PACIFIC JOURNAL OF MATHEMATICS
Vol. 16, No. 1, 1966

# THE DISTRIBUTION OF CUBIC AND QUINTIC NON-RESIDUES

JAMES H. JORDAN

**For a prime $p \equiv 1 \pmod 3$, the reduced residue system $S_3$, modulo $p$, has a proper multiplicative subgroup, $C^0$, called the cubic residues modulo $p$. The other two cosets formed with respect to $C^0$, say $C^1$ and $C^2$, are called classes of cubic non-residues. Similarly for a prime $p \equiv 1 \pmod 5$ the reduced residue system $S_5$, modulo $p$, has a proper multiplicative subgroup, $Q^0$, called the quintic residues modulo $p$. The other four cosets formed with respect to $Q^0$, say $Q^1$, $Q^2$, $Q^3$ and $Q^4$ are called classes of quintic non-residues. Two functions, $f_3(p)$ and $f_5(p)$, are sought so that (i) if $p \equiv 1 \pmod 3$ then there are positive integers $a_i \in C^i$, $i = 1, 2$, such that $a_i < f_3(p)$, and (ii) if $p \equiv 1 \pmod 5$ then there are positive integers $a_i \in Q^i$, $i = 1, 2, 3, 4$ such that $a_i < f_5(p)$. The results established in this paper are that for $p$ sufficiently large, (i) $f_3(p) = p^{\alpha+\varepsilon}$, where $\alpha$ is approximately .191, and (ii) $f_5(p) = p^{\beta+\varepsilon}$, where $.27 < \beta < .2725$.**

Davenport and Erdös [3] raised the general question about the size of the smallest element in any given class of $k$th power non-residues. The special cases $k = 3$ and $k = 5$ are of primary concern in this paper. They proved a quite general theorem of which two special cases are:

THEOREM A. *For sufficiently large primes $p \equiv 1 \pmod 3$ and $\varepsilon > 0$ each class of cubic non-residues possess a positive integer smaller than $p^{55/112+\varepsilon}$.*

THEOREM B. *For sufficiently large primes $p \equiv 1 \pmod 5$ and $\varepsilon > 0$ each class of quintic non-residues possess a positive integer smaller than $p^{197/396+\varepsilon}$.*

In the same paper Davenport and Erdös used a result of de Bruijn [2] to improve the constant of Theorem A to approximately .383.

Recently D. A. Burgess [1] succeeded in improving Polya's inequality concerning character sums. Burgess' result is

THEOREM C. *If $p$ is a prime and if $\chi$ is a nonprincipal character, modulo $p$, and if $H$ and $r$ are arbitrary positive integers then*

Received April 8, 1963 and in revised form May 4, 1964.

$$I\colon \sum_{m=n+1}^{n+H} \chi(m) \ll H^{1-1/r+1} p^{1/4r} \, ln \, p \; ,$$

*for any integer n, where* $A \ll B$ *is Vinogradov's notation for* $|A| < cB$ *for some constant c, and in this Theorem c is absolute.*

The application of Theorem C to the arguments of Davenport and Erdös cuts each of the exponents of $p$ in half.

The achievement of this paper is to obtain the same result about cubic non-residues by an argument which is independent of the de Bruijn result, reduce the exponent on the result for quintic non-residues by a similar argument, and indicate a method of obtaining results for any primeth power non-residues.

## 2. Cubic Non-Residues.

A well known result about sums of inverses of primes is:

$$\mathrm{II}: \sum_{q \leqq x} 1/q = ln \, ln \, x + K + O(1/ln \, x) \; ,$$

where $K$ is a positive constant.[1]

LEMMA 1. *If* $0 \leqq v < 1/2$ *then*

$$\sum_{x^{1-v}}^{x} 1/q = \int_{1-v}^{1} 1/y \, dy + O(1/ln \, x) \, ,$$

*where the error term is independent of v.*

The proof of Lemma 1 follows directly from II.

LEMMA 2. *If* $0 \leqq v < 1/2$ *then*

$$\sum_{x^{(1-v)/2}}^{\sqrt{x}} \sum_{q_1}^{x/q_1} 1/q_1 q_2 = \int_{(1-v)/2}^{1/2} \int_{y}^{1-y} (yz)^{-1} dz dy + O(1/ln \, x) \; ,$$

*where* $q_1$ *and* $q_2$ *run only over primes and the error term is independent of v.*

*Proof.*

$$\sum_{x^{(1-v)/2}}^{\sqrt{x}} \sum_{q_1}^{x/q_1} 1/q_1 q_2 = \sum_{x^{(1-v)/2}}^{\sqrt{x}} 1/q_1 (ln \, ln \, (x/q_1) - ln \, ln \, q_1 + O(1/ln \, x))$$

$$= \sum_{x^{(1-v)/2}}^{\sqrt{x}} 1/q_1 (ln \, ln \, (x/q_1) - ln \, ln \, q_1) + O(1/ln \, x) \, .$$

Now by a well known summation Theorem,[2]

[1] See for example LeVeque, *Topics in Number Theory*, Vol. 1, Th. 6-20, p. 108.

[2] See for example LeVeque, Ibid, Th. 6-15, p. 103, with $\lambda_n$ the $n$th prime, $c_n = 1/\lambda_n$, and $f(y) = ln \, ln \, (x/y) - ln \, ln \, y + O(1/ln \, x)$.

$$\sum_{x^{(1-v)/2}}^{\sqrt{x}} \sum_{q_1}^{x/q_1} 1/q_1q_2 = \int_{x^{(1-v)/2}}^{\sqrt{x}} \frac{(ln\, ln\, t + K + 0(1/ln\, x))ln\, x\, dt}{(t\, ln\, t\, ln\,(x/t))}$$
$$- (ln((1-v)/2) + ln\, ln\, x + K$$
$$+ O(1/ln\, x))(ln\,((1+v)/(1-v)) + O(1/ln\, x)\ .$$

If the change of variable $t = x^s$ *is* made then

$$\sum_{x^{(1-v)/2}}^{\sqrt{x}} \sum_{q_1}^{x/q_1} 1/q_1q_2 = \int_{(1-v)/2}^{1/2} \frac{ln\, s}{s(1-s)} ds + \int_{(1-v)/2}^{1/2} \frac{ln\, ln\, x + K + O(1/ln\, x))}{s(1-s)} ds$$
$$- (ln\,((1-v)/2) + ln\, ln\, x + K$$
$$+ O(1/ln\, x))(ln\,(1+v)/(1-v)) + O(1/ln\, x)$$
$$= \int_{(1-v)/2}^{1/2} \frac{ln\, s}{s(1-s)} ds - ln\,((1-v)/2)\, ln\,((1+v)/(1-v))$$
$$+ O(1/ln\, x)$$
$$= \int_{(1-v)/2}^{1/2} \frac{ln(1-s) - ln\, s}{s} ds + O(1/ln\, x)$$
$$= \int_{(1-v)/2}^{1/2} \int_{y}^{1-y} (yz)^{-1} dz dy + O(1/ln\, x)\ .$$

For any positive integer $r$ and primes $p \equiv 1 \pmod 3$ let $x = 3[p^{(1+1/r)/4}(ln^2 p)^{r+1}/3]$. Let $C^j(x) = C^j \cap \{m \mid 0 < m \leqq x\}$, $j = 0, 1, 2$, and let $N(C^j(x))$ be the cardinality of $C^j(x)$.

The following is a special case of a general theorem of Vinogradov [4], [5].

LEMMA 3. $N(C^j(x)) = x/3 + O(x/ln\, x)$, $j = 0, 1, 2$.

*Proof.* Formula I with $H = x$, and $n = 0$ reads as

$$\sum_{m=1}^{x} \chi(m) \ll x^{1-1/r+1} p^{1/4r}\, ln\, p$$
$$\leqq (p^{(1+1/r)/4}(ln^2 p)^{r+1})^{r/r+1} p^{1/4r}\, ln\, p$$
$$= p^{1/4+1/4r}\,(ln^2 p)^r \cdot ln\, p$$
$$= p^{(1+1/r)/4}(ln^2 p)^{r+1}/ln\, p\ .$$

In other notation

$$\sum_{m=1}^{x} \chi(m) = O(x/ln\, x)\ .$$

Let $\chi_{3,p}$ be the cubic residue character for primes $p \equiv 1 \pmod 3$. By the above there is an absolute constant, $K_1$, such that

$$\text{III}: \left| \sum_{m=1}^{x} \chi_{3,p}(m) \right| < K_1 x/ln\, x\ .$$

Set $N(C^j(x)) = x/3 + T_j$, $j = 0, 1, 2$. Notice that $T_0 = -T_1 - T_2$. Let $w = \cos 2\pi/3 + i\sin 2\pi/3$.

It now follows that

$$\begin{aligned}\sum_{m=1}^{x} \chi_{3,p}(m) &= \sum_{j=0}^{2} (x/3 + T_j)w^j \\ &= \sum_{j=0}^{2} T_j w^j \\ &= -(T_1 + T_2)3/2 + i(T_1 - T_2)\sqrt{3}/2 .\end{aligned}$$

Now by III: $|T_1 + T_2| < 2K_1 x/3 \ln x$ and $|T_1 - T_2| < 2K_1 x/\sqrt{3} \ln x$. These inequalities imply that $|T_1|$ and $|T_2|$ are less than $2K_1 x/\sqrt{3} \ln x$. Hence $|T_0| < 4K_1 x/\sqrt{3} \ln x$ completing the proof of the lemma.

THEOREM 1. *Let $d$ be the solution of*

$$1/3 = \int_{1-v}^{1} 1/y\, dy + \int_{(1-v)/2}^{1/2} \int_{y}^{1-y} (yz)^{-1} dz dy .$$

*For all sufficiently large primes $p \equiv 1 \pmod 3$ there is in each class of cubic non-residues modulo $p$, a positive integer smaller than $p^{(1-d)/4+\varepsilon}$. ($d$ satisfies the inequality $.234 < d < .235$).*

*Proof.* Given $\varepsilon > 0$ let $r = [1/\varepsilon] + 1$. Define $x$ in terms of $p$ as above and notice that as long as $\varepsilon < d$ then

$$\begin{aligned}x^{1-d+\varepsilon} &= [p^{(1+1/r)/4}(\ln^2 p)^{r+1}/3]^{1-d+\varepsilon}3^{1-d+\varepsilon} \\ &\leqq p^{(1-d+\varepsilon)/4+(1-d+\varepsilon)/4r} \cdot (\ln^2 p)^{(1-d+\varepsilon)(r+1)} \\ &< p^{(1-d+\varepsilon)/4+1/4r} \cdot (\ln^2 p)^{r+1} \\ &< p^{(1-d)/4+\varepsilon}, \qquad \text{for sufficiently large primes } p.\end{aligned}$$

It therefore suffices to prove that for sufficiently large primes, each class of cubic non-residues contains a positive integer smaller than $x^{1-d+\varepsilon}$.

Assume that Theorem 1 is false. Then, for some fixed $\varepsilon > 0$, there are infinitely many primes $p \equiv 1 \pmod 3$ such that one of their classes of non-residues fails to contain a positive integer less than $x^{1-d+\varepsilon}$. Let $p_1$ be one such prime. Notice that $x, C^0, C^1$ and $C^2$ are defined in terms of $p_1$ and will therefore be fixed in this argument.

Without loss of generality $C^2$ can represent that class of non-residues modulo $p_1$ that has no positive integers less than $x^{1-d+\varepsilon}$. Since $C^2$ has this property it follows that $C^1$ has no positive integer less than $x^{(1-d+\varepsilon)/2}$ because $a$ in $C^1$ implies $a^2$ in $C^2$.

Since $C^0$ is closed under multiplication, modulo $p_1$, an integer $w$ in $C^2(x)$ must have prime factors not in $C^0$. If $w$ has exactly one prime factor, $q$, not in $C^0$ then $q$ must be in $C^2$. If $w$ has exactly two prime factors, $q_1$ and $q_2$, not in $C^0$ then both $q_1$ and $q_2$ must be in $C^0$. Further $w$ cannot have more than two prime factors not in $C^0$ since the product of any three or more prime factors not in $C^0$ exceeds $x$.

A consequence of the above conditions on positive integers in $C^2(x)$ is the following upper bound for $N(C^2(x))$:

$$\mathrm{IV}: \sum_{x^{1-d+\varepsilon}}^{x} [x/q_1] + \sum_{\sqrt{x^{1-d+\varepsilon}}}^{\sqrt{x}} \sum_{q_1}^{x/q_1} [x/q_1q_2]$$

where the $q_1$ and $q_2$ are taken only over primes. But

$$\begin{aligned}\mathrm{IV} &\leqq x\Big(\sum_{x^{1-d+\varepsilon}}^{x} 1/q_1 + \sum_{\sqrt{x^{1-d+\varepsilon}}}^{\sqrt{x}} \sum_{q_1}^{x/q_1} 1/q_1q_2\Big) \\ &< x\Big(-ln\,((1-d+\varepsilon)/(1-d)) + \int_{1-d}^{1} 1/y dy \\ &\quad + \int_{(1-d)/2}^{1/2}\int_{y}^{1-y} (yx)^{-1} dzdy + K_2/ln\, x\Big) \\ &= x(-ln\,(1+\varepsilon/(1-d)) + 1/3) + K_2x/ln\, x\ ,\end{aligned}$$

where $K_2$ is a constant independent of $x$. But this inequality can hold only for finitely many primes to be compatible with Lemma 3.

**3. Quintic Non-Residues.** It is helpful to adopt the following notations: Let

$$I_1 = \int_{(1-v)}^{1} 1/y dy$$

$$I_2 = \int_{(1-v)/2}^{1/2}\int_{y}^{1-y} (yz)^{-1} dzdy$$

$$I_3 = \int_{(1-v)/4}^{(1-v)/2}\int_{1-v-y}^{1-y} (yz)^{-1} dzdy$$

$$I_4 = \int_{(1-v)/4}^{(1-v)/3}\int_{y}^{(1-v-y)/2}\int_{1-v-y-z}^{1-y-z} (yzu)^{-1} dudzdy$$

$$I_5 = \int_{(1-v)/4}^{(1-v)/3}\int_{(1-v-y)/2}^{(1-y)/2}\int_{z}^{1-y-z} (yzu)^{-1} dudzdy$$

$$I_6 = \int_{(1-v)/3}^{1/3}\int_{y}^{(1-y)/2}\int_{z}^{1-y-z} (yzu)^{-1} dudzdy$$

$$I_7 = \int_{(1-v)/4}^{1/4}\int_{y}^{(1-y)/3}\int_{z}^{(1-y-z)/2}\int_{u}^{1-y-z-u} (yzut)^{-1} dtdudzdy\ .$$

In the following summation the $q_i$ run only over primes.

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

$$S_2 = \sum_{x^{(1-v)/2}}^{\sqrt{x}} \sum_{q_1}^{x/q_1} 1/q_1q_2$$

$$S_3 = \sum_{x^{(1-v)/4}}^{x^{(1-v)/2}} \sum_{x^{1-v}/q_1}^{x/q_1} 1/q_1q_2$$

$$S_4 = \sum_{x^{(1-v)/4}}^{x^{(1-v)/3}} \sum_{q_1}^{\sqrt{x^{(1-v)}/q_1}} \sum_{x^{1-v}/q_1q_2}^{x/q_1q_2} 1/q_1q_2q_3$$

$$S_5 = \sum_{x^{(1-v)/4}}^{x^{(1-v)/3}} \sum_{\sqrt{x^{(1-v)}/q_1}}^{\sqrt{x/q_1}} \sum_{q_2}^{x/q_1q_2} 1/q_1q_2q_3$$

$$S_6 = \sum_{x^{(1-v)/3}}^{\sqrt[3]{x}} \sum_{q_1}^{\sqrt{x/q_1}} \sum_{q_2}^{x/q_1q_2} 1/q_1q_2q_3$$

$$S_7 = \sum_{x^{(1-v)/4}}^{\sqrt[4]{x}} \sum_{q_1}^{\sqrt[3]{x/q_1}} \sum_{q_2}^{\sqrt{x/q_1q_2}} \sum_{q_3}^{x/q_1q_2q_3} 1/q_1q_2q_3q_4 .$$

We can now restate

LEMMA 1. *If* $0 \leqq v < 1/2$ *then* $S_1 = I_1 + O(1/ln\, x)$, *and*

LEMMA 2. *If* $0 \leqq v < 1/2$ *then* $S_2 = I_2 + O(1/ln\, x)$, *and similarly*

LEMMA $j + 1$. *If* $0 \leqq v < 1/2$ *then* $S_j = I_j + O(1/ln\, x)$ *for* $j = 3, 4, 5, 6, 7$.

The proofs of Lemmas 4, 5, 6, 7, and 8 are straight forward generalizations of Lemmas 1 and 2 and are much too lengthy to be exhibited here.

For any positive integer $r$ and primes $p \equiv 1 \pmod 5$ let $x = 5[p^{(1+1/r)/4}(ln^2 p)^{r+1}/5]$. Let $Q^j(x) = Q^j \cap \{m \mid 0 < m \leqq x\}$, $j = 0, 1, 2, 3, 4$, and let $N(Q^j(x))$ be the cardinality of $Q^j(x)$.

The following is another special case of the general Theorem of Vinogradov [4], [5]:

LEMMA 9. $N(Q^j(x)) = x/5 + O(x/ln\, x)$, $j = 0, 1, 2, 3, 4$.

*Proof.* Let $\chi_{5,p}$ be the quintic residue character for primes $p \equiv 1 \pmod 5$. By the argument in the proof of Lemma 3 there is an absolute constant $K_3$ such that

$$\text{V}: \left| \sum_{m=1}^{x} \chi_{5,p}(m) \right| < K_3 x/ln\, x .$$

Set $N(Q^j(x)) = x/5 + T_j$, $j = 0, 1, 2, 3, 4$. Notice that $T_0 = -\sum_{j=1}^{4} I_j$. Let $\rho = \cos 2\pi/5 + i \sin 2\pi/5$.

It now follows that

$$\begin{aligned}\sum_{m=1}^{x} \chi_{5,p}(m) &= \sum_{j=0}^{4} (x/5 + T_j)\rho^j \\ &= \sum_{j=0}^{4} T_j\rho^j \\ &= \sum_{j=1}^{4} T_j(\cos 2\pi j/5 - 1) + i \sum_{j=1}^{4} T_j \sin 2\pi j/5 .\end{aligned}$$

Now from V it follows that

(i): $|(T_1 + T_4)(\cos 2\pi/5 - 1) + (T_2 + T_3)(\cos 4\pi/5 - 1)| < K_3x/ln\, x$

and

(ii): $|(T_1 - T_4)\sin 2\pi/5 + (T_2 - T_3)\sin 4\pi/5| < K_3x/ln\, x$.

Notice that $\chi^2_{5,p}$ is also a character and by the argument in the proof of Lemma 3 of § 2 there is an absolute constant $K_4$ such that

$$\text{VI}: \left|\sum_{m=1}^{x} \chi^2_{5,p}(m)\right| < K_4x/ln\, x .$$

But on the other hand

$$\begin{aligned}\sum_{m=1}^{x} \chi^2_{5,p}(m) &= \sum_{j=0}^{4} (x/5 + T_j)\rho^{2j} \\ &= \sum_{j=0}^{4} T_j\rho^{2j} \\ &= \sum_{j=1}^{4} T_j (\cos 4\pi j/5 - 1) + i \sum_{j=1}^{4} T_j \sin 4\pi j/5 .\end{aligned}$$

Now by VI it follows that

(iii): $|(T_1 + T_4)(\cos 4\pi/5 - 1) + (T_2 + T_3)(\cos 2\pi/5 - 1)| < K_4x/ln\, x$

(iv): $|(T_1 + T_4)\sin 4\pi/5 + (T_3 - T_2)\sin 2\pi/5| < K_4x/ln\, x$.

With a little manipulation of (i), (ii), (iii), and (iv) one can obtain $|T_j| < K_5x/ln\, x$, $j = 0, 1, 2, 3, 4$, where $K_5$ is an absolute constant independent of $x$, proving Lemma 9.

THEOREM 2. *Let $d$ denote the solution of $1/5 = \sum_{i=1}^{7} I_i$. For all sufficiently large primes $p \equiv 1 \pmod 5$ there is in each class of quintic non-residues, modulo $p$, a positive integer smaller than $p^{(1+d)/4+\varepsilon}$ ($d$ satisfies the inequality $.08 < d < .09$).*

*Proof.* Given $\varepsilon > 0$ let $r = [1/\varepsilon] + 1$. Define $x$ in terms of $p$ as above and notice as long as $\varepsilon < d$ then $x^{1-d+\varepsilon} < p^{(1-d)/4+\varepsilon}$ for sufficiently large values of $p$. It will suffice to prove that for sufficiently large primes $p \equiv 1$ (mod 5) that each class of quintic non-residues modulo $p$ contains a positive integer less than $x^{1-d+\varepsilon}$.

Assume that Theorem 2 is false. Then, for some fixed $\varepsilon > 0$, there are infinitely many primes $p \equiv 1 \pmod 5$ such that one of their classes of non-residues fails to contain a positive integer less than $x^{1-d+\varepsilon}$.

Let $p_1$ be one such prime. Notice that $x, Q^0, Q^1, Q^2, Q^3$ and $Q^4$ are defined in terms of $p_1$ and will therefore be fixed in this argument.

Without loss of generality $Q^4$ can represent that class of non-residues modulo $p_1$ that has no positive integers less than $x^{1-d+\varepsilon}$. Since $Q^4$ has this property it follows that $Q^1, Q^2$ and $Q^3$ have no positive integers less than $x^{(1-d+\varepsilon)/4}$ because $a$ in $Q^1$ or $Q^3$ implies $a^4$ in $Q^4$ and $a$ in $Q^2$ implies $a^2$ in $Q^4$.

Since $Q^0$ is closed under multiplication, modulo $p_1$, an integer $w$ in $Q^4(x)$ must have prime factors not in $Q^0$. One of the following conditions holds depending on the exact number of primes, $q_i$, not in $Q^0$ that divide $w$.

(i) There exists a prime $q_1$ such that $q_1 \mid w$ and $x^{1-d+\varepsilon} \leqq q_1 \leqq x$, since $q_1$ is in $Q^4(x)$.

(ii) There exist primes $q_1$ and $q_2$ such that $q_1q_2 \mid w$ and $x^{1-d+\varepsilon} < q_1q_2 < x$, since $q_1q_2$ is in $Q^4(x)$.

(iii) There exist primes $q_1$, $q_2$ and $q_3$ such that $q_1q_2q_3 \mid w$ and $x^{1-d+\varepsilon} < q_1q_2q_3 < x$, since $q_1q_2q_3$ is in $Q^4(x)$.

(iv) There exists primes $q_1, q_2, q_3$, and $q_4$ such that $q_1q_2q_3q_4 \mid w$ and $x^{1-d+\varepsilon} < q_1q_2q_3q_4 < x$, since $q_1q_2q_3q_4$ is in $Q^4(x)$.

It should be noticed that $w$ cannot have more than four prime divisors which are not in $Q^0$ since the product of any five or more primes not in $Q^0$ would exceed $x$. The number of $w$'s that could possibly satisfy (i) is less than or equal to

$$\sum_{x^{1-d+\varepsilon}}^{x} [x/q_1] \, .$$

The number of $w$'s that could possibly satisfy (ii) is less than $x(S_2 + S_3)$. The number of $w$'s that could possibly satisfy (iii) is less than $x(S_4 + S_5 + S_6)$. The number of $w$'s that could possibly satisfy (iv) is less than $xS_7$. Combining the above we have

$$\begin{aligned} N(Q^4(x)) &< \sum_{x^{1-d+\varepsilon}}^{x} [x/q_1] + x\sum_{i=2}^{7} S_i \\ &\leqq -\sum_{x^{1-d}}^{x^{1-d+\varepsilon}} [x/q_1] + x\sum_{i=1}^{7} S_i \\ &= -x\, ln\,((1-d+\varepsilon)/(1-d)) + x\Big(\sum_{i=1}^{7} I_i + K_6/ln\, x\Big) \\ &= x(-ln(1+\varepsilon/(1-d)) + 1/5) + K_6x/ln\, x \, , \end{aligned}$$

where $K_6$ is a constant independent of $x$. But this inequality can hold only for finitely many primes to be compatible with Lemma 9.

**4. Remarks.** The techniques of the previous sections generalize for $K$th power non-residues when $K$ is a prime. In these cases the definition of $d$ involves $(K^2 - 3K + 4)/2$ integrals ranging from multiplicity 1 through $K-1$. There are $K-1$ possible divisibility conditions imposed on the elements of $A^{K-1}(x)$. The upper bound for $N(A^{k-1}(x))$ involves $(K^2-3K+4)/2$ summations ranging from multiplicity 1 through $K-1$. The contradiction is reached in the same manner. The details are lengthy but straightforward. For example for seventh power residues the results of Davenport and Erdös imply an exponent of $p$ equal to 959/3840. While using methods exhibited in § 3 one obtains an exponent smaller than 25/104.

When $K$ is composite the job is more difficult since the subgroup of $K$th power residues and the $K-1$ cosets form a cyclic group of composite order. These cyclic groups have proper subgroups. The "without loss of generality" comment is no longer valid and some arguments concerning the number of prime factors of $K$ must be called upon. The author intends to present these techniques at a future date.

## REFERENCES

1. D. A. Burgess, *On character sums and primitive roots*, London Math. J. **12**, No. 45, (1962), 179-192.
2. N. G. de Bruijn, *On the number of positive integers* $< x$ *and free of prime factors* $< y$, Indagationes Mathematicae, **13**, No. 1, (1951), 50-60.
3. H. Davenport, and P. Erdös, *The distribution of quadratic and higher residues*, Publications Mathematicae, 2: (1952), 252-265.
4. I. M. Vinogradov, *Sur la distribution des residues et des non-residus des puissances*, Journal Physico-Mathematical Society University Perm, No. 1 (1918), 94-96.
5. ———, *On a general theorem concerning the distribution of the residues and non-residues of powers*, Trans. Amer. Math. Soc. **29** (1927), 209-217.