Tôhoku Math. Journ.
20(1968), 498-510.

THE DISTRIBUTION OF kTH POWER RESIDUES AND NON-RESIDUES IN THE GAUSSIAN INTEGERS

JAMES H. JORDAN *)

(Received March 24, 1968)

1. Notation and Introduction. In this paper the Greek letters α, β, μ, σ, and ω will always be Gaussian integers, the Greek letters τ and λ will be complex numbers, the Greek letters γ and γ_j will always denote Gaussian primes. Also in this paper the Latin letters c, d, j, h, k, m, n, r, s, t, H and j^* will represent rational integers, the Latin letters p, q and q_j's will represent primes, and the Latin letters a, b, and C_j will represent real constants. The Latin letter e is the base of the natural logarithms and i is the imaginary unit.

Early in the century Vinogradov [13] considered the size of the smallest quadratic non-residue modulo p and established

THEOREM A. *If d is the smallest quadratic non-residue modulo p then*

$$d = O(p^a \log^2 p)$$

where

$$a = (2\sqrt{e})^{-1}.$$

In 1927 Vinogradov [14], [15] proved

THEOREM B. *If $k|p-1$ and if H_j is the class of kth power residues or a class of kth power non-residues, modulo p, then the number of elements of H_j that are $\leqq x$ is $x/k+\Delta$, where*

$$|\Delta| \leqq \sum_{h=1}^{x} \sum_{y=1}^{p/h} (p/xy+1).$$

A transformation on the sum implies that

$$|\Delta| < \sqrt{p} \log p$$

*) Research on this paper was supported by NSF Grant No. GP-6227.

and

THEOREM C. *If p is a prime and $k|p-1$ and $k \geqq m^m$, where $m \geqq 8$, then the least kth power non-residue is less than $p^{1/m}$ for all sufficiently large p.*

In 1952 Davenport and Erdös [5] improved Theorem C by using the positive continuous, strictly decreasing, function ρ defined on $[1, \infty]$ by

$$\rho(u) = 1 - \log u \quad \text{for} \quad 1 \leqq u \leqq 2$$

and

$$u\rho'(u) = -\rho(u-1) \quad \text{for} \quad u \geqq 2 .$$

Asymptotically $\rho(u) = \exp(-u \log u - u \log\log u + O(u))$. This function is apparently due to Dickman [6] but has been considerably condensed and clarified by de Bruijn [1].

Davenport and Erdös were able to prove

THEOREM D. *If p is a prime and $k|p-1$ and let d be the least kth power non-residue then $d = O(p^{a_k+\epsilon})$ for any fixed $\epsilon > 0$, where $(2a_k)^{-1}$ is the unique solution to $\rho(u) = k^{-1}$.*

All of these results lie quite heavily on the Polya [12]-Vinogradov [13] inequality.

In 1957 Burgess [2] succeeded in improving the Polya-Vinogradov inequality for the Legendre symbol. Specifically he established

THEOREM E. *Let σ and ϵ be any fixed positive numbers. Then, for all sufficiently large p and any N we have*

$$\left| \sum_{n=N+1}^{N+H} \left(\frac{n}{p} \right) \right| < \epsilon H$$

provided $H > p^{1/4+\sigma}$, where ( ) is the Legendre symbol.

Burgess improved Theorem A in the same paper by proving

THEOREM F. *If d denotes the least positive quadratic non-residue modulo p then $d = O(p^a)$ as $p \to \infty$ for any fixed $a > (4\sqrt{e})^{-1}$.*

In 1962 Burgess [3] generalized Theorem E with

THEOREM G. *If p is a prime and if χ is nonprincipal character, modulo p, and if H and r are arbitrary positive integers then*

$$\sum_{m=n+1}^{n+H} \chi(m) \ll H^{1-1/(r+1)} p^{1/4r} \log p$$

for any integer n, where $A \ll B$ is Vinogradov's notation for $|A| < C_1 B$ for same constant C_1 and in this theorem C_1 is absolute.

Burgess remarked that this theorem essentially halves the exponents of Theorem D.

It is the purpose of this paper to investigate the analogous concepts in the Gaussian integers. Specifically, if kth power non-residues modulo a Gaussian prime are defined as expected:

DEFINITION. If the equation $\eta^k \equiv \alpha \pmod{\gamma}$ is solvable in Gaussian integers, then α is called a kth power residue modulo γ and if the equation is not solvable in Gaussian integers then α is called a kth power non-residue modulo γ.

The results of this paper are:

THEOREM 1. *If α is a quadratic non-residue modulo γ, and $|\alpha| \leqq |\beta|$ for β a quadratic non-residue modulo γ, then $|\alpha| < |\gamma|^{a+\epsilon}$, for all $\epsilon > 0$, $a = (4\sqrt{e})^{-1}$, for all sufficiently large $|\gamma|$'s.*

And:

THEOREM 2. *Let $k \mid |\gamma|^2 - 1$ and let $(4a)^{-1}$ be the unique solution of $\rho(u) = k^{-1}$. If α is a kth power non-residue modulo γ and $|\gamma| \leqq |\beta|$ for β a kth power non-residue modulo γ then $|\alpha| < \gamma^{a+\epsilon}$, for all $\epsilon > 0$, and for all sufficiently large $|\gamma|$'s.*

2. Lemmas. Let $\hat{\tau}$ be the Hardman Square [7] centered at the origin with a vertex at $(1+i)\tau/2$ and the two half open line segments $((\pm 1 - i)\tau/2, (-1-i)\tau/2)$. Let $L(\tau)$ represent the number of lattice points in $\hat{\tau}$.

It was shown in [8] that if τ is a Gaussian integer, then $L(\tau) = |\tau|^2$. A less precise result is

LEMMA 1. $L(\tau) = |\tau|^2 + O(|\tau|)$.

Let P_1 represent the set of Gaussian primes in the first quadrant except $1+i$ and let P_2 represent the set of Gaussian primes on the positive real axis and denote $P_1 \cup P_2 = P$.

LEMMA 2. *There is a natural two to one correspondence between* P_1 *and the positive real primes congruent to* 1 *modulo* 4 *and a natural one to one correspondence between* P_2 *and the positive real primes congruent to* 3 *modulo* 4.

Essentially a prime $p \equiv 1 \pmod 4$ can be expressed uniquely as $p = c^2 + d^2$ with c and $d > 0$. Then the Gaussian primes $c + di$ and $d + ci$ are associated with p. The one to one correspondence is the identity correspondence.

A well known result is

LEMMA 3. *If* $(h, k) = 1$, *then*

$$\sum_{\substack{q \leq x \\ q \equiv h \pmod k}} q^{-1} = (\log\log x)(\phi(k))^{-1} + K + O(1/\log x)$$

where K *is a constant independent of* x *and* ϕ *is the Euler function.*

For the proof see Landau [11].

In [8] the following is established

LEMMA 4. *If* $-1 < b < 0$, *then*

$$\sum_{q \leq x} q^b = x^{1+b}/((1+b)\log x) + O(x^{b+1}/\log^2 x)\,.$$

Now following the pattern of [8], for $n \leq a^{-1} < n+1$, define

$$S_1 = \sum_{x^a}^{x} q_1^{-1}$$

$$S_2 = \sum_{x^a}^{\sqrt{x}} \sum_{q_1}^{x/q_1} (q_1 q_2)^{-1}$$

$$S_3 = \sum_{x^a}^{\sqrt[3]{x}} \sum_{q_1}^{\sqrt{x/q_1}} \sum_{q_2}^{x/q_1 q_2} (q_1 q_2 q_3)^{-1}$$

$$\vdots$$

$$S_j = \sum_{x^a}^{\sqrt[j]{x}} \sum_{q_1}^{\sqrt[j-1]{x/q_1}} \cdots \sum_{q_{j-1}}^{x/q_1 q_2 \cdots q_{j-1}} (q_1 q_2 \cdots q_j)^{-1}$$

and

$$I_1 = \int_a^1 y_1^{-1}\,dy_1$$

$$I_2 = \int_a^{1/2}\int_{y_1}^{1-y_1} (y_1y_2)^{-1}\,dy_2\,dy_1$$

$$I_3 = \int_a^{1/3}\int_{y_1}^{(1-y_1)/2}\int_{y_2}^{1-y_1-y_2} (y_1y_2y_3)^{-1}\,dy_3\,dy_2\,dy_1$$

$$\vdots$$

$$I_j = \int_a^{1/j}\int_{y_1}^{(1-y_1)/(j-1)}\cdots\int_{y_{j-1}}^{1-y_1-y_2\cdots-y_{j-1}} (y_1y_2\cdots y_j)^{-1}dy_j\cdots dy_1\,.$$

Implicit in the papers of Chowla and Vijayaragharan [4] and de Bruijn [1] are the fomulas

$$\lim_{x\to\infty}\sum_{j=1}^{n}(-1)^{j+1}S_j = \sum_{j=1}^{n}(-1)^{j+1}I_j$$

and

$$\sum_{j=1}^{n}(-1)^{j+1}I_j = 1-\rho(a^{-1})\,.$$

Let S_j^* be S_j only the primes are to run only over the arithmetic progression $wk+h$ where $(k,h)=1$.

Also in [8] is established

LEMMA 5. $(\phi(k))^j S_j^* = S_j + O(1/\log x)$, *where* ϕ *is the Euler function.*

Let $S_j(2)$ and $S_j^*(2)$ stand for S_j and S_j^* respectively only with the x's in the limits of summation replaced by x^2.

Also in [8] is

LEMMA 6. *If* $1>a>0$ *then* $S_j(2) = S_j + O(1/\log x)$ *and* $S_j^*(2) = S_j^* + O(1/\log x)$.

Let $\Psi(a, \mu)$ represent the set of Gaussian integers in $\hat{\mu}$ that have a prime factor that exceeds $|\mu|^a$.

LEMMA 7. $\lim_{|\mu|\to\infty} \Psi(a, \mu)/|\mu|^2 = 1 - \rho(a^{-1})$.

PROOF. Let γ_1 be a Gaussian prime. Then the Gaussian integers in $\hat{\mu}$ that are multiples of γ_1 are in one to one correspondence with the lattice points in $\widehat{(\mu/\gamma_1)}$ and by Lemma 1 $L(\mu/\gamma_1) = |\mu/\gamma_1|^2 + O(|\mu/\gamma_1|)$.

Now set $x = |\mu|/\sqrt{2}$ and adopt the notation that $\sum_A^B F(\gamma_j)$ means a summation over all γ_j in $P_1 \cup P_2$ with $A < |\gamma_j| < B$. Primes in other quadrants are merely associates of primes in $P_1 \cup P_2$. For $n \leqq a^{-1} < n+1$ one has

$$\begin{aligned}\Psi(a, \mu) - 1 = &\sum_{x^a}^{x} (L(\mu/\gamma_1) - 1)\\ &- \sum_{x^a}^{\sqrt{x}} \sum_{|\gamma_1|}^{x/|\gamma_1|} (L(\mu/\gamma_1\gamma_2) - 1)\\ &+ \sum_{x^a}^{\sqrt[3]{x}} \sum_{|\gamma_1|}^{\sqrt{x/|\gamma_1|}} \sum_{|\gamma_2|}^{x/|\gamma_1\gamma_2|} (L(\mu/\gamma_1\gamma_2\gamma_3) - 1)\\ &\cdot\\ &\cdot\\ &\cdot\\ &+ (-1)^{n+1} \sum_{x^a}^{\sqrt[n]{x}} \sum_{|\gamma_1|}^{\sqrt[n-1]{x/|\gamma_1|}} \cdots \sum_{|\gamma_{n-1}|}^{x/|\gamma_1\gamma_2\cdots\gamma_{n-1}|} (L(\mu/\gamma_1\gamma_2\cdots\gamma_{n-1}) - 1).\end{aligned}$$

Now consider the first of these sums:

$$\sum_{x^a}^{x} (L(\mu/\gamma_1) - 1) = \sum_{x^a}^{x} (|\mu/\gamma_1|^2 - 1) + O\left(\sum_{x^a}^{x} |\mu/\gamma_1|\right).$$

The first term on the right can be separated into those γ_1 in P_1 and those γ_1 in P_2, yielding

$$\begin{aligned}\sum_{x^a}^{x} (|\mu/\gamma_1|^2 - 1) &= 2|\mu|^2 \sum_{\substack{x^{2a}\\ q\equiv 1(4)}}^{x^2} q_1^{-1} + |\mu|^2 \sum_{\substack{x^a\\ q\equiv 3(4)}}^{x} q_1^{-2} + \sum_{\substack{x^{2a}\\ q\equiv 1(4)}}^{x^2} 2 - \sum_{\substack{x^a\\ q\equiv 3(4)}}^{x} 1\\ &= 2|\mu|^2 S_1^*(2) + |\mu|^2 o(1) + O(x^2/\log x) + O(x/\log x)\\ &= 2|\mu|^2 S_1^*(2) + o(|\mu|^2),\end{aligned}$$

where the progression indicated for $S_1^*(2)$ is $1+4h$.

The second term on the right is

$$O\left(2|\mu|\sum_{x^{2a}}^{x^2} q_1^{-1/2} + |\mu|\sum_{x^a}^{x} q_1^{-1}\right) = O(|\mu|x/\log x^2 + |\mu|\log(a^{-1}))$$

$$= o(|\mu|^2)\,.$$

So combining it follows that

$$\sum_{x^a}^{x} (L(\mu/\gamma_1) - 1) = 2|\mu|^2 S_1^*(2) + o(|\mu|^2)\,.$$

Now the second of these sums yields to the same type of treatment. Consider

$$\sum_{x^a}^{\sqrt{x}} \sum_{|\gamma_1|}^{x/|\gamma_1|} (L(\mu/\gamma_1\gamma_2) - 1) = \sum_{x^a}^{\sqrt{x}} \sum_{|\gamma_1|}^{x/|\gamma_1|} (|\mu/\gamma_1\gamma_2|^2 - 1) + O\left(\sum_{x^a}^{\sqrt{x}} \sum_{|\gamma_1|}^{x/|\gamma_1|} |\mu/\gamma_1|\right).$$

The first term on the right can be broken into two cases. Case one: Both γ_1 and γ_2 in P_1. Then

$$\sum_{\substack{x^a \\ \gamma_1,\gamma_2 \text{ in } P_1}}^{\sqrt{x}} \sum_{|\gamma_1|}^{x/|\gamma_1|} (|\mu/\gamma_1\gamma_2|^2 - 1) = 4|\mu|^2 \sum_{x^{2a}}^{x} \sum_{q_1}^{x^2/q_1} (q_1 q_2)^{-1} - \sum_{x^{2a}}^{x} \sum_{q_1}^{x^2/q_1} 2$$

$$= 4|\mu|^2 S_2^*(2) + O(x^2/\log x)$$

$$= 4|\mu|^2 S_2^*(2) + o(|\mu|^2)\,.$$

Case two: At least one of γ_1 or γ_2 is in P_2. It follows that

$$\sum_{x^a}^{\sqrt{x}} \sum_{|\gamma_1|}^{x/|\gamma_1|} (|\mu/\gamma_1\gamma_2|^2 - 1) \leqq |\mu|^2 \left(\sum_{\substack{x^{2a} \\ q_1 \text{ in } P_1}}^{x^2} q_1^{-1}\right)\left(\sum_{\substack{x^a \\ q_2 \text{ in } P_2}}^{x} q_2^{-2}\right) + |\mu|^2 \left(\sum_{\substack{x^a \\ q_1 \text{ in } P_2}}^{x} q_1^{-2}\right)^2 + O(x^2/\log x)$$

$$= |\mu|^2 S_1^*(2)\, o(1) + |\alpha|^2 (o(1))^2 + O(x^2/\log x)$$

$$= o(|\mu|^2)\,.$$

Hence the first term of the right hand side is

$$4|\mu|^2 S_2^*(2) + o(|\mu|^2)\,.$$

It is also a simple procedure to show that

$$O\left(\sum_{x^a}^{\sqrt{x}} \sum_{|\gamma_1|}^{x/|\gamma_1|} |\mu/\gamma_1\gamma_2|^{-1}\right) = o(|\mu|^2).$$

Therefore the entire second sum is

$$4|\mu|^2 S_2^* + o(|\mu|^2).$$

A similar general argument would show that

$$\sum_{x^a}^{\sqrt[t]{x}} \sum_{|\gamma_1|}^{\sqrt[t-1]{x/|\gamma_1|}} \cdots \sum_{|\gamma_{t-1}|}^{x/|\gamma_1\gamma_2\cdots\gamma_{t-1}|} L(\mu/\gamma_1\gamma_2\cdots\gamma_t) = (\phi(4))^t|\mu|^2 S_t^*(2) + o(|\mu|^2).$$

Combining the results in

$$\begin{aligned}\Psi(a, \mu) - 1 &= \sum_{m=1}^{n} (-1)^{m+1}(\phi(4))^m |\mu|^2 S_m^*(2) + o(|\mu|^2) \\ &= \sum_{m=1}^{n} (-1)^{m+1} |\mu|^2 (\phi(4))^m S_m^* + o(|\mu|^2) \\ &= \sum_{m=1}^{n} (-1)^{m+1} |\mu|^2 S_m + o(|\mu|^2)\end{aligned}$$

or equivalently

$$\frac{\Psi(a, \mu)}{|\mu|^2} = \frac{1}{|\mu|^2} + \sum_{m=1}^{n} (-1)^{m+1} S_m + o(1),$$

which is the result of Lemma 7.

Define $\hat{\tau} \oplus \sigma = \{\beta : \beta = \alpha + \sigma,\ \alpha \text{ in } \hat{\tau}\}$. A generalization of Theorem G established in [9] is

LEMMA 8. *If p is a prime congruent to 3 modulo 4, if χ is a non-principal Dirichlet character defined for the non-zero elements of $Z(i)/(p)$, (p) the principal ideal generated by p, and if μ and r are arbitrary, then*

$$\sum_{\alpha \in \hat{\mu} \oplus \sigma} \chi(\alpha) \ll |\mu|^{2-4/(2r+3)} p^{(r+1)/r(2r+3)} \log p$$

for any σ, where $\ll$ is Vinogradov's notation.

A result that follows from Lemma 8 that is a generalization of a theorem in [10] is

LEMMA 9. *If p is a prime congruent to 3 modulo 4, if $k | p^2 - 1$, if χ_k*

is a Dirichlet kth power character defined for the non-zero elements of $Z(i)/(p)$, *if* $K_0, K_1, \cdots, K_{k-1}$ *are the class of kth power residues and the* $k-1$ *classes of kth power non-residues, and* $N(K_j, \mu)$ *is the number of Gaussian integers in* $K_j \cap \hat{\mu}$, *then* $N(K_j, \mu) = |\mu|^2/k + E_j$ *where* $E_j \ll |\mu|^{2-4/(2r+3)} p^{(r+1)/r(2r+3)} \cdot \log p$.

PROOF. Let $E_j = N(K_j, \mu) - |\mu|^2/k$. Now

$$\text{(A)} \qquad \sum_{j=0}^{k-1} E_j = \sum_{j=0}^{k-1} N(K_j, \mu) - \sum_{j=0}^{k-1} |\mu|^2/k = 0\,.$$

Since χ_k^s is a non-principal Dirichlet character for $s = 1, 2, 3, \cdots, k-1$ it follows that

$$\Big| \sum_{\alpha \text{ in } \hat{\mu}} \chi_k^s(\alpha) \Big| < C_s |\mu|^{2-4/(2r+3)} p^{(r+1)/r(2r+3)} \log p\,.$$

If we let λ be a primitive kth root of unity the above expression becomes

$$\text{(B)} \qquad \Big| \sum_{j=0}^{k-1} \lambda^{js} N(K_j, \mu) \Big| < C_s |\mu|^{2-4/(2r+3)} p^{(r+1)/r(2r+3)} \log p\,.$$

But

$$\begin{aligned} \sum_{j=0}^{k-1} \lambda^{js} N(K_j, \mu) &= \sum_{j=0}^{k-1} \lambda^{js} (|\mu|^2/k + E_j) \\ &= \sum_{j=0}^{k-1} \lambda^{js} |\mu|^2/k + \sum_{j=0}^{k-1} \lambda^{js} E_j \\ &= \sum_{j=0}^{k-1} \lambda^{js} E_j\,. \end{aligned}$$

Examining a particular j, say j^*, and multiplying through (B) by λ^{-j^*s} one has

$$\text{(C)} \qquad \Big| \sum_{j=0}^{k-1} \lambda^{js-j^*s} E_j \Big| \leq C_s |\mu|^{2-4/(2r+3)} p^{(r+1)/r(2r+3)} \log p\,.$$

Adding over $s = 1, 2, \cdots, k-1$, throwing in expression (A) and using the triangular inequality one has

$$\left|\sum_{s=0}^{k-1}\sum_{j=0}^{k-1}\lambda^{js-j^*s}E_j\right| < \sum_{s=1}^{k-1}C_s|\mu|^{2-4/(2r+3)}p^{(r+1)/r(2r+3)}\log p .$$

But

$$\sum_{s=0}^{k-1}\sum_{j=0}^{k-1}\lambda^{(j-j^*)s}E_j = \sum_{j=0}^{k-1}E_j\sum_{s=0}^{k-1}\lambda^{(j-j^*)s}$$
$$= kE_{j^*}.$$

Hence

$$|E_{j^*}| < \sum_{s=1}^{k-1}C_s/k|\mu|^{2-4/(2r+3)}p^{(r+1)/r(2r+3)}\log p,$$

as claimed.

A parallel to Lemma 8 that can be established by identical arguments is

LEMMA 10. *If γ is in P_1 and χ is a non-principal Dirichlet character modulo γ and if the Gaussian integer μ and the positive integer r are arbitrary, then*

$$\sum_{\alpha\in\hat{\mu}\oplus\sigma}\chi(\alpha) \ll |\mu|^{2-4/(2r+3)}|\gamma|^{(r+1)/r(2r+3)}\log|\gamma|, \quad \text{for any } \sigma.$$

The slight difference in arguments for this Lemma and Lemma 8 occurs specifically in Lemma 4, and the replacing of $|\gamma|$ and $\hat{\gamma}$ for p and $\hat{p}$ respectively in article [9].

A parallel to Lemma 9 that is established in an identical manner is

LEMMA 11. *If γ is in P_1 and $k\,|\,|\gamma|^2-1$ and χ_k is a Dirichlet kth power character modulo γ, if $K_0, K_1, \cdots, K_{k-1}$ are the class of kth power non-residues and $N(K_j,\mu)$ is the number of Gaussian integers in $K_j\cap\hat{\mu}$, then*

$$N(K_j,\mu) = |\mu|^2/k+E_j$$

where

$$E_j \ll |\mu|^{2-4/(2r+3)}|\gamma|^{(r+1)/r(2r+3)}\log|\gamma|.$$

3. Proof of Theorem 1. Assume that Theorem 1 is false. That is, there is an infinite set of Gaussian primes, $\{\gamma\}$, such that for some $\varepsilon>0$ every $\omega\neq 0$ that satisfies the inequality $|\omega|\leqq|\gamma|^{a+\varepsilon}$ is a quadratic residue modulo γ. Let γ_1 be one such Gaussian prime. Choose $[\varepsilon]^{-1}+1 = r$. Let μ be such that

$$|\mu| = |\gamma_1|^{(1+1/r)/4}(\log|\gamma_1|)^{(2r+3)/2} + b, \quad -1 < b < 0.$$

Now by Lemma 9 or 11

$$N(K_j, \mu) = |\mu|^2/2 + E_j, \quad j = 0 \text{ or } 1,$$

where

$$\begin{aligned} |E_j| &< C_j|\mu|^{2-4/2r+3}|\gamma_1|^{(r+1)/r(2r+3)} \log|\gamma_1| \\ &= C_j|\mu|^2|\gamma_1^{(1+1/r)/4}(\log|\gamma_1|)^{(2r+3)/2}|^{-4/2r+3}|\gamma_1|^{(r+1)/r(2r+3)} \log|\gamma_1| \\ &= C_j|\mu|^2/\log|\gamma_1|. \end{aligned}$$

Hence

$$E_j = O(|\mu|^2/\log|\mu|) = o(|\mu|^2).$$

Also

$$\begin{aligned} |\gamma_1|^{a+\varepsilon} &\geqq (|\mu|^{4r/r+1}/(\log|\gamma_1|)^{2r(2r+3)/r+1})^{a+\varepsilon} \\ &= |\mu|^{4a-4a/r+1+4r\varepsilon/r+1}/(\log|\gamma_1|)^{2r(2r+3)(a+\varepsilon)/r+1} \\ &= |\mu|^{4a+4(r\varepsilon-a)/r+1}/(\log|\gamma_1|)^{2r(2r+3)(a+\varepsilon)/r+1} \\ &\geqq |\mu|^{4a+2\varepsilon}, \qquad \text{for } |\gamma_1| \text{ sufficiently large.} \end{aligned}$$

The value $4a + 2\varepsilon = e^{-1/2} + 2\varepsilon$ can be assumed to be less than 2.

Now since the quadratic residues modulo γ are closed under multiplication a quadratic non-residue in $\hat{\mu}$ must have a prime factor that exceeds $|\mu|^{4a+2\varepsilon}$. Therefore

$$\begin{aligned} N(K_1, \mu) = |\mu|^2/2 + E_1 &\leqq \Psi(4a+2\varepsilon, \mu) \\ &= (1-\rho((4a+2\varepsilon)^{-1}))|\mu|^2 + o(|\mu|^2) \\ &= \log((4a+2\varepsilon)^{-1})|\mu|^2 + o(|\mu|^2) \\ &= -\log(4a+2\varepsilon)|\mu|^2 + o(|\mu|^2) \\ &= (-\log(4a) - \log(1+\varepsilon/2a))|\mu|^2 + o(|\mu|^2) \\ &= |\mu|^2/2 - |\mu|^2\log(1+\varepsilon/2a) + o(|\mu|^2), \end{aligned}$$

since $a=1/4\sqrt{e}$. Therefore $|\mu|^2\log(1+\varepsilon/2a) \leqq -E_1 + o|\mu|^2$, which can happen for only finitely many γ's to be consistent with Lemmas 9 and 11.

4. Proof of Theorem 2. Assume that Theorem 2 is false. That is there is an infinite set of Gaussian primes, $\{\gamma\}$, such that for some $\varepsilon > 0$ every $\omega \neq 0$ that satisfies the inequality $|\omega| \leqq |\gamma|^{a+\varepsilon}$ is a kth power residue modulo γ. Let γ_1 be one of the primes of this set. Choose $r=1+[\varepsilon^{-1}]$ and select a μ such that

$$|\mu| = |\gamma_1|^{(1+1/r)/4}(\log|\gamma_1|)^{(2r+3)/2} + b\,, \quad \text{with } -1 \leqq b < 0\,.$$

Now by Lemma 9 or 11

$$N(K_j, \mu) = |\mu^2|/k + E_j\,, \quad j = 0, 1, 2, \cdots, k-1\,,$$

and in particular

$$\sum_{j=1}^{k-1} N(K_j, \mu) = (k-1)|\mu|^2/k - E_0$$

where

$$E_0 = o(|\mu|^2)\,.$$

Also

$$|\gamma_1|^{a+\varepsilon} \geqq |\mu|^{4a+2\varepsilon}, \quad \text{for } |\gamma_1| \text{ sufficiently large.}$$

Now since the kth power residues modulo γ are closed under multiplication a kth power non-residue in $\hat{\mu}$ must have a prime factor that exceeds $|\mu|^{4a+2\varepsilon}$. Therefore

$$\begin{aligned}\sum_{j=1}^{k-1} N(K_j, \mu) &= (k-1)|\mu|^2/k - E_0 \\ &\leqq \Psi(4a+2\varepsilon, \mu) \\ &= (1-\rho((4a+2\varepsilon)^{-1})|\mu|^2 + o(|\mu|^2) \\ &= (1-\rho((4a)^{-1}))|\mu|^2 + (\rho((4a)^{-1}) - \rho((4a+2\varepsilon)^{-1}))|\mu|^2 + o(|\mu|^2) \\ &= (k-1)|\mu|^2/k + (\rho((4a)^{-1}) - \rho((4a+2\varepsilon))^{-1}|\mu|^2 + o(|\mu|^2)\end{aligned}$$

or equivalently

$$-E_0 = c_\varepsilon|\mu|^2 + o(|\mu|^2) \qquad \text{and } c_\varepsilon < 0$$

since ρ is a strictly monotonic decreasing function. But this can happen for only finitely many γ's to be consistent with Lemmas 9 and 11.

REFERENCES

[1] N. G. DE BRUIJN, On the Number of positive Integers$\leqq x$ and Free of Prime Factors$<y$, Nederl. Akad. van Wetensch. Proc., Series A, 54(1951), 50-60.
[2] D. A. BURGESS, The Distribution of Quadratic Residues and Non-Residues, Mathematika, 4(1957), 106-112.
[3] D. A. BURGESS, On Character Sums and Primitive Roots, Proc. London Math. Soc., (3), 12(1962), 179-192.
[4] S. CHOWLA AND T. VIJAYARAGHARAN, On the Largest Prime Divisions of Numbers, J. Indian Math. Soc., (N. S.), 11(1947), 31-37.
[5] H. DAVENPORT AND P. ERDÖS, The Distribution of Quadratic and Higher Residues, Publ. Math., 2(1952), 252-265.
[6] K. DICKMAN, On the frequency of numbers containing prime factors of a certain relative magnitude, Ark. Mat. Astr. Fys., 22 No. A, 10(1930).
[7] N. R. HARDMAN AND I. H. JORDAN, A Minimal Problem Connected with Complete Residue Systems in the Gaussian Integers, Math. Monthly, 74, No. 5(1967), 559-561.
[8] J. H. JORDAN, The Divisibility of Gaussian Integers by Large Gaussian Primes, Duke Math. J., 32, No. 3, 503-510.
[9] J. H. JORDAN, Character Sums in $Z(i)/(p)$, Proc. London Math. Soc., (3), 17(1967), 1-10.
[10] J. H. JORDAN, The Distribution of kth Power Residues and Non-Residues, Proc. AMS., 19(1968), 678-680.
[11] E. LANDAU, Primzahlen, 1(1909), 449-450.
[12] G. POLYA, Über die Verteilung der Quadratischen Reste und Nichtreste, Göltunge Nachrichter, (1918), 21-29.
[13] I. M. VINOGRADOV, Sur la Distribution des Residues et des Non-Residues des Puissances, J. Soc. Phys. Math. Perm, 1(1918), 94-98.
[14] I. M. VINOGRADOV, On a General Theorem Concerning the Distribution of the Residues and Non-Residues of Powers, Trans. Amer. Math Soc., 29(1927), 209-217.
[15] I. M. VINOGRADOV, On the Bound of the Least Non-Residue of nth Powers, Trans. Amer. Math. Soc., 29(1927), 218-226.

DEPARTMENT OF MATHEMATICS
WASHINGTON STATE UNIVERSITY
PULLMAN, WASHINGTON, U. S. A.