ACTA ARITHMETICA
XV (1969)

Upper bounds for kth power coset representatives modulo n

by

KARL K. NORTON (Boulder, Colo.)

1. Introduction. Let n and k be positive integers, let $C(n)$ denote the multiplicative group consisting of the residue classes mod n which are relatively prime to n, and let $C_k(n)$ denote the subgroup of kth powers. Write $\nu = \nu_k(n) = [C(n): C_k(n)]$, and let

$$1 = g_0(n, k) < g_1(n, k) < \ldots < g_{\nu-1}(n, k)$$

be the smallest positive representatives of the ν cosets of $C_k(n)$. In this paper we shall obtain upper bounds for $g_m(n, k)$, $0 \leqslant m \leqslant \nu-1$.

To the best of the author's knowledge, all previously published work on this problem depended on the assumption that n is a prime p, and many of the estimates obtained are effective only for large p. Much of this work was restricted to special values of k (e.g., $k = 2, 3$, or 5), and all of it was devoted to obtaining estimates for either $g_1(p, k)$ (the smallest kth power non-residue mod p) or $g_{\nu-1}(p, k)$, with no attention being given to the estimation of $g_m(p, k)$ as a function of m.

In [21], [22] (note that [21] is reprinted in [24], pp. 54-57), I. M. Vinogradov obtained results from which it follows immediately that

$$g_{\nu-1}(p, k) < 1+\nu p^{1/2}\log p \tag{1.1}$$

(here $\nu = (k, p-1)$), and in [23], he obtained a better inequality for $g_1(p, k)$ when p is very large. Davenport and Erdös [8] improved Vinogradov's estimate for $g_1(p, k)$ when $\nu \geqslant 4$, and they showed also that

$$g_{\nu-1}(p, k) < p^{1/2-\beta} \tag{1.2}$$

for p sufficiently large, where $\beta = \beta(\nu)$ is positive and tends to 0 as $\nu \to +\infty$. J. H. Jordan [12] showed that $\beta(\nu)$ could be replaced by a function $\beta^*(\nu)$ which is larger but still tends to 0.

Using D. A. Burgess's remarkable estimates for character sums [4], [5], [6], it is possible to obtain dramatic improvements of some of the above results. In [3], Burgess improved a result of Vinogradov by showing that

$$(1.3)\qquad g_1(p,2) = O(p^{\gamma+\varepsilon})$$

for each $\varepsilon > 0$, where $\gamma = (4e^{1/2})^{-1}$. In [7], he showed that the maximum number of consecutive integers in a given coset of $C_k(p)$ is $O(p^{1/4}\log p)$, where the implied constant is absolute (this improves a result of Davenport and Erdös [8], p. 264). Jordan [13], using one of Burgess's estimates, showed that

$$(1.4)\qquad g_{\nu-1}(p,3) = O(p^{\zeta+\varepsilon}), \qquad g_{\nu-1}(p,5) = O(p^{\theta+\varepsilon})$$

for each $\varepsilon > 0$, where ζ is approximately 0.191 and $0.2275 < \theta < 0.23$ (these bounds for θ are misprinted in his paper). The first of these results improves Theorem 3 of [8].

For further results and references, see [1], [2].

In the present paper, we do not restrict the modulus n to prime values, and some of our results give specific estimates which are often fairly effective even for small values of n. In Theorem (3.18), we give a general inequality for $g_m(n,k)$ involving character sums. From this we can derive inequalities such as

$$(1.5)\qquad g_m(n,k) \leqslant 1 + \frac{n}{\varphi(n)}\, 2^{3r/2}\left(\frac{m\nu}{\nu-m}\right)^{1/2} n^{1/2}\log n$$

for $0 \leqslant m \leqslant \nu-1$, where r denotes the number of distinct prime factors of n. Using (1.5), it can be shown that $g_{\nu-1}(n,k) = O(n^{1/2+\varepsilon})$ for each $\varepsilon > 0$, where the implied constant depends only on k and ε. We obtain better results by using Burgess's inequalities for character sums. In particular, we show that

$$(1.6)\qquad g_{\nu-1}(n,k) = O(n^{3/8+\varepsilon}),$$

and in certain cases (for example, if n is cubefree, or if $2\nmid(n,k)$ and k is squarefree), we have

$$(1.7)\qquad g_{\nu-1}(n,k) = O(n^{1/4+\varepsilon}).$$

If we make the further assumption that the number of distinct prime factors of n is bounded above by a function of k alone, then (1.6) and (1.7) can be improved slightly by using a method due to Davenport and Erdös, and we obtain

$$(1.8)\qquad g_{\nu-1}(n,k) = O(n^{3(1-\delta)/8+\varepsilon}),$$

whereas if the conditions for (1.7) hold, it follows that

$$(1.9)\qquad g_{\nu-1}(n,k) = O(n^{(1-\delta)/4+\varepsilon}).$$

Here δ is a very small positive function of k (and $\delta \to 0$ as $k \to +\infty$).

In Section 8, we mention an application of results like (1.5) to a seemingly unrelated problem in the theory of congruences. This will be the subject of a future paper.

This paper is an extension of part of the author's Ph. D. thesis [17], which was written at the University of Illinois. I would like to thank Professor Paul T. Bateman, my thesis advisor, for his guidance. Thanks are due also to Dr. Richard L. Roth for some helpful comments.

2. Notation. Except in a few obvious cases, small Latin letters other than e and i represent integers, and p always denotes a (positive) prime number. When $n > 1$ and we have occasion to refer to the prime factorization of n, we shall always write $n = p_1^{a_1}\dots p_r^{a_r}$, where $p_1 < \dots < p_r$ and $a_j \geqslant 1$ for each j. With reference to this factorization of n, we write $k = p_1^{f_1}\dots p_r^{f_r}k_0$, where $f_j \geqslant 0$ for each j and $(k_0, p_1\dots p_r) = 1$. We define

$$\gamma_j = \begin{cases} \min\{a_j, f_j+1\} & \text{if} \quad p_j \text{ is odd,} \\ \min\{a_j, f_j+2\} & \text{if} \quad p_j = 2. \end{cases}$$

Also, let

$$\lambda = \lambda_k(n) = \begin{cases} 2 & \text{if} \quad n \text{ is even and } k \text{ is odd,} \\ 1 & \text{otherwise.} \end{cases}$$

When there is no risk of confusion, we write $\nu_k(n) = \nu$, $g_j(n,k) = g_j$.

φ denotes Euler's function, and μ is the Möbius function. χ always denotes a residue character, and χ_0 is the principal character with respect to the modulus in question. ψ denotes a typical character mod n such that $\psi^k = \chi_0$. (Such a character is said to have *exponent* k.)

If B is a set, $|B|$ means the number of elements in B. An empty sum means 0, and an empty product means 1. $[\beta]$ means the largest integer $\leqslant \beta$. Finally, "iff" means "if and only if".

3. Basic lemmas.

(3.1) Lemma. *Let G be a finite multiplicative Abelian group, and let G^* denote its character group. If H is any subgroup of G, define*

$$(3.2)\qquad H' = \{\theta \in G^*:\ \theta(x) = 1 \text{ for all } x \in H\}.$$

For each $\theta \in H'$, define θ^* on G/H by $\theta^*(xH) = \theta(x)$. Then:

$$(3.3)\qquad G \text{ is isomorphic to } G^*;$$

$$(3.4)\qquad H = \{x \in G:\ \theta(x) = 1 \text{ for all } \theta \in H'\};$$

(3.5) *The mapping $\theta \to \theta^*$ is an isomorphism of H' onto $(G/H)^*$;*

$$(3.6)\qquad \sum_{x\in H}\theta(x) = \begin{cases} |H| & \text{if} \quad \theta \in H', \\ 0 & \text{if} \quad \theta \in G^* - H'; \end{cases}$$

(3.7) $$\sum_{\theta\in H'}\theta(x) = \begin{cases}[G:H] & \textit{if} \quad x\in H,\\ 0 & \textit{if} \quad x\in G-H;\end{cases}$$

(3.8) *If* $\sigma=[G:H]$ *and* $x_1,\ldots,x_\sigma$ *are any representatives of the distinct cosets of* H, *then*

$$\sum_{j=1}^{\sigma}\theta(x_j)=\begin{cases}\sigma & \textit{if} \quad \theta \textit{ is the principal character},\\ 0 & \textit{if} \quad \theta\in H' \textit{ and } \theta \textit{ is non-principal}.\end{cases}$$

Proof. (3.3), (3.4), and (3.5) are proved in [9], pp. 194-196, and in [11], pp. 212-214. The first part of (3.6) is obvious, while if $\theta\in G^*-H'$, there exists $y\in H$ such that $\theta(y)\neq 1$, and

$$\sum_{x\in H}\theta(x)=\sum_{x\in H}\theta(xy)=\theta(y)\sum_{x\in H}\theta(x),$$

so that the second part of (3.6) follows. (3.7) is proved similarly (using (3.3), (3.4), and (3.5)).

To prove (3.8), we apply (3.5).

$$\sum_{j=1}^{\sigma}\theta(x_j)=\sum_{j=1}^{\sigma}\theta^*(x_jH)=\begin{cases}\sigma & \text{if} \quad \theta^* \text{ is principal},\\ 0 & \text{otherwise},\end{cases}$$

by (3.6) (with G and H both replaced by G/H). Since θ^* is principal iff θ is principal, (3.8) follows.

For the remainder of this section, all residue characters are to the modulus n, and ψ denotes the typical character of exponent k. Recall that r is the number of distinct prime factors of n.

(3.9) Lemma. *For* $0\leqslant s\leqslant \nu-1$ *and* $0\leqslant h\leqslant n$, *let* $N_s(h)$ *be the number of* x *satisfying* $1\leqslant x\leqslant h$ *and* $x\in g_sC_k(n)$. *Then*

(3.10) $$N_s(h)=\nu^{-1}\{n^{-1}\varphi(n)h+R_n(h)+\Delta_s(h)\},$$

where

(3.11) $$R_n(h)=\sum_{d|n}\mu(d)([h/d]-h/d)$$

and

(3.12) $$\Delta_s(h)=\sum_{\psi\neq\chi_0}\bar{\psi}(g_s)\sum_{x=1}^{h}\psi(x).$$

Furthermore,

(3.13) $$\sum_{s=0}^{\nu-1}\Delta_s(h)=0,$$

(3.14) $$\sum_{s=0}^{\nu-1}\Delta_s^2(h)=\nu\sum_{\psi\neq\chi_0}\Big|\sum_{x=1}^{h}\psi(x)\Big|^2,$$

and

(3.15) $$|R_n(h)|<2^{r-1} \quad \textit{if} \quad n>1.$$

Proof. In Lemma (3.1), take $G=C(n)$ and $H=C_k(n)$, so H' is just the set of all ψ. By (3.5) and (3.3), the number of ψ is $[G:H]=\nu$, and by (3.7),

$$\nu^{-1}\sum_{\psi}\psi(x)\bar{\psi}(g_s)=\begin{cases}1 & \text{if} \quad x\in g_sC_k(n),\\ 0 & \text{otherwise}.\end{cases}$$

Summing this formula over $1\leqslant x\leqslant h$, we get

(3.16) $$N_s(h)=\nu^{-1}\sum_{\psi}\sum_{x=1}^{h}\psi(x)\bar{\psi}(g_s)=\nu^{-1}\sum_{x=1}^{h}\chi_0(x)+\nu^{-1}\Delta_s(h).$$

Now,

(3.17) $$\sum_{x=1}^{h}\chi_0(x)=\sum_{x=1}^{h}\sum_{d|(x,n)}\mu(d)=\sum_{d|n}\mu(d)\sum_{1\leqslant x\leqslant h,d|x}1 = \sum_{d|n}\mu(d)h/d+R_n(h).$$

Thus (3.10) is proved, with $R_n(h)$, $\Delta_s(h)$ defined by (3.11) and (3.12) respectively.

(3.13) can be obtained by summing (3.12) over s and applying (3.8), or by noting that

$$\sum_{s=0}^{\nu-1}N_s(h)=\sum_{x=1}^{h}\chi_0(x)$$

and using (3.16).

To prove (3.14), square both sides of (3.12) and sum over s to get

$$\sum_{s=0}^{\nu-1}\Delta_s^2(h)=\sum_{s=0}^{\nu-1}\sum_{\psi_1\neq\chi_0\neq\psi_2}\sum_{x_1,x_2=1}^{h}\psi_1(x_1)\bar{\psi}_2(x_2)(\bar{\psi}_1\psi_2)(g_s).$$

Inverting the order of summation and using (3.8), we get (3.14).

Finally, if $n>1$,

$$-R_n(h)\leqslant\sum_{d|n,\mu(d)=1}(h/d-[h/d])<\sum_{d|n,\mu(d)=1}1=\Sigma_1,$$

say, and likewise

$$-R_n(h)>-\sum_{d|n,\mu(d)=-1}1=\Sigma_2.$$

Since

$$\Sigma_1+\Sigma_2=\sum_{d|n}\mu(d)=0$$

and

$$\Sigma_1-\Sigma_2=\sum_{d|n}|\mu(d)|=2^r,$$

(3.15) follows immediately.

The following fundamental result indicates that upper estimates for character sums can be applied to obtain upper bounds for the numbers $g_m(n, k)$.

(3.18) THEOREM. *For* $0 \leqslant m \leqslant \nu-1$, *we have*

$$g_m \leqslant 1+\frac{n}{\varphi(n)}\left(\frac{m}{\nu-m}\right)^{1/2}\Big\{\sum_{\psi\neq\chi_0}\Big|\sum_{x=1}^{g_m-1}\psi(x)\Big|^2\Big\}^{1/2}-\frac{n}{\varphi(n)}R_n(g_m-1).$$

Proof. Let m be fixed throughout this proof, and write $h_m = g_m-1$. Also write $H_m = n^{-1}\varphi(n)h_m+R_n(h_m)$. By definition,

$$N_s(h) = 0 \quad \text{for} \quad 0 \leqslant h \leqslant g_s-1,$$

so by (3.10),

$$\Delta_s(h_m) = -H_m \quad \text{for} \quad m \leqslant s \leqslant \nu-1. \tag{3.19}$$

By (3.13), it follows that

$$0 = \sum_{s=0}^{m-1}\Delta_s(h_m)-(\nu-m)H_m,$$

and applying the Cauchy-Schwarz inequality, we get

$$(\nu-m)^2H_m^2 \leqslant \Big\{\sum_{s=0}^{m-1}1\Big\}\Big\{\sum_{s=0}^{m-1}\Delta_s^2(h_m)\Big\}. \tag{3.20}$$

If $m \neq 0$, it follows from (3.19) and (3.20) that

$$\sum_{s=0}^{\nu-1}\Delta_s^2(h_m) \geqslant \{m^{-1}(\nu-m)^2+(\nu-m)\}H_m^2,$$

so by (3.14),

$$H_m^2 \leqslant \frac{m}{\nu(\nu-m)}\sum_{s=0}^{\nu-1}\Delta_s^2(h_m) = \frac{m}{\nu-m}\sum_{\psi\neq\chi_0}\Big|\sum_{x=1}^{h_m}\psi(x)\Big|^2,$$

and this is obviously true for $m = 0$ as well. By (3.17), $H_m \geqslant 0$, and the conclusion of the theorem follows.

In order to obtain specific estimates for g_m, we examine the sum in braces in Theorem (3.18). The method is as follows: for each positive divisor d of n, we collect the terms for which ψ has conductor d, then apply well-known estimates for character sums. The next three sections are devoted to facilitating this program. We shall first find the value of ν, then discuss various upper bounds for absolute values of character sums, and finally calculate the number of characters mod n having given conductor and exponent.

4. The value of ν.

In this section, we always write $\nu = \nu_k(n)$.

(4.1) LEMMA. *For* $n > 1$, $\nu_k(n) = \nu_k(p_1^{a_1}) \ldots \nu_k(p_r^{a_r})$.

Proof. By an easy application of the Chinese remainder theorem, $C(n)$ is isomorphic to the (external) direct product of $C(p_1^{a_1}), \ldots, C(p_r^{a_r})$ (see [11], p. 58). Hence $C_k(n)$ is isomorphic to the (external) direct product of $C_k(p_1^{a_1}), \ldots, C_k(p_r^{a_r})$. The lemma follows immediately.

(4.2) LEMMA. *If* p *is odd and* $a \geqslant 1$, *then* $\nu_k(p^a) = \big(k, \varphi(p^a)\big)$. *Also,* $\nu_k(2) = 1$, *and* $\nu_k(2^a) = (k, 2)(k, 2^{a-2})$ *for* $a \geqslant 2$.

Proof. Suppose that p is odd, and let g be a primitive root mod p^a. Then g^t is a kth power mod p^a iff the congruence $t \equiv mk \big(\text{mod}\ \varphi(p^a)\big)$ can be solved for m. As is well-known, this congruence is solvable iff $d = \big(k, \varphi(p^a)\big)$ divides t. Thus $C_k(p^a)$ is represented by the numbers g^{du}, $0 \leqslant u < \varphi(p^a)/d$, so $|C_k(p^a)| = \varphi(p^a)/d$ and $\nu_k(p^a) = d$.

If $a \geqslant 2$, then any odd number x satisfies a congruence of the form $x \equiv (-1)^y5^z (\text{mod}\ 2^a)$, where y and z are uniquely determined mod 2 and mod 2^{a-2}, respectively. Proceeding as before, it follows easily that $\nu_k(2^a) = (k, 2)(k, 2^{a-2})$.

(4.3) LEMMA. *For* $n > 1$,

$$\nu_k(n) = \prod_{j=\lambda}^{r}\{p_j^{\gamma_j-1}(k, p_j-1)\}.$$

Also, $\nu_k(n) \leqslant 2k^r$. (λ *and* γ_j *are defined in Section* 2.)

Proof. If $(b, c) = 1$, then $(ab, c) = (a, c)$. Applying this twice, we get

$$\big(k, \varphi(p_j^{a_j})\big) = p_j^{\min\{f_j, a_j-1\}}(k, p_j-1) = p_j^{\gamma_j-1}(k, p_j-1), \text{ if } p_j \text{ is odd}. \tag{4.4}$$

Now suppose that $p_1 = 2$. If $a_1 \geqslant 2$ and $f_1 = 0$, then $\nu_k(2^{a_1}) = 1$ by Lemma (4.2). If $a_1 = 1$, or if $a_1 \geqslant 2$ and $f_1 > 0$, it is easy to see that $\nu_k(2^{a_1}) = 2^{\gamma_1-1}$. The first conclusion follows, and the second is obvious after Lemmas (4.1) and (4.2).

5. Bounds for character sums.

Let χ be a character mod n, and let D be the set of positive divisors d of n with the following property: $\chi(x) = 1$ whenever $x \equiv 1 (\text{mod}\ d)$ and $(x, n) = 1$. The *conductor* of χ (which we denote by $K(\chi)$) is defined to be the smallest member of D. If $K(\chi) = n$, then χ is said to be *primitive* mod n (or to *belong properly to the modulus* n). (The basic properties of conductors and primitive characters are discussed in [15], pp. 479-494, [16], Vol. III, pp. 330-334, and [11], pp. 217-224.)

(5.1) LEMMA. *Let* χ *be a character* mod n, *let* d *be its conductor, and define* X *as follows: if* $(y, d) > 1$, *let* $X(y) = 0$; *if* $(y, d) = 1$, *choose* y' *so that*

$y' \equiv y \pmod{d}$ *and* $(y', n) = 1$, *and let* $X(y) = \chi(y')$. *Then* X *is a (well-defined) primitive character* mod d *(we refer to* X *as the primitive character* mod d *induced by* χ*). If* $q_1, \ldots, q_v$ *are the distinct primes dividing* n *but not* d *(*v *may be* 0*), then for* $h \geqslant 1$,

$$\Big|\sum_{y=1}^{h} \chi(y)\Big| \leqslant \sum_{c|q_1\ldots q_v} \Big|\sum_{1\leqslant y\leqslant h/c} X(y)\Big|. \tag{5.2}$$

Proof. We refer to [15]. The first assertion is proved on pp. 481-482, and (5.2) follows easily from the identity

$$\sum_{m=1}^{\infty} \chi(m) m^{-\sigma} = \Big\{\prod_{j=1}^{v} \big(1 - X(q_j) q_j^{-\sigma}\big)\Big\} \sum_{m=1}^{\infty} X(m) m^{-\sigma},$$

which is proved for $\sigma > 1$ on pp. 482-483.

The following lemma collects much of the known information on bounds for character sums. The rather odd phrasing of the lemma is for the purpose of convenience in obtaining our main results.

(5.3) Lemma. *Let* q, h, t *be any positive integers with* $q \geqslant 3$, *and suppose that* χ *is primitive* mod q. *Then for* $1 \leqslant z \leqslant 6$,

$$\Big|\sum_{y=1}^{h} \chi(y)\Big| < q^{(t+1)/4t^2} F_z(q, h, t), \tag{5.4}$$

where:

$$F_1(q, h, t) = \begin{cases} (3/4)\log q & \textit{if} \quad t = 1, \\ h & \textit{if} \quad t > 1; \end{cases} \tag{5.5}$$

$$F_2(q, h, t) = \begin{cases} (2\pi)^{-1}(\log q + 2\log\log q + A_2) & \textit{if} \quad t = 1, \\ h & \textit{if} \quad t > 1; \end{cases} \tag{5.6}$$

$$F_3(q, h, t) = \begin{cases} \pi^{-2}(\log q + 2\log\log q + A_3) & \textit{if} \quad t = 1 \ \textit{and}\ \chi(-1) = 1, \\ h & \textit{otherwise}; \end{cases} \tag{5.7}$$

$$F_4(q, h, t) = \begin{cases} A_4(\varepsilon) h^{1/2} q^{\varepsilon} & \textit{for any given}\ \varepsilon > 0,\ \textit{if}\ t = 2, \\ h & \textit{if} \quad t \neq 2; \end{cases} \tag{5.8}$$

$$F_5(q, h, t) = \begin{cases} A_5 h^{1-1/t} \log q & \textit{if} \quad q\ \textit{is prime}, \\ h & \textit{if} \quad q\ \textit{is not prime}; \end{cases} \tag{5.9}$$

$$F_6(q, h, t) = \begin{cases} A_6(\varepsilon, t) h^{1-1/t} q^{\varepsilon} & \textit{for any given}\ \varepsilon > 0,\ \textit{if}\ q\ \textit{is cubefree}, \\ h & \textit{if} \quad q\ \textit{is not cubefree}. \end{cases} \tag{5.10}$$

("Cubefree" means not divisible by the cube of any prime.) A_2, A_3, A_5 *are absolute constants, while* $A_4(\varepsilon)$, $A_6(\varepsilon, t)$ *depend only on the indicated arguments.*

Proof. (5.5), (5.6), and (5.7) applied to (5.4) give variants of the Pólya-Vinogradov inequality ([18], [21], [24], pp. 54-57, [20], [14]). For completeness, and also for the sake of a future application (see Section 8), we shall give a complete proof of (5.4) when $z = 1$.

Write $e(t)$ for $e^{2\pi i t}$, and define

$$\tau(q, \chi) = \sum_{y=1}^{q} \chi(y) e(y/q).$$

Since χ is primitive mod q, we have

$$|\tau(q, \chi)| = q^{1/2} \tag{5.11}$$

and

$$\sum_{y=1}^{q} \chi(y) e(my/q) = \bar{\chi}(m) \tau(q, \chi) \tag{5.12}$$

for any integer m (see [15], pp. 483-486 and 492-494 or [16], Vol. III, pp. 330-334). Using (5.12) (with χ replaced by $\bar{\chi}$), we have

$$\begin{aligned} \tau(q, \bar{\chi}) \sum_{m=a}^{b} \chi(m) &= \sum_{y=1}^{q-1} \bar{\chi}(y) \sum_{m=a}^{b} e(my/q) \\ &= \sum_{y=1}^{q-1} \bar{\chi}(y) \{e(ya/q) - e(y(b+1)/q)\} \{1 - e(y/q)\}^{-1}. \end{aligned}$$

Applying (5.11), it follows that

$$q^{1/2} \Big|\sum_{m=a}^{b} \chi(m)\Big| \leqslant \sideset{}{^*}\sum_{y=1}^{q-1} \csc(\pi y/q) = 2 \sum_{y=1}^{l} \csc(\pi y/q),$$

where $l = [(q-1)/2]$ and $*$ indicates that the term $y = q/2$ is omitted if q is even. Since

$$\csc(\pi y/q) \leqslant \int_{y-1/2}^{y+1/2} \csc(\pi u/q)\, du$$

for $1 \leqslant y \leqslant l$, we have

$$\begin{aligned} q^{1/2} \Big|\sum_{m=a}^{b} \chi(m)\Big| &\leqslant 2 \int_{1/2}^{q/2} \csc(\pi u/q)\, du \\ &= 2\pi^{-1} q \log\cot(\pi/4q) < 2\pi^{-1} q \log(4\pi^{-1} q). \end{aligned} \tag{5.13}$$

Now if $z = 1$ and q is 3 or 4, (5.4) is obvious.

If $q \geqslant 5$, then

$$(3\pi/8 - 1)\log q > (0.17)(1.6) > \log(4/\pi),$$

so by (5.13),

$$\Big|\sum_{m=a}^{b}\chi(m)\Big| < (3/4)q^{1/2}\log q,$$

which completes the proof of (5.4) when $z = 1$.

When $z = 2$ or $z = 3$, (5.4) can be obtained by a more complicated method using Fourier series. This was essentially carried out by Landau in [14], pp. 79-86. Landau's method yields the values of $F_2(q, h, t)$ and $F_3(q, h, t)$ given in (5.6) and (5.7), respectively, except that the constant $2^{-3/2}\pi^{-1}$ is obtained in (5.7) instead of the smaller constant π^{-2}. The latter constant can be obtained by using the Fourier series of $|\sin x|$ to improve Landau's estimate of

$$\sum_{m=1}^{n} m^{-1}|\sin mx|$$

(see [19], pp. 81 and 274).

Finally, if $z = 4, 5$, or 6, then (5.4) follows immediately from theorems of Burgess ([6], p. 524).

In (5.6) and (5.7), the respective constants $(2\pi)^{-1}$ and π^{-2} seem to be the best known. It is not hard to calculate explicit values for A_2 and A_3 using Landau's method. Burgess did not calculate admissible values of $A_4(\varepsilon)$, A_5, and $A_6(\varepsilon, t)$, and it is apparently not known how small they can be taken.

Using (5.2), each of the inequalities in Lemma (5.3) can easily be extended to arbitrary non-principal χ, only a change in the constant factor being required (see [14], pp. 85-86). This is not necessary for our purposes.

6. The number of characters mod n with given exponent and conductor.

(6.1) Definition. For each positive integer d, let $\Omega_k(d)$ denote the number of primitive characters mod d having exponent k.

(6.2) Lemma. *Let d be any positive divisor of n. Then there are exactly $\Omega_k(d)$ characters* mod n *having conductor d and exponent k.*

Proof. Let $C^*(n, d, k)$ be the set of χ mod n such that $K(\chi) = d$ and χ^k is principal. If $\chi \in C^*(n, d, k)$, define $f(\chi) = X$, the primitive character mod d induced by χ (see Lemma (5.1)). It is easy to see that f is a one-one mapping of $C^*(n, d, k)$ into $C^*(d, d, k)$; we shall show that f has image $C^*(d, d, k)$.

Suppose that X is any member of $C^*(d, d, k)$, and define $\chi(z)$ to be $X(z)$ if $(z, n) = 1$ and 0 otherwise. Clearly χ is a character mod n of exponent k. Let $d' = K(\chi)$. If $y \equiv 1 \pmod{d}$ and $(y, n) = 1$, then $\chi(y) = X(y) = 1$, so $d' | d$ (see [16], Vol. III, p. 331, Hilfssatz 4 or [11], p. 219, XI). On the other hand, suppose $y \equiv 1 \pmod{d'}$ and $(y, d) = 1$. Let $q_1, \ldots, q_v$ be the distinct primes dividing n but not d (v may be 0). Choose z such that $z \equiv y \pmod{d}$ and $z \equiv 1 \pmod{q_1 \ldots q_v}$. Then $z \equiv y \equiv 1 \pmod{d'}$ and $(z, n) = 1$, so $X(y) = X(z) = \chi(z) = 1$ (since $d' = K(\chi)$). Hence $d \leqslant d'$ (because $K(X) = d$), so $d = d'$ and $\chi \in C^*(n, d, k)$. Finally, it is clear that $f(\chi) = X$.

Hence $|C^*(n, d, k)| = |C^*(d, d, k)| = \Omega_k(d)$.

(6.3) Lemma. *For fixed k, $\Omega_k(n)$ is multiplicative, and*

$$\Omega_k(p^b) = \nu_k(p^b) - \nu_k(p^{b-1}) \quad \textit{for} \quad b \geqslant 1.$$

Proof. As we remarked in the proof of Lemma (3.9), the number of characters ψ mod n with exponent k is $\nu_k(n)$. From this it follows that

$$\nu_k(n) = \sum_{d|n} \Omega_k(d),$$

by Lemma (6.2). By the Möbius inversion formula,

$$\Omega_k(n) = \sum_{d|n} \mu(d)\nu_k(n/d). \tag{6.4}$$

Since $\Omega_k(n)$ is a "Dirichlet product" of multiplicative functions (cf. Lemma (4.1)), it must be multiplicative, and the formula for $\Omega_k(p^b)$ follows from (6.4).

7. The main results.

After Theorem (3.18), we need upper estimates for sums of the form

$$S = \sum_{\psi \neq \chi_0} \Big|\sum_{x=1}^{h} \psi(x)\Big|^2, \tag{7.1}$$

where ψ runs through the non-principal characters mod n having exponent k. The following lemma gives such estimates.

(7.2) Lemma. *Assume that $\nu = \nu_k(n) > 1$ (so $n \geqslant 3$ and $k \geqslant 2$). Let h and t be any positive integers, and let S be defined by (7.1). Then for $1 \leqslant z \leqslant 6$, we have*

$$S < 2^{2r-2} F_z^2(p_\lambda^{\gamma_\lambda} \ldots p_r^{\gamma_r}, h, t)T, \tag{7.3}$$

where

$$T = -1 + \prod_{j=\lambda}^{r} \big(1 + (k, p_j - 1)p_j^{\gamma_j\{1+(t+1)/2t^2\}-1}\big). \tag{7.4}$$

Furthermore,

$$T < 2^r \nu \Big(\prod_{j=\lambda}^{r} p_j^{\gamma_j}\Big)^{(t+1)/2t^2}. \tag{7.5}$$

(We are using the notation of Lemma (5.3). If $z = 3$, we can take F_z to have the first value given in (5.7) if $t = 1$ and if $\psi(-1) = 1$ for each $\psi \neq \chi_0$; otherwise $F_3 = h$.)

Proof. Temporarily fix $\psi \neq \chi_0$, and let $d = K(\psi)$, so $d|n$ and $d \geqslant 3$. Let Ψ be the primitive character mod d induced by ψ, and let $q_1, \ldots, q_v$ be the distinct primes dividing n but not d, so $0 \leqslant v \leqslant r-1$. By (5.2),

$$(7.6) \qquad \Big|\sum_{x=1}^{h} \psi(x)\Big| \leqslant \sum_{c|q_1\ldots q_v} \Big|\sum_{1 \leqslant x \leqslant h/c} \Psi(x)\Big|,$$

and by Lemma (5.3),

$$(7.7) \qquad \Big|\sum_{1 \leqslant x \leqslant h/c} \Psi(x)\Big| < d^{(t+1)/4t^2} F_z(d, [h/c], t) \leqslant d^{(t+1)/4t^2} F_z(d, h, t)$$

for $1 \leqslant z \leqslant 6$ (for the case $z = 3$, note that $\Psi(-1) = \psi(-1)$). Combining (7.6) and (7.7), we get

$$\Big|\sum_{x=1}^{h} \psi(x)\Big| < 2^{r-1} d^{(t+1)/4t^2} F_z(d, h, t).$$

Hence

$$\begin{aligned}(7.8) \qquad S &= \sum_{d|n, d>1} \sum_{\psi, K(\psi)=d} \Big|\sum_{x=1}^{h} \psi(x)\Big|^2 \\ &< \sum_{d|n, d>1} 2^{2r-2} d^{(t+1)/2t^2} F_z^2(d, h, t)\, \Omega_k(d) \\ &= \sum\nolimits_1 \Big\{2^{2r-2}(p_1^{b_1} \ldots p_r^{b_r})^{(t+1)/2t^2} F_z^2(p_1^{b_1} \ldots p_r^{b_r}, h, t) \prod_{j=1}^{r} \Omega_k(p_j^{b_j})\Big\},\end{aligned}$$

where Σ_1 indicates summation over all r-tuples $b_1, \ldots, b_r$ with $0 \leqslant b_j \leqslant a_j$ (for all j) and some $b_j \neq 0$, and where we have applied Lemmas (6.2) and (6.3) (if $z = 3$, F_z is interpreted as in the statement of the present lemma).

Applying Lemmas (6.3) and (4.2), as well as the first equation in (4.4), it is easy to see that if p_j is odd, then

$$(7.9) \qquad \Omega_k(p_j^{b_j}) \leqslant \begin{cases} 1 & \text{if} \quad b_j = 0, \\ p_j^{b_j-1}(k, p_j-1)(1-p_j^{-1}) & \text{if} \quad 1 \leqslant b_j \leqslant f_j+1, \\ 0 & \text{if} \quad b_j > f_j+1. \end{cases}$$

Likewise, if $p_1 = 2$ and k is odd, then

$$(7.10) \qquad \Omega_k(2^{b_1}) = \begin{cases} 1 & \text{if} \quad b_1 = 0, \\ 0 & \text{if} \quad b_1 \geqslant 1, \end{cases}$$

while if k is even,

$$(7.11) \qquad \Omega_k(2^{b_1}) = \begin{cases} 1 & \text{if} \quad b_1 = 0, \\ 0 & \text{if} \quad b_1 = 1 \text{ or } b_1 > f_1+2, \\ 2^{b_1-2} & \text{if} \quad 2 \leqslant b_1 \leqslant f_1+2. \end{cases}$$

Recalling the definitions of γ_j and $\lambda = \lambda_k(n)$ (see Section 2), and applying (7.9), (7.10), and (7.11), we see that the sum $\sum_1$ in (7.8) can be written in the form

$$(7.12) \qquad 2^{2r-2} \sum\nolimits_2 \Big\{F_z^2(p_\lambda^{b_\lambda} \ldots p_r^{b_r}, h, t) \prod_{j=\lambda}^{r} \big(p_j^{b_j(t+1)/2t^2}\, \Omega_k(p_j^{b_j})\big)\Big\},$$

where Σ_2 indicates summation over all $b_\lambda, \ldots, b_r$ with $0 \leqslant b_j \leqslant \gamma_j$ (for all j) and some $b_j \neq 0$. It is clear that the quantity in (7.12) does not exceed

$$\begin{aligned} &2^{2r-2} F_z^2(p_\lambda^{\gamma_\lambda} \ldots p_r^{\gamma_r}, h, t) \sum\nolimits_2 \prod_{j=\lambda}^{r} \{p_j^{b_j(t+1)/2t^2}\, \Omega_k(p_j^{b_j})\} \\ &\qquad = 2^{2r-2} F_z^2(p_\lambda^{\gamma_\lambda} \ldots p_r^{\gamma_r}, h, t) \Big\{-1 + \prod_{j=\lambda}^{r} \sum_{b=0}^{\gamma_j} \big(p_j^{b(t+1)/2t^2}\, \Omega_k(p_j^{b})\big)\Big\}. \end{aligned}$$

Suppose that p_j is odd. Using (7.9), a routine calculation gives

$$(7.13) \qquad \sum_{b=0}^{\gamma_j} p_j^{b(t+1)/2t^2}\, \Omega_k(p_j^{b}) < 1 + (k, p_j-1)\, p_j^{\gamma_j\{1+(t+1)/2t^2\}-1},$$

and an application of (7.11) shows that (7.13) holds also when k is even and $p_j = p_1 = 2$. Combining (7.8) and (7.13) with (7.12) (and the result immediately following it), we get (7.3). Finally, we note that

$$T < \prod_{j=\lambda}^{r} \{2(k, p_j-1)\, p_j^{\gamma_j\{1+(t+1)/2t^2\}-1}\},$$

so that (7.5) follows from Lemma (4.3).

In applying (7.3) and (7.5), it is useful to note the obvious inequality

$$(7.14) \qquad \prod_{j=\lambda}^{r} p_j^{\gamma_j} \leqslant n.$$

There is equality in (7.14) if, for example, n is squarefree and $\lambda = 1$.

We can now derive (1.5), which is trivial if $m = 0$. If $1 \leqslant m \leqslant \nu-1$ and $h = g_m(n, k)-1$, then by Theorem (3.18) and (3.15),

$$h \leqslant \frac{n}{\varphi(n)} \Big\{\Big(\frac{m}{\nu-m}\Big)^{1/2} S^{1/2} + 2^{r-1}\Big\},$$

where S is defined by (7.1). Applying Lemma (7.2) with $z = t = 1$ and using (5.5), we obtain (1.5) by an easy calculation.

If $t = 1$, then (7.13) can be improved slightly. Using (7.9) and (7.11), we find that

$$\sum_{b=0}^{\gamma_j} p_j^b \, \Omega_k(p_j^b) \leqslant 1 + (k, p_j - 1)(p_j^{2\gamma_j} - 1)(p_j + 1)^{-1} \tag{7.15}$$

if p_j is odd, or if $p_j = 2$ and k is even. This fact is applied in the proof of the next theorem, which is of particular importance for the application mentioned in Section 8.

(7.16) Theorem. *Let p be odd, $a \geqslant 1$, and write $k = p^f k_0$, where $p \nmid k_0$. Also write $\gamma = \min\{a, f+1\}$ and $\delta = (k, p-1) = (k_0, p-1)$. Then for $0 \leqslant m \leqslant \nu_k(p^a) - 1 = p^{\gamma-1}\delta - 1$, we have*

$$g_m(p^a, k) \leqslant 1 + \{m\delta/(p^{\gamma-1}\delta - m)\}^{1/2} \gamma p^{\gamma - 1/2} \log p.$$

Proof. Write $h = g_m(p^a, k) - 1$, and let $n = p^a$ in Theorem (3.18). By (3.11), $R_n(h) = h/p - [h/p] \geqslant 0$, so

$$h \leqslant \frac{p}{p-1} \left(\frac{m}{\nu - m}\right)^{1/2} S^{1/2}, \tag{7.17}$$

where $\nu = \nu_k(p^a) = p^{\gamma-1}\delta$ (by (4.4)) and S is given by (7.1). If $\nu = 1$, there is nothing to prove. Otherwise, we can combine (7.8), (7.12) (and the result immediately following it), (7.15), and (7.17) (taking $r = z = \lambda = t = 1$, $p_1 = p$, $\gamma_1 = \gamma$) to get

$$h \leqslant \left\{\frac{3p}{4(p-1)} (1 + p^{-1})^{-1/2}\right\} \left(\frac{m\delta}{\nu - m}\right)^{1/2} \gamma p^{\gamma - 1/2} \log p \leqslant \left(\frac{m\delta}{\nu - m}\right)^{1/2} \gamma p^{\gamma - 1/2} \log p.$$

The estimate of Theorem (7.16) is sometimes weaker than the trivial estimate $g_m(p^a, k) < p^a$ (for example, suppose $\gamma = a \geqslant 2$ and $m = p^{\gamma-1}\delta - 1$). Vinogradov's classical result (1.1) follows on taking $a = 1$ in Theorem (7.16).

We shall not write down explicitly the estimates for $g_m(n, k)$ which can be obtained by combining Theorem (3.18), Lemma (5.3), and Lemma (7.2) when $z = 2$ or $z = 3$. It is interesting to note that when k is odd, we can apply the non-trivial part of (5.7) to Lemma (7.2), for in this case, the fact that $\psi(-1) = 1$ for each ψ follows from the equation $\psi^k(-1) = \chi_0(-1) = 1$.

We now apply the estimates of Burgess given in (5.8) and (5.10) to obtain inequalities for $g_m(n, k)$.

(7.18) Theorem. *Let $\varepsilon > 0$, let t be any positive integer, and suppose $\nu > 1$. If $t = 1$ or $t = 2$ or $\max\{\gamma_\lambda, \ldots, \gamma_r\} \leqslant 2$, then*

$$g_m(n, k) < A_8(\varepsilon, t) \left(\frac{n}{\varphi(n)} 2^{3r/2 - 1}\right)^t \left(\frac{m\nu}{\nu - m}\right)^{t/2} \left(\prod_{j=\lambda}^{r} p_j^{\gamma_j}\right)^{(t+1)/4t + \varepsilon t} \tag{7.19}$$

for $1 \leqslant m \leqslant \nu - 1$, where $A_8(\varepsilon, t)$ depends only on ε and t.

Proof. Let $h = g_m(n, k) - 1$, and let S be given by (7.1). By (7.3), (7.5), and (5.5), (5.8), or (5.10), we can say that

$$S^{1/2} < A_7(\varepsilon, t) 2^{3r/2 - 1} \nu^{1/2} h^{1 - 1/t} \left(\prod_{j=\lambda}^{r} p_j^{\gamma_j}\right)^{(t+1)/4t^2 + \varepsilon} \tag{7.20}$$

for any $\varepsilon > 0$, if $t = 1$ or $t = 2$ or $\max\{\gamma_\lambda, \ldots, \gamma_r\} \leqslant 2$. Using Theorem (3.18) and (3.15), we get the result with a little computation.

If $p_\lambda^{\gamma_\lambda} \ldots p_r^{\gamma_r}$ is prime, then Theorem (7.18) can be improved slightly by using (5.9) instead of (5.8) and (5.10).

We shall now show how to obtain (1.6), (1.7), (1.8), and (1.9), which generalize and strengthen certain results of Davenport, Erdös, and Jordan (cf. (1.2) and the comments after it).

(7.21) Theorem. *For any $\varepsilon > 0$, we have (1.6). Furthermore, if $\max\{\gamma_\lambda, \ldots \ldots, \gamma_r\} \leqslant 2$ (e.g., if n is cubefree, or if $2 \nmid (n, k)$ and k is squarefree), then (1.7) holds. In each case, the constant implied by the O-notation depends only on k and ε.*

Proof. By [10], Chap. XVIII, Theorems 315 and 327, we have

$$2^r \leqslant d(n) < A_9(\varepsilon) n^\varepsilon, \tag{7.22}$$

where $d(n)$ is the number of positive divisors of n, and

$$n/\varphi(n) < A_{10}(\varepsilon) n^\varepsilon. \tag{7.23}$$

Combining these results with (7.19), (7.14), and Lemma (4.3), we find that if $t = 2$ or $\max\{\gamma_\lambda, \ldots, \gamma_r\} \leqslant 2$, then

$$g_{\nu-1}(n, k) < A_{11}(\varepsilon, t)(2^{3/2} k)^{rt} n^{(t+1)/4t + 2\varepsilon t} < A_{12}(k, \varepsilon, t) n^{(t+1)/4t + 3\varepsilon t}.$$

Taking $t = 2$, we get (1.6). If $\max\{\gamma_\lambda, \ldots, \gamma_r\} \leqslant 2$, then there is no restriction on t, and we can take t to be the smallest integer $\geqslant 2^{-1}(3\varepsilon)^{-1/2}$. Thus (1.7) follows.

Before proving (1.8) and (1.9), we need to establish the following result, which is of interest in itself. (For the notation, see Lemma (3.9).)

(7.24) Theorem. *Let $0 \leqslant s \leqslant \nu - 1$ and $1 \leqslant h \leqslant n$, let $\varepsilon > 0$, and let t be any positive integer. If $t = 1$ or $t = 2$ or $\max\{\gamma_\lambda, \ldots, \gamma_r\} \leqslant 2$, then*

$$|N_s(h) - (\nu n)^{-1} \varphi(n) h| < A_{13}(\varepsilon, t) h^{1 - 1/t} n^{(t+1)/4t^2 + \varepsilon}.$$

Proof. By (3.10) and (3.15),

$$|N_s(h)-(\nu n)^{-1}\varphi(n)h| < \nu^{-1}\{2^{r-1}+|\varDelta_s(h)|\}. \tag{7.25}$$

Applying the Cauchy-Schwarz inequality to (3.12), we get

$$|\varDelta_s(h)| \leqslant \Big(\sum_{\psi\neq\chi_0} 1\Big)^{1/2} S^{1/2} = (\nu-1)^{1/2}S^{1/2}, \tag{7.26}$$

where S is given by (7.1). If $\nu = 1$, then $|\varDelta_s(h)| = 0$ by (7.26), and the result follows from (7.25) and (7.22). Suppose that $\nu > 1$. If $t = 1$ or $t = 2$ or $\max\{\gamma_\lambda, \ldots, \gamma_r\} \leqslant 2$, then (7.20) holds for any $\varepsilon > 0$ and any h with $1 \leqslant h \leqslant n$. Applying (7.14), (7.22), and (7.26), we get the result from (7.25).

We will now show how to obtain a slight improvement in Theorem (7.21) under the additional assumption that the number of distinct prime factors of n does not exceed a bound depending only on k.

(7.27) THEOREM. *Suppose that $r \leqslant r_k$, where r_k depends only on k. Then there exists a (very small) positive number δ, depending only on k, such that (1.8) holds for each $\varepsilon > 0$, and if $\max\{\gamma_\lambda, \ldots, \gamma_r\} \leqslant 2$, then (1.9) holds for each $\varepsilon > 0$. In each case, the constant implied by the O-notation depends only on k and ε.*

Proof. Let μ denote the total number of prime factors of $\nu = \nu_k(n)$ (multiple prime factors counted according to their multiplicity). Let Q_j denote the jth prime ($Q_1 = 2$), and define

$$D_k = \prod_{j\leqslant r_k}(1-Q_j^{-1}), \qquad E_k = 2k^{r_k},$$
$$F_k = (D_k/2E_k^2)^{E_k/2-1}(E_k+1)^{-E_k/2}.$$

Since $r \leqslant r_k$, it follows that for $n > 1$,

$$n^{-1}\varphi(n) = \prod_{j=1}^{r}(1-p_j^{-1}) \geqslant D_k. \tag{7.28}$$

By Lemma (4.3),

$$\nu \leqslant E_k. \tag{7.29}$$

We define

$$\delta_1 = (E_k+1)^{-1}, \qquad \delta_{s+1} = D_k\delta_s^2(2E_k^2)^{-1} \quad \text{for} \quad 1 \leqslant s \leqslant \mu.$$

Clearly $1 > \delta_1 > \ldots > \delta_{\mu+1} > 0$, and since $\mu \leqslant \log\nu/\log 2$, it follows from (7.29) that

$$\delta_\mu \geqslant F_k. \tag{7.30}$$

We now define the δ of the theorem by the equation

$$\delta = D_kF_k^2(2E_k+1)^{-1}, \tag{7.31}$$

so $\delta < F_k \leqslant \delta_\mu$, and we take $x = n^{(t+1)/4t+2\varepsilon t}$, where ε is any given positive real number and t is chosen as follows: if $\max\{\gamma_\lambda, \ldots, \gamma_r\} \leqslant 2$, t is the smallest integer $\geqslant (8\varepsilon)^{-1/2}$; otherwise $t = 2$. Under our standing assumption that $r \leqslant r_k$, we shall show that $g_{\nu-1}(n, k) < x^{1-\delta}$ for k fixed and $n > n_0(k, \varepsilon)$. The method of proof is indirect: assuming that A is any given coset of $C_k(n)$ and that every positive member of A is $\geqslant x^{1-\delta}$, we shall deduce a contradiction.

Let $P_s = x^{\delta_s}$ for $1 \leqslant s \leqslant \mu+1$, so $P_1 > P_2 > \ldots$ The primes $\leqslant P_s$ and not dividing n belong to certain cosets of $C_k(n)$, and these cosets generate a subgroup of the quotient group $C(n)/C_k(n)$. We now follow the argument of Davenport and Erdös ([8], pp. 258-261), with occasional changes in their notation (in particular, their k is replaced by our ν, their ν by our μ). We find that there is some s, $1 \leqslant s \leqslant \mu$, such that if we write $y = x^{1-\delta-\nu\delta_{s+1}}$ and use Theorem (7.24), we can replace the inequality (21) of [8] by

$$\begin{aligned}\sideset{}{^*}\sum_{y\leqslant q\leqslant x} q^{-1} &> (\nu n)^{-1}\varphi(n) - A_{14}(\varepsilon)x^{-1/t}n^{(t+1)/4t^2+\varepsilon} \\ &= (\nu n)^{-1}\varphi(n) - A_{14}(\varepsilon)n^{-\varepsilon},\end{aligned} \tag{7.32}$$

where * indicates summation over those integers q all of whose prime factors are $\geqslant P_s$. The sum on the left in (7.32) can be estimated from above as in [8], and this leads to the inequality

$$(\nu n)^{-1}\varphi(n) - A_{14}(\varepsilon)n^{-\varepsilon} < (\delta+\nu\delta_{s+1})\,\delta_s^{-2} + O(1/\log n),$$

where the constant implied by O depends only on k. Using the results (7.28) to (7.31) and the fact that $\delta_s \geqslant \delta_\mu$, we get

$$\begin{aligned}D_kE_k^{-1} &< \delta\delta_\mu^{-2} + \nu\delta_{s+1}\delta_s^{-2} + O(1/\log n) \\ &\leqslant D_k(2E_k+1)^{-1} + D_k(2E_k)^{-1} + O(1/\log n),\end{aligned}$$

where the implied constant depends only on k and ε. This gives a contradiction if k and ε are fixed and $n > n_0(k, \varepsilon)$.

8. An application. Let $\varGamma^*(k)$ denote the smallest s with the following property: for each prime p, each $h \geqslant 1$, and each set of integers $c_1, \ldots, c_s$, the congruence

$$c_1x_1^k + c_2x_2^k + \ldots + c_sx_s^k \equiv 0 \pmod{p^h}$$

has a solution with some x_j not divisible by p. Define

$$\sigma = \limsup\{\varGamma^*(k)(k\log k)^{-1}\},$$

where the lim sup is taken over odd k tending to $+\infty$. Chowla and Shimura have shown that

$$1/\log 2 \leqslant \sigma \leqslant 2/\log 2. \tag{8.1}$$

Using Theorem (7.16) and a number of other lemmas, the author showed in [17] that

$$\sigma \leqslant 3/\log 4. \tag{8.2}$$

It seems likely that $\sigma = 1/\log 2$, but this may be very difficult to prove. It is interesting that the proof of Theorem (7.16) used a version of the relatively elementary Pólya-Vinogradov inequality for character sums, whereas the very deep inequalities of Burgess yield estimates (such as (7.19)) for $g_m(p^a, k)$ which, although stronger when p^a is large, seem to be ineffective in obtaining upper bounds for σ.

Details of the proof of (8.2), as well as other facts about $\Gamma^*(k)$, will be presented in forthcoming papers.

Note added January, 1968. An easy application of (5.5) to (5.2) shows that the left-hand side of (5.4) is less than $(\frac{1}{2}\sqrt{6})q^{1/2}\log q$ whenever χ is non-principal mod q (cf. [14], pp. 85-86). Applying this result directly to Theorem (3.18) (without using the methods of Section 7), we find that the factor $2^{3r/2}$ in (1.5) can be replaced by an absolute constant, e.g., $(2+3\sqrt{5})/\sqrt{30}$.

References

[1] N. C. Ankeny, *The least quadratic non-residue*, Ann. of Math. 55 (1952), pp. 65-72.

[2] M. B. Barban, *The "Large Sieve" method and its applications in the theory of numbers*, Russian Math. Surveys 21 (1966), pp. 49-104.

[3] D. A. Burgess, *The distribution of quadratic residues and non-residues*, Mathematika 4 (1957), pp. 106-112.

[4] — *On character sums and primitive roots*, Proc. London Math. Soc. (3) 12 (1962), pp. 179-192.

[5] — *On character sums and L-series*, Proc. London Math. Soc. (3) 12 (1962), pp. 193-206.

[6] — *On character sums and L-series, II*, Proc. London Math. Soc. (3) 13 (1963), pp. 524-536.

[7] — *A note on the distribution of residues and non-residues*, J. London Math. Soc. 38 (1963), pp. 253-256.

[8] H. Davenport and P. Erdös, *The distribution of quadratic and higher residues*, Pub. Math. Debrecen 2 (1951-1952), pp. 252-265.

[9] M. Hall, Jr., *The Theory of Groups*, New York 1959.

[10] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, 3rd ed., Oxford 1954.

[11] H. Hasse, *Vorlesungen über Zahlentheorie*, 2nd ed., Berlin 1964.

[12] J. H. Jordan, *The Distribution of k-th Power Non-Residues*, Ph. D. Thesis, University of Colorado, 1962.

[13] — *The distribution of cubic and quintic non-residues*, Pacific J. Math. 16 (1966), pp. 77-85.

[14] E. Landau, *Abschätzungen von Charaktersummen, Einheiten und Klassenzahlen*, Göttinger Nachr. (Phys. -Math. Klasse) (1918), pp. 79-97.

[15] E. Landau, *Handbuch der Lehre von der Verteilung der Primzahlen*, Vol. I, New York 1953.

[16] — *Vorlesungen über Zahlentheorie*, New York 1955.

[17] K. K. Norton, *On Homogeneous Diagonal Congruences of Odd Degree*, Ph. D. Thesis, University of Illinois, 1966.

[18] G. Pólya, *Über die Verteilung der quadratischen Reste und Nichtreste*, Göttinger Nachr. (Phys.-Math. Klasse) (1918), pp. 21-29.

[19] — and G. Szegö, *Aufgaben und Lehrsätze aus der Analysis*, Vol. II, Berlin 1925.

[20] I. Schur, *Einige Bemerkungen zu der vorstehenden Arbeit des Herrn G. Pólya*, Göttinger Nachr. (Phys.-Math. Klasse) (1918), pp. 30-36.

[21] I. M. Vinogradov, *Sur la distribution des résidus et des non-résidus des puissances*, J. Phys.-Math. Soc. Perm 1 (1918), pp. 94-96.

[22] — *On a general theorem concerning the distribution of the residues and non-residues of powers*, Trans. Amer. Math. Soc. 29 (1927), pp. 209-217.

[23] — *On the bound of the least non-residue of n-th powers*, Trans. Amer. Math. Soc. 29 (1927), pp. 218-226.

[24] — *Selected Works*, Moscow 1952.

Erratum. On p. 173, the statement in lines 10 to 13 may not be true if $z = 5$ or $z = 6$ and $p_\lambda^{\gamma_\lambda} \ldots p_r^{\gamma_r}$ is not prime or not cubefree, respectively. However, the lemma is obvious in these cases, since $T \geqslant \nu$ by Lemma (4.3) and trivially $S \leqslant (\nu - 1)h^2$

UNIVERSITY OF COLORADO
Boulder, Colorado

Reçu par la Rédaction le 1. 12. 1967