1)_{12}\big)$:

Table 2

Case	$6\sum_{l=1}^{11} l((l, 5)_{12}-(l, 1)_{12})$	p (mod 24)	c	ind 2 (mod 6)	ind 3 (mod 4)
1	$-2+8A+9B-6x-8y$	1	1	0	0
2	$-2+2A+3B-4y$	1	-1	0	0
3	$-2+2A+3B+4y$	1	1	2	0
4	$-2-4A-3B+6x+8y$	1	-1	2	0
5	$-2+5A+15B-3x-20y$	1	1	4	0
6	$-2-A+9B+3x-16y$	1	-1	4	0
7	$-2+8A+9B+2x+12y$	1	i	0	2
8	$-2+2A+3B+4x$	1	$-i$	0	2
9	$-2+2A+3B-4x$	1	i	2	2
10	$-2-4A-3B-2x-12y$	1	$-i$	2	2
11	$-2+5A+15B-x+24y$	1	i	4	2
12	$-2-A+9B+x+12y$	1	$-i$	4	2
13	$-2+11A+15B-5x$	13	i	1	0
14	$-2+5A-3B-7x-12y$	13	$-i$	1	0
15	$-2+2A+9B+4x$	13	i	3	0
16	$-2-4A-9B+2x-12y$	13	$-i$	3	0
17	$-2+2A+21B+4x$	13	i	5	0
18	$-2-4A+3B+2x-12y$	13	$-i$	5	0
19	$-2+5A-3B+3x+8y$	13	1	1	2
20	$-2+11A+15B+9x+4y$	13	-1	1	2
21	$-2-4A-9B-6x+8y$	13	1	3	2
22	$-2+2A+9B+4y$	13	-1	3	2
23	$-2-4A+3B-6x+8y$	13	1	5	2
24	$-2+2A+21B+4y$	13	-1	5	2

Treating the equations given by Whiteman for the cyclotomic numbers as congruences mod 16, we obtain

$$\text{(5.6)} \qquad A \equiv \begin{cases} \tfrac{1}{2}(p+1) \pmod 8, & \text{if} \quad p \equiv 1 \pmod{24}, \quad \operatorname{ind} 3 \equiv 0 \pmod 4, \\ \tfrac{1}{2}(p-3) \pmod 8, & \text{if} \quad p \equiv 1 \pmod{24}, \quad \operatorname{ind} 3 \equiv 2 \pmod 4, \\ \tfrac{1}{2}(p+5) \pmod 8, & \text{if} \quad p \equiv 13 \pmod{24}, \quad \operatorname{ind} 3 \equiv 0 \pmod 4, \\ \tfrac{1}{2}(p+1) \pmod 8, & \text{if} \quad p \equiv 13 \pmod{24}, \quad \operatorname{ind} 3 \equiv 2 \pmod 4, \end{cases}$$

$$\text{(5.7)} \qquad B \equiv \begin{cases} 0 \pmod 4, & \text{if} \quad p \equiv 1 \pmod{24}, \\ 2 \pmod 4, & \text{if} \quad p \equiv 13 \pmod{24}, \end{cases}$$

$$\text{(5.8)} \qquad x \equiv \begin{cases} \tfrac{1}{2}(p+1) \pmod 8, & \text{if} \quad p \equiv 1 \pmod{24}, \\ \tfrac{1}{2}(p-3) \pmod 8, & \text{if} \quad p \equiv 13 \pmod{24}, \end{cases}$$

$$\text{(5.9)} \qquad y \equiv \begin{cases} 0 \pmod 2, & \text{if} \quad p \equiv 1 \pmod{24}, \\ 1 \pmod 2, & \text{if} \quad p \equiv 13 \pmod{24}. \end{cases}$$

Similarly reducing the equations modulo 9 we obtain

$$(5.10)\quad A \equiv \begin{cases} 2p-1 \pmod 9, & \text{if } p \equiv 1 \pmod{24},\ \operatorname{ind} 2 \equiv 0 \pmod 6 \\ & \text{or} \\ & p \equiv 13 \pmod{24},\ \operatorname{ind} 2 \equiv 3 \pmod 6, \\ 2p+2 \pmod 9, & \text{if } p \equiv 1 \pmod{24},\ \operatorname{ind} 2 \equiv 2,4 \pmod 6 \\ & \text{or} \\ & p \equiv 13 \pmod{24},\ \operatorname{ind} 2 \equiv 1,5 \pmod 6, \end{cases}$$

$$(5.11)\quad B \equiv -\operatorname{ind} 2 \pmod 3,$$

$$(5.12)\quad x \equiv \begin{cases} 0 \pmod 3, & \text{if } p \equiv 1 \pmod{24},\ \operatorname{ind} 3 \equiv 2 \pmod 4 \\ & \text{or} \\ & p \equiv 13 \pmod{24},\ \operatorname{ind} 3 \equiv 0 \pmod 4, \\ 2p-1 \pmod 9, & \text{if } p \equiv 1 \pmod{24},\ \operatorname{ind} 3 \equiv 0 \pmod 4, c = +1 \\ & \text{or} \\ & p \equiv 13 \pmod{24},\ \operatorname{ind} 3 \equiv 2 \pmod 4, c = -1, \\ p-2 \pmod 9, & \text{if } p \equiv 1 \pmod{24},\ \operatorname{ind} 3 \equiv 0 \pmod 4, c = -1 \\ & \text{or} \\ & p \equiv 13 \pmod{24},\ \operatorname{ind} 3 \equiv 2 \pmod 4, c = +1, \end{cases}$$

$$(5.13)\quad y \equiv \begin{cases} 0 \pmod 3, & \text{if } p \equiv 1 \pmod{24},\ \operatorname{ind} 3 \equiv 0 \pmod 4 \\ & \text{or} \\ & p \equiv 13 \pmod{24},\ \operatorname{ind} 3 \equiv 2 \pmod 4, \\ 2p+2 \pmod 9, & \text{if } p \equiv 1 \pmod{24},\ \operatorname{ind} 3 \equiv 2 \pmod 4, c = +i \\ & \text{or} \\ & p \equiv 13 \pmod{24},\ \operatorname{ind} 3 \equiv 0 \pmod 4, c = -i, \\ p+4 \pmod 9, & \text{if } p \equiv 1 \pmod{24},\ \operatorname{ind} 3 \equiv 2 \pmod 4, c = -i \\ & \text{or} \\ & p \equiv 13 \pmod{24},\ \operatorname{ind} 3 \equiv 0 \pmod 4, c = +i. \end{cases}$$

Appealing to (5.1), Table 2, and the congruences (5.6)–(5.13), we obtain congruences for $\operatorname{ind}(2+\sqrt{3}) \bmod 8$ and $\bmod 9$ in each of the twenty-four cases. We just give the details in case 1 as the rest of the cases can be treated

similarly. By (5.1) and case 1 of Table 2 we have

$$(5.14)\qquad 6\operatorname{ind}(2+\sqrt{3}) \equiv -12f-2+8A+9B-6x-8y \pmod{72}.$$

Reducing (5.14) modulo 8 we obtain, as f is even in this case,

$$-2\operatorname{ind}(2+\sqrt{3}) \equiv -2+B+2x \pmod 8.$$

Appealing to (5.7) and (5.8) we obtain

$$-2+B+2x \equiv -B \pmod 8,$$

so that

$$(5.15)\qquad \operatorname{ind}(2+\sqrt{3}) \equiv B/2 \pmod 4.$$

Reducing (5.14) modulo 9, we obtain

$$-3\operatorname{ind}(2+\sqrt{3}) \equiv -3f-2-A+3x+y \pmod 9.$$

Appealing to (5.10) and (5.12) we obtain

$$-3f-2-A+3x+y \equiv y \pmod 9,$$

so that

$$(5.16)\qquad \operatorname{ind}(2+\sqrt{3}) \equiv -y/3 \pmod 3.$$

Putting all the twenty-four cases together we obtain

THEOREM 4. *Let $p = 12f+1$ be a prime. Let g be a primitive root* (mod p). *Define $\sqrt{3}$ modulo p by*

$$2\sqrt{3} \equiv g^f - g^{5f} - g^{7f} + g^{11f} \pmod p.$$

Let (x, y) be the solution of

$$p = x^2+4y^2, \qquad x \equiv 1 \pmod 4,$$

given by (5.2), *and let (A, B) be the solution of*

$$p = A^2+3B^2, \qquad A \equiv 1 \pmod 6,$$

given by (5.3). *Then we have*

$$(5.17)\qquad \operatorname{ind}(2+\sqrt{3}) \equiv (-1)^{\operatorname{ind}3/2+f-1}\, xy/3 \pmod 3$$

and

$$(5.18)\qquad \operatorname{ind}(2+\sqrt{3}) \equiv (-1)^{f(1+\operatorname{ind}3/2)} \frac{B}{2} \pmod 4.$$

A few values of p, g, A, B, x, y are given in Tables 3 and 4 to illustrate Theorem 4.

Table 3

$p \equiv 1 \pmod{12}$ $p < 500$	f (mod 2)	g	A	B	ind 3 (mod 4)	$\operatorname{ind}(2+\sqrt{3})$ (mod 4)	$(-1)^{f(1+\operatorname{ind}3/2)} B/2$ (mod 4)
13	1	2	+1	+2	0	3	3
37	1	2	−5	+2	2	1	1
61	1	2	+7	+2	2	1	1
73	0	5	−5	+4	2	2	2
97	0	5	+7	−4	2	2	2
109	1	6	+1	−6	0	3	3
157	1	5	+7	−6	2	1	1
181	1	2	+13	+2	0	3	3
193	0	5	+1	+8	0	0	0
229	1	6	−11	−6	0	3	3
241	0	7	+7	+8	2	0	0
277	1	5	+13	+6	0	1	1
313	0	10	−11	+8	0	0	0
337	0	10	−17	−4	2	2	2
349	1	2	+7	−10	2	3	3
373	1	2	+19	+2	2	1	1
397	1	5	−17	+6	2	3	3
409	0	21	+19	−4	2	2	2
421	1	2	−11	−10	0	1	1
433	0	5	+1	+12	0	2	2
457	0	13	−5	+12	2	2	2

Table 4

$p \equiv 1 \pmod{12}$ $p < 500$	f (mod 2)	g	ind 3 (mod 4)	x	y	$\operatorname{ind}(2+\sqrt{3})$ (mod 3)	$(-1)^{\operatorname{ind}3/2+f-1} xy/3$ (mod 3)
13	1	2	0	−3	−1	1	1
37	1	2	2	1	3	2	2
61	1	2	2	5	3	1	1
73	0	5	2	−3	4	2	2
97	0	5	2	9	−2	0	0
109	1	6	0	−3	−5	2	2
157	1	5	2	−11	3	2	2
181	1	2	0	9	−5	0	0
193	0	5	0	−7	6	2	2
229	1	6	0	−15	−1	2	2
241	0	7	2	−15	2	2	2
277	1	5	0	9	−7	0	0
313	0	10	0	13	−6	2	2
337	0	10	2	9	8	0	0
349	1	2	2	5	−9	0	0
373	1	2	2	−7	−9	0	0
397	1	5	2	−19	−3	2	2
409	0	21	2	−3	10	2	2
421	1	2	0	−15	7	1	1
433	0	5	0	17	−6	1	1
457	0	13	2	21	2	2	2

Remark 1. If $p \equiv 1 \pmod{24}$ (so that $f \equiv 0 \pmod 2$) by Theorem 4 we have

(5.19) $\operatorname{ind}(2+\sqrt{3}) \equiv 0 \pmod 4 \Leftrightarrow \frac{1}{2}B \equiv 0 \pmod 4 \Leftrightarrow B \equiv 0 \pmod 8,$

which is a result of Emma Lehmer ([9], Theorem 3).

Remark 2. Since

$$2(2+\sqrt{3}) = (1+\sqrt{3})^2,$$

the congruences in Theorem 4 give congruences for $\operatorname{ind}(1+\sqrt{3})$ modulo both 2 and 3.

Remark 3. From Theorem 4 we have

(5.20) $$\operatorname{ind}(2+\sqrt{3}) \equiv 0 \pmod 3 \Leftrightarrow xy/3 \equiv 0 \pmod 3.$$

If $p \equiv 1 \pmod{24}$, $\operatorname{ind} 3 \equiv 2 \pmod 4$ or $p \equiv 13 \pmod{24}$, $\operatorname{ind} 3 \equiv 0 \pmod 4$, by (5.12) and (5.13), we have $x \equiv 0 \pmod 3$, $y \not\equiv 0 \pmod 3$, so that (5.20) becomes in this case

(5.21) $$\operatorname{ind}(2+\sqrt{3}) \equiv 0 \pmod 3 \Leftrightarrow x \equiv 0 \pmod 9.$$

If $p \equiv 1 \pmod{24}$, $\operatorname{ind} 3 \equiv 0 \pmod 4$ or $p \equiv 13 \pmod{24}$, $\operatorname{ind} 3 \equiv 2 \pmod 4$, by (5.12) and (5.13), we have $x \not\equiv 0 \pmod 3$, $y \equiv 0 \pmod 3$, so that (5.20) becomes in this case

(5.22) $$\operatorname{ind}(2+\sqrt{3}) \equiv 0 \pmod 3 \Leftrightarrow y \equiv 0 \pmod 9.$$

Congruences (5.21) and (5.22) are due to Barrucand (see for example [8], p. 385).

6. $K = Q(\sqrt{5})$. In this case $n = D = 5$, $\varepsilon_D = \frac{1}{2}(1+\sqrt{5})$, $h_D = 1$, and for k satisfying $(k, 5) = 1$

$$\chi_D(k) = \left(\frac{5}{k}\right) = \begin{cases} +1, & \text{if } k \equiv 1, 4 \pmod 5, \\ -1, & \text{if } k \equiv 2, 3 \pmod 5. \end{cases}$$

Let $p = 5f+1$ be a prime with primitive root g. Interpreting $\sqrt{5}$ modulo p as $\lambda(\sqrt{5}) \equiv g^f - g^{2f} - g^{3f} + g^{4f} \pmod p$, Theorem 2 gives

(6.1) $$\operatorname{ind}\left(\tfrac{1}{2}(1+\sqrt{5})\right) \equiv -\frac{f}{2} + \sum_{l=1}^{4} l\left((l, 2)_5 - (l, 1)_5\right) \pmod 5.$$

Following Whiteman ([15], pp. 100–101), we may define integers x, u, v, w by

(6.2) $$4 \sum_{m=2}^{p-1} \beta^{\operatorname{ind} m + \operatorname{ind}(1-m)} = (-x+2u+4v+5w)\beta + (-x+4u-2v-5w)\beta^2 + +(-x-4u+2v-5w)\beta^3 + (-x-2u-4v+5w)\beta^4,$$

where $\beta = e^{2\pi i/5}$, or equivalently by

$$(6.3)\qquad \begin{cases} 3x = -p+14+25(0,0)_5, \\ u = (0,2)_5-(0,3)_5, \\ v = (0,1)_5-(0,4)_5, \\ w = (1,3)_5-(1,2)_5. \end{cases}$$

The 4-tuple (x, u, v, w) is a solution of Dickson's system

$$(6.4)\qquad \begin{cases} 16p = x^2+50u^2+50v^2+125w^2, \quad x \equiv 1 \pmod 5, \\ xw = v^2-4uv-u^2. \end{cases}$$

Whiteman has given the cyclotomic numbers of order 5 in terms of p, x, u, v, w (see [15], (4.9)). Using these in (6.1) we obtain

$$\operatorname{ind}\tfrac{1}{2}(1+\sqrt{5}) \equiv -u+3v \pmod 5.$$

We have thus proved

THEOREM 5. *Let $p = 5f+1$ be a prime. Let g be a primitive root* (mod p). *Define $\sqrt{5}$ modulo p by*

$$\sqrt{5} \equiv g^f - g^{2f} - g^{3f} + g^{4f} \pmod p.$$

Table 5

$p \equiv 1 \pmod 5$ $p < 500$	g	x	u	v	w	$\operatorname{ind}(\frac{1}{2}(1+\sqrt{5}))$ (mod 5)	$-u+3v$ (mod 5)
11	2	1	0	1	1	3	3
31	3	11	−2	−1	−1	4	4
41	6	−9	0	3	−1	4	4
61	2	1	−4	1	1	2	2
71	7	−19	2	3	1	2	2
101	2	−29	2	−3	−1	4	4
131	2	11	−6	1	−1	4	4
151	6	−4	−2	2	−4	3	3
181	2	11	−2	−7	−1	1	1
191	19	41	−4	3	1	3	3
211	2	1	2	−1	5	0	0
241	7	16	4	4	−4	3	3
251	6	−4	2	6	4	1	1
271	6	31	−8	1	−1	1	1
281	3	11	−4	−3	−5	0	0
311	17	−49	7	0	1	3	3
331	3	61	2	−5	1	3	3
401	3	−29	10	−3	−1	1	1
421	2	−19	8	1	5	0	0
431	7	36	6	6	−4	2	2
461	2	1	−2	−9	5	0	0
491	2	−9	−12	3	−1	1	1

Let (x, u, v, w) be the solution of (6.4) *given by* (6.2) *or equivalently by* (6.3). *Then we have*

$$(6.5)\qquad \operatorname{ind}\tfrac{1}{2}(1+\sqrt{5}) \equiv -u+3v \pmod 5.$$

A few values of p, g, x, u, v, w are given in Table 5 to illustrate Theorem 5.

Remark 1. The congruence (6.5) can also be deduced from the theorem proved in [17].

Remark 2. From the second equation in (6.4), we have, as $x \not\equiv 0 \pmod 5$,

$$u \equiv 3v \pmod 5 \Leftrightarrow w \equiv 0 \pmod 5.$$

Thus $\frac{1}{2}(1+\sqrt{5})$ is a fifth power (mod p) if and only if $w \equiv 0 \pmod 5$. This result is due to Emma Lehmer [7].

7. Acknowledgements. The authors would like to thank Control Data Canada Ltd. for providing the computer resources used in the preparation of this paper, and an unknown referee whose suggestions significantly improved the presentation of this paper.

References

[1] R. G. Ayoub, *Introduction to the analytic theory of numbers*, American Mathematical Society, Providence, Rhode Island 1963.

[2] P. Barrucand and H. Cohn, *Note on primes of type x^2+32y^2, class number, and residuacity*, J. Reine Angew. Math. 238 (1969), pp. 67–70.

[3] B. C. Berndt and R. J. Evans, *Sums of Gauss, Jacobi, and Jacobsthal*, J. Number Theory 11 (1979), pp. 349–398.

[4] Z. I. Borevich and I. R. Shafarevich, *Number Theory*, Academic Press, New York and London 1966.

[5] R. J. Evans, *Table of cyclotomic numbers of order twenty-four*, Math. Comp. 35 (1980), pp. 1036–1038; UMT file 12 [9.10], 98 pp.

[6] Emma Lehmer, *On the number of solutions of $u^k+D \equiv w^2 \pmod p$*, Pacific J. Math. 5 (1955), pp. 103–118.

[7] — *Artiads characterized*, J. Math. Anal. Appl. 15 (1966), pp. 118–131.

[8] — *On the cubic character of quadratic units*, J. Number Theory 5 (1973), pp. 385–389.

[9] — *On the quartic character of quadratic units*, J. Reine Angew. Math. 268/269 (1974), pp. 294–301.

[10] P. A. Leonard and K. S. Williams, *The cyclotomic numbers of order seven*, Proc. Amer. Math. Soc. 51 (1975), pp. 295–300.

[11] J. B. Muskat, *The cyclotomic numbers of order fourteen*, Acta Arith. 11 (1966), pp. 263–279.

[12] — *On Jacobi sums of certain composite orders*, Trans. Amer. Math. Soc. 134 (1968), pp. 483–502.

[13] W. Sinnott, *On the Stickelberger ideal and the circular units of an abelian field*, Invent. Math. 62 (1980), pp. 181–234.

[14] T. Storer, *Cyclotomy and difference sets*, Markham Publishing Co., Chicago 1967.

[15] A. L. Whiteman, *The cyclotomic numbers of order ten*, Proceedings of the Symposia in Applied Mathematics 10, pp. 95–111, Amer. Math. Soc., Providence, Rhode Island 1960.
[16] – *The cyclotomic numbers of order twelve*, Acta Arith. 6 (1960), pp. 53–76.
[17] K. S. Williams, *Explicit forms of Kummer's complementary theorems to his law of quintic reciprocity*, J. Reine Angew. Math. 288 (1976), pp. 207–210.

DEPARTMENT OF MATHEMATICS AND STATISTICS
CARLETON UNIVERSITY
OTTAWA, ONTARIO, CANADA
K1S 5B6

Received on 10.5.1984
and in revised form on 25.10.1984 (1425)

ACTA ARITHMETICA
XLVI (1985)

The distribution of square-free numbers

by

R. C. BAKER (Egham) and J. PINTZ (Budapest)

1. Introduction. Let

$$\Delta(x) = \sum_{n \leqslant x} \mu^2(n) - \frac{6}{\pi^2} x.$$

We write

$$\psi(\theta) = \theta - [\theta] - \tfrac{1}{2} \quad (\theta \text{ real}).$$

Let $\varepsilon > 0$. Montgomery and Vaughan [3] showed, on the Riemann hypothesis, that

(1) $$\Delta(x) = -\sum_{n \leqslant M} \mu(n) \psi\left(\frac{x}{n^2}\right) + O(x^{1/2+\varepsilon} M^{-1/2} + M^{1/2+\varepsilon}),$$

for any $M > 0$. They deduced that

$$\Delta(x) = O(x^{9/28+\varepsilon}).$$

Graham [1] improved the exponent 9/28 to 8/25. In the present note we sharpen this, proving

THEOREM. *If the Riemann hypothesis is correct, then*

$$\Delta(x) = O(x^{7/22+\varepsilon}).$$

The new idea is contained in Lemma 3, which is quite similar to work of Heath-Brown ([2], Section 4). We shall make several appeals to the exponential sum estimate

(2) $$\sum_{a < n \leqslant b} e(\lambda n^{-2}) \ll |\lambda|^{1/2} a^{-1} + |\lambda|^{-1/2} a^2$$

($0 < a < b \leqslant 2a$, λ real non-zero). See [4], Theorem 5.9. Here $e(\theta) = e^{2\pi i\theta}$; we also write $L = \log x$. Constants implied by '$\ll$' and 'O' notations depend at most on ε.

LEMMA 1. *For some N, H with*

(3) $$x^{7/22} < N \leqslant x^{4/11}, \quad 1/2 \leqslant H \leqslant x^{1/22},$$