ACTA ARITHMETICA
XVII (1970)

A refinement of a theorem of Gerst on power residues

by

A. Schinzel (Warsaw)

Let n be a positive integer, a rational, $P(n, a)$ the set of primes p such that the congruence $x^n \equiv a \bmod p$ is soluble. Under the assumption that a, b are non-zero integers I. Gerst in the preceding paper [2] gave necessary and sufficient condition for the equality $P(n, a) = P(n, b)$ understood in the sense that the set $P(n, a) \dot{-} P(n, b)$ has Dirichlet density zero. The following theorem gives a necessary and sufficient condition that $P(n, a) \setminus P(n, b)$ has density zero (the natural density exists).

Theorem 1. *Let a, b non-zero rationals. $P(n, a) \setminus P(n, b)$ has density zero if and only if there exists an integer t such that either*

(i) $$ba^t = d^n \text{ for some rational } d,$$

or

(ii) $$n \equiv 0 \bmod 8, \quad ba^t = 2^{n/2} d^n \text{ for some rational } d,$$

or

(iii) $$n \equiv 4 \bmod 8, \quad a = -c^2, \quad ba^t = -2^{n/2} d^n \text{ for some rational } c, d.$$

The deduction of Gerst theorem from the above result is mechanical and is left to the reader. It is only of interest that if we assume $P(n, a) = P(n, b)$ the case (iii) disappears. The proof of Theorem 1 is based on a result of Elliott [1] and the theory of cyclotomy. It would be preferable to have a proof which would generalize to algebraic number fields.

As an application we prove

Theorem 2. *Let a, b non-zero rationals. If the congruence $a^x \equiv b \bmod p$ is soluble for almost all primes p then $b = a^k$ with integer k.*

This is a generalization of a theorem of the writer [4] concerning the case a, b integers, $a > 0$. The proof given in [4] extends to the general case but the paper abounds in misprints which make it difficult to understand. The case a integer, b rational has been treated but not completely disposed of by G. Jaeschke and E. Trost [3].

LEMMA 1. *The density of primes $p \equiv 1 \bmod m$ such that each congruence $x^m \equiv a_i \pmod{p}$ $(a_i \neq 0,\ 1 \leqslant i \leqslant r)$ is soluble equals*

$$d(m, a_1, \ldots, a_r) = \frac{1}{\varphi(m)\, m^r} \sum_{\substack{\nu_1=1 \\ a_1^{\nu_1}\ldots a_r^{\nu_r}=\delta^m,\ \delta\in Q(\zeta_m)}}^{m} \cdots \sum_{\nu_r=1}^{m} 1.$$

Proof. This is a special case of Theorem 1 of Elliott [1].

LEMMA 2. *The density of primes p such that $(p-1, n) = k$ and each congruence $x^n \equiv a_i \pmod{p}$, $(a_i \neq 0,\ 1 \leqslant i \leqslant r)$ is soluble equals*

$$\sum_{t \mid \frac{n}{k}} \mu(t)\, d(kt, a_1^t, \ldots, a_r^t).$$

Proof. Let for a given x, $k \mid n$ and $u \mid \frac{n}{k}$, $f(u, x)$ be the number of primes $p \leqslant x$ such that $(p-1, n) = n/u$ and each congruence $x^k \equiv a_i \pmod{p}$ $(1 \leqslant i \leqslant r)$ is soluble. Then for any $v \,\Big|\, \frac{n}{k}$

$$\frac{\log x}{x} \sum_{u \mid v} f(u, x) = d\left(\frac{n}{v};\ a_1^{n/vk}, a_2^{n/vk}, \ldots, a_r^{n/vk}\right) + o(1).$$

It follows by the Möbius inversion formula that for any $u \,\Big|\, \frac{n}{k}$

$$\frac{\log x}{x} f(u, x) = \sum_{t \mid u} \mu(t)\, d\left(\frac{nt}{u};\ a_1^{nt/uk}, \ldots, a_r^{nt/uk}\right) + o(1)$$

and in particular

$$\frac{\log x}{x} f\left(\frac{n}{k}, x\right) = \sum_{t \mid \frac{n}{k}} \mu(t)\, d(kt;\ a_1^t, \ldots, a_r^t) + o(1).$$

However, under the condition $(p-1, n) = k$ solubility of $x^k \equiv a_i \pmod{p}$ is equivalent to solubility of $x^n \equiv a_i \pmod{p}$ and the proof is complete.

LEMMA 3. *Let d be a rational integer, $k(d)$ its square-free kernel. $\sqrt{d} \in Q(\zeta_m)$ if and only if $k(d) \mid m$ and either $m \not\equiv 0 \bmod 4$, $k(d) \equiv 1 \bmod 4$ or $m \equiv 4 \bmod 8$, $k(d) \equiv 1 \bmod 2$ or $m \equiv 0 \bmod 8$.*

Proof. This is an equivalent formulation of Lemma 5 of [2].

LEMMA 4. *A number C is rational of the form γ^m with $\gamma \in Q(\zeta_m)$ if and only if either $m \equiv 1 \bmod 2$, $C = c^m$, $c \in Q$ or $m \equiv 0 \bmod 2$, $C = c^{m/2}$, $c \in Q$, $\sqrt{c} \in Q(\zeta_m)$ or $m \equiv 4 \bmod 8$, $C = -2^{m/2} c^{m/2}$, $c \in Q$, $\sqrt{c} \in Q(\zeta_m)$.*

Proof. In order to prove the necessity of the condition set $C = \eta C_1^t$, where $\eta = \pm 1$, C_1 is a positive integer, not a power. If $\eta = 1$, then

$|C_1^{t/m}| \in Q(\zeta_m)$ and since all the subfields of $Q(\zeta_m)$ are normal, $C_1^{t/m}$ has only real values and $m/(t, m) \leqslant 2$.

If $m \equiv 1 \bmod 2$, $m \mid t$ and we take $c = C_1^{t/m}$, if $m \equiv 0 \bmod 2$ we take $c = C_1^{2t/m}$. If $\eta = -1$, $\zeta_{2m} |C_1^{t/m}| \in Q(\zeta_m)$. If $m \equiv 1 \bmod 2$, $|C_1^{t/m}| \in Q(\zeta_m)$ and as before $m \mid t$, $c = -C_1^{t/m}$. If $m \equiv 0 \bmod 2$, $|C_1^{t/m}| \notin Q(\zeta_m)$, since otherwise $\zeta_{2m} \in Q(\zeta_m)$. It follows that $m \nmid t$. On the other hand, $|C_1^{t/m}| \in Q(\zeta_{2m})$, thus $t \equiv m/2 \bmod m$. Therefore, we have $\sqrt{C_1} \notin Q(\zeta_m)$, $\sqrt{C_1} \in Q(\zeta_{2m})$. By Lemma 3 either $m \equiv 2 \bmod 4$, $k(C_1) \equiv 3 \bmod 4$ or $m \equiv 4 \bmod 8$, $k(C_1) \equiv 0 \bmod 2$. In the former case $\sqrt{-C_1} \in Q(\zeta_m)$ and we take $c = -C_1^{2t/m}$, in the latter case $\sqrt{C_1/2} \in Q(\zeta_m)$ and we take $c = \frac{1}{2} C_1^{2t/m}$.

In order to show the sufficiency of the condition we take $\gamma = c$, $\gamma = \sqrt{c}$ or $\gamma = (1+i)\sqrt{c}$ in the first, second or third case, respectively.

LEMMA 5. *Let $e_m(d)$ be the least positive exponent such that $d^e = \gamma^m$ with $\gamma \in Q(\zeta_m)$. If $a = \eta a_1^l$, where $\eta = \pm 1$, a_1 is a positive integer, not a power and $t \equiv 1 \bmod 2$ then*

$$e_m(a^t) = \frac{(m, l)}{(m, lt)}\, e_m(a).$$

Proof (due to I. Gerst) (¹). Let $m_1 = \dfrac{m}{(m, 2l)}$, $l_1 = \dfrac{2l}{(m, 2l)}$. Then it is clear that

$$e_m(a) = m_1 \text{ or } 2m_1.$$

Indeed, if m is odd it follows from Lemma 4 immediately that $e_m(a) = m_1$, if m is even $\eta^e a_1^{le} = c^{m/2}$ or $-(2c)^{m/2}$ requires e to be a multiple of m_1 and $a^{2m_1} = (a_1^{2l_1})^{m/2}$ with $\sqrt{a_1^{2l_1}} \in Q(\zeta_m)$. Using the characterization of the rationals γ^m with $\gamma \in Q(\zeta_m)$ given in Lemma 4 we find easily

$$e_m(a) = \begin{cases} m_1 & \text{if (1) or (2) or (3) or (4),} \\ 2m_1 & \text{otherwise,} \end{cases}$$

where (1), (2), (3), (4) are the following conditions

$$m \equiv 1 \bmod 2, \tag{1}$$

$$\eta^{m_1} = 1, \quad \sqrt{a_1^{l_1}} \in Q(\zeta_m), \tag{2}$$

$$m \equiv 2 \bmod 4, \quad \eta = -1, \quad \sqrt{-a_1^{l_1}} \in Q(\zeta_m), \tag{3}$$

$$m \equiv 4 \bmod 8, \quad \eta^{m_1} = -1, \quad \sqrt{2a_1^{l_1}} \in Q(\zeta_m). \tag{4}$$

(¹) The writer's original proof was rather involved.

Now if a is replaced by a^t (t odd), l is replaced by lt, η, a_1 and the parity of m_1 and l_1 are unchanged. Therefore the conditions (1)–(4) remain the same and we get

$$\frac{e_m(a^t)}{e_m(a)} = \frac{(m, 2l)}{(m, 2lt)} = \frac{(m, l)}{(m, lt)},$$

q.e.d.

Proof of Theorem 1. It is clearly sufficient to prove the theorem for a, b integers. Assume that $P(n, a) \setminus P(n, b)$ has density zero. It follows from Lemmata 1 and 2 that for each $k|n$

$$\sum_{t|\frac{n}{k}} \frac{\mu(t)}{\varphi(kt)kt} \sum_{\substack{\nu=1 \\ a^{\nu t}=\gamma_1^{kt},\ \gamma_1 \in Q(\zeta_{kt})}}^{k} 1 = \sum_{t|\frac{n}{k}} \frac{\mu(t)}{\varphi(kt)(kt)^2} \sum_{\substack{\nu_1=1 \\ a^{\nu_1 t} b^{\nu_2 t}=\gamma_2^{kt},\ \gamma_2 \in Q(\zeta_{kt})}}^{kt} \sum_{\nu_2=1}^{kt} 1.$$

Clearly, the inner sum on the left hand side equals

$$\frac{kt}{e_{kt}(a^t)}$$

and the inner (double) sum on the right hand side equals

$$\frac{(kt)^2}{e_{kt}(a^t) f_{kt}(a^t, b^t)},$$

where $f_m(d_1, d_2)$ is the least positive exponent e such that for suitable integer ν: $d_1^\nu d_2^e = \gamma^m$ with $\gamma \in Q(\zeta_m)$. Thus we get for each $k|n$

$$(5) \qquad \sum_{t|\frac{n}{k}} \frac{\mu(t)}{\varphi(kt)} \cdot \frac{1}{e_{kt}(a^t)} \left(1 - \frac{1}{f_{kt}(a^t, b^t)}\right) = 0.$$

Applying (5) with $k = n$, we get

$$f_n(a, b) = 1,$$

that is for suitable ν_0

$$a^{\nu_0} b = \gamma^n, \qquad \gamma \in Q(\zeta_n).$$

By Lemma 4 we have either

$$n \text{ odd}, \qquad a^{\nu_0} b = c^n, \qquad c \in Q$$

or

$$(6) \qquad 2|n, \qquad a^{\nu_0} b = c^{n/2}, \qquad c \in Q$$

or

$$(7) \qquad n \equiv 4 \bmod 8, \qquad a^{\nu_0} b = -2^{n/2} c^{n/2}, \qquad c \in Q.$$

In the first case (i) holds. Consider the case (6). Clearly if $2\left|\frac{n}{k}\right.$, then

$$f_{kt}(a^t, b^t) = 1.$$

If $2 \nmid \frac{nt}{k}$, then

$$(8) \qquad f_{kt}(a^t, b^t) = \begin{cases} 1 & \text{if for some } \nu\text{: } a^\nu c^{kt/2} = \gamma^{kt},\ \gamma \in Q(\zeta_{kt}), \\ 2 & \text{otherwise.} \end{cases}$$

Indeed, if $a^\nu c^{kt/2} = \gamma^{kt}$, $\gamma \in Q(\zeta_{kt})$; then $a^{2\nu} = \gamma_1^{kt}$, $\gamma_1 \in Q(\zeta_{kt})$, hence $e_{kt}(a)|2\nu$. Since $2 \nmid t$, we have $(t, e_{kt}(a))|\nu$, thus there exist integers u and v such that $tu - e_{kt}(a)v = \nu$. Hence

$$a^\nu = a^{tu - e_{kt}(a)v} = a^{tu}\gamma_2^{-kt}, \qquad \gamma_2 \in Q(\zeta_{kt}).$$

Similarly, by (6)

$$c^{kt/2} = c^{nt/2}(c^{-\frac{n}{2k}-\frac{1}{2}})^{-kt} = a^{\nu_0 t} b^t \gamma_3^{-kt}, \qquad \gamma_3 \in Q(\zeta_{kt}),$$

thus

$$(a^t)^{u+\nu_0} b^t = (\gamma\gamma_2\gamma_3)^{kt}, \qquad \gamma\gamma_2\gamma_3 \in Q(\zeta_{kt})$$

and $f_{kt}(a^t, b^t) = 1$. On the other hand, if $a^\nu c^{kt/2} \neq \gamma^{kt}$ for all integers ν and all $\gamma \in Q(\zeta_{kt})$, then also

$$a^{\nu t} b^t = a^{(\nu-\nu_0)t} c^{kt/2} (c^{\frac{n}{2k}-\frac{1}{2}})^{kt} \neq \gamma^{kt} \quad \text{and} \quad f_{kt}(a^t, b^t) \neq 1.$$

Since

$$a^{2\nu_0 t} b^{2t} = (c^{n/k})^{kt}, \qquad f_{kt}(a^t, b^t) = 2.$$

The formula (8) follows and, if nt/k is odd, $f_{kt}(a^t, b^t) = f_{kt}(a, b)$. On substituting into (5) and using Lemma 5 we get for each k such that n/k is odd

$$(9) \qquad \sum_{t|\frac{n}{k}} \frac{\mu(t)}{\varphi(kt)} \cdot \frac{(kt, lt)}{e_{kt}(a)(kt, l)} \left(1 - \frac{1}{f_{kt}(a, b)}\right) = 0.$$

Let $n = 2^\alpha n_1$, n_1 odd. We perform the summation over all k such that n/k is odd and we get

$$\sum_{k_1|n_1} \frac{k_1}{(2^\alpha k_1, l)} \sum_{t|\frac{n_1}{k_1}} \frac{\mu(t)}{\varphi(2^\alpha k_1 t)} \cdot \frac{(2^\alpha k_1 t, lt)}{e_{2^\alpha k_1 t}(a)(2^\alpha k_1 t, l)} \left(1 - \frac{1}{f_{2^\alpha k_1 t}(a, b)}\right) = 0.$$

The left hand side can be written alternatively as

$$\sum_{m_1|n_1} \frac{m_1}{\varphi(2^\alpha m_1)\, e_{2^\alpha m_1}(a)\,(2^\alpha m_1, l)} \left(1 - \frac{1}{f_{2^\alpha m_1}(a, b)}\right) \sum_{t|m_1} \mu(t)$$
$$= \frac{1}{\varphi(2^\alpha)\, e_{2^\alpha}(a)\,(2^\alpha, l)} \left(1 - \frac{1}{f_{2^\alpha}(a, b)}\right).$$

It follows that $f_{2^\alpha}(a, b) = 1$, thus by (8) for suitable ν

$$a^\nu c^{2^{\alpha-1}} = \gamma^{2^\alpha}, \qquad \gamma \in Q(\zeta_{2^\alpha}).$$

By Lemma 4 we have either $a^\nu c^{2^{\alpha-1}} = c_1^{2^{\alpha-1}}$ with $\sqrt{c_1} \in Q(\zeta_{2^\alpha})$ or $\alpha = 2$ and $a^\nu c^2 = -4c_2^2$ with $\sqrt{c_2} \in Q(\zeta_4)$. Therefore, by Lemma 3 there are the following possibilities:

$$\alpha = 1,\ c_1 = d^2,\ a^\nu c = d^2,\ ba^{\nu_0 + \nu n_1} = d^n;$$
$$\alpha \geqslant 2,\ c_1 = \pm d^2,\ a^\nu c^{2^{\alpha-1}} = d^{2^\alpha},\ ba^{\nu_0 + \nu n_1} = d^n;$$
$$\alpha > 2,\ c_1 = \pm 2d^2,\ a^\nu c^{2^{\alpha-1}} = 2^{2^{\alpha-1}} d^{2^\alpha},\ ba^{\nu_0 + \nu n_1} = 2^{n/2} d^n;$$
$$\alpha = 2,\ c_2 = \pm d^2,\ a^\nu c^2 = -4d^4,\ ba^{\nu_0 + \nu n_1} = -2^{n/2} d^n.$$

In the last case, clearly ν is odd and $a = -e^2$, thus in each case (i), (ii) or (iii) holds.

Assume now (7). If n/k is odd we have like previously

$$f_{kt}(a^t, b^t) = f_{kt}(a, b) = \begin{cases} 1 & \text{if for some } \nu\colon\ -a^\nu (2c)^{kt/2} = \gamma^{kt},\ \gamma \in Q(\zeta_{kt}), \\ 2 & \text{otherwise} \end{cases}$$

and (9) holds. It follows hence as before that $f_4(a, b) = 1$, thus for suitable ν

$$-a^\nu (2c)^2 = d^4 \quad \text{or} \quad -4d^4.$$

In virtue of (7) we obtain

$$ba^{\nu_0 + \nu_1 n} = d^n \quad \text{or} \quad -2^{n/2} d^n,$$

respectively.

Consider now $k \equiv 2 \bmod 4$. If t is even, $f_{kt}(a^t, b^t) = 1$. If t is odd

$$(10) \qquad f_{kt}(a^t, b^t) = \begin{cases} 1 & \text{if for some } \nu\colon\ -a^\nu = \gamma^{kt},\ \gamma \in Q(\zeta_{kt}), \\ 2 & \text{otherwise}. \end{cases}$$

Indeed, if for some ν: $-a^\nu = \gamma^{kt}$, $\gamma \in Q(\zeta_{kt})$ then $e_{kt}(a) | 2\nu$. Since t is odd $(t, e_{kt}(a)) | \nu$ and there exist integers u, v such that $\nu = tu - e_{kt}(a) v$. Hence

$$a^\nu = a^{tu - e_{kt}(a) v} = a^{tu} \gamma_1^{-kt}, \qquad \gamma_1 \in Q(\zeta_{kt}).$$

Thus by (7)

$$(a^t)^{u + \nu_0} b^t = (\gamma\gamma_1)^{kt} (2c)^{nt/2} = (\gamma\gamma_1 2^{n/2k} c^{n/2k})^{kt}$$

and $f_{kt}(a^t, b^t) = 1$. On the other hand, if $-a^\nu \neq \gamma^{kt}$ for all t integers ν and all $\gamma \in Q(\zeta_{kt})$ then also

$$a^{\nu t} b^t = -a^{(\nu - \nu_0)t} (2c)^{n/2} = -a^{(\nu - \nu_0)t} (2^{n/2k} c^{n/2k})^{kt} \neq \gamma^{kt} \quad \text{and} \quad f_{kt}(a^t, b^t) \neq 1.$$

Since

$$a^{2\nu_0 t} b^{2t} = (2^{n/k} c^{n/k})^{kt}, \qquad f_{kt}(a^t, b^t) = 2.$$

Thus (10) holds and for t odd $f_{kt}(a^t, b^t) = f_{kt}(a, b)$. The formula (9) follows as before. We perform the summation over all $k \equiv 2 \bmod 4$, $k | n$ and we get

$$\sum_{k_1|n_1} \frac{k_1}{(2k_1, l)} \sum_{t | \frac{n_1}{k_1}} \frac{(2k_1 t, lt)}{(2k_1 t, l)\, e_{2k_1 t}(a)} \left(1 - \frac{1}{f_{2k_1 t}(a, b)}\right) = 0.$$

The left hand side can be written alternatively, as

$$\sum_{m_1|n_1} \frac{m_1}{\varphi(2m_1)(2m_1, l)\, e_{2m_1}(a)} \big(1 - f_{2m_1}^{-1}(a, b)\big) \sum_{t|m_1} \mu(t) = \frac{1}{(2, l)\, e_2(a)} \big(1 - f_2^{-1}(a, b)\big).$$

It follows that $f_2(a, b) = 1$ and by (10): $-a = \gamma^2$ with $\gamma \in Q(\zeta_2)$. Since γ is rational, $a = -e^2$ and the necessity of alternative (i), (ii) or (iii) is proved. The sufficiency of the conditions (i) and (ii) follows immediately from the fact that $P(n, d^n)$ and for $n \equiv 0 \bmod 8$ also $P(n, 2^{n/2} d^n)$ consists of all primes. As to (iii) note that by the condition $a = -c^2$, all but finitely many primes from $P(n, a)$ are of the form $4k+1$. For every such prime p the congruence $x^4 \equiv -4 \bmod p$ is soluble, thus $p \in P(n, -2^{n/2} d^n)$ and $P(n, a) \setminus P(n, b)$ is finite.

Proof of Theorem 2. Let $a = \varepsilon \prod_{i=1}^{r} p_i^{\alpha_i}$, $b = \eta \prod_{i=1}^{r} p_i^{\beta_i}$, where $\varepsilon = \pm 1$, $\eta = \pm 1$, p_i are distinct primes, α_i, β_i are integers. If the congruence $a^x \equiv b \bmod p$ is soluble for almost all p then clearly for every positive integer n $P(n, a) \setminus P(n, b)$ has density zero. It follows hence by Theorem 1 with $n = 8m$ that for every positive integer m and suitable integers t_m, d_m

$$ba^{t_m} = d_m^{4m}.$$

The last equality implies

$$\eta \varepsilon^{t_m} = 1,$$

$$(11) \qquad \beta_i + t_m \alpha_i \equiv 0 \bmod 4m \qquad (1 \leqslant i \leqslant r).$$

For all $i, j \leqslant r$ we have $\beta_i \alpha_j - \beta_j \alpha_i = 0$, since otherwise there is a contradiction for $m = |\beta_i \alpha_j - \beta_j \alpha_i|$. $\alpha_i = 0$ implies $\beta_i = 0$, otherwise there is a contradiction for $m = |\beta_i|$. Thus we get for some rational q: $\beta_i = q\alpha_i$ $(1 \leqslant i \leqslant r)$. If $\alpha_i = 0$ $(1 \leqslant i \leqslant r)$ then Theorem 2 holds with $k = t_1$. If for some i, $\alpha_i \neq 0$ then (11) with $m = |\alpha_i|$ implies q integer and $t_{|\alpha_i|} \equiv q \bmod 2$. Hence $\eta = \varepsilon^q$ and Theorem 2 holds with $k = q$.

References

[1] P. D. T. A. Elliott, *The distribution of power residues and certain related results*, Acta Arith., this volume, pp. 141–159.

[2] I. Gerst, *On the theory of n-th power residues and a conjecture of Kronecker*, Acta Arith., this volume, pp. 121–139.

[3] G. Jaeschke and E. Trost, *Über die Nichtprimteiler von ab^x+c*, Elem. Math. 21 (1966), pp. 30–31.

[4] A. Schinzel, *On the congruence $a^x \equiv b \pmod{p}$*, Bull. Acad. Polon. Sci. 8 (1960), pp. 307–309.

Received on 3. 2. 1970

ACTA ARITHMETICA
XVII (1970)

On the probability that n and $f(n)$ are relatively prime

by

R. R. Hall (Nottingham)

It is a well-known theorem of Čebyšev that if n and m are randomly chosen positive integers, then $(n, m) = 1$ with probability $6/\pi^2$. One can expect this to remain true if $m = f(n)$ is a function of n, provided that $f(n)$ does not preserve arithmetic properties of n. Erdös and Lorentz [1] proved that this is so, in the case $f(n) = [f_1(n)]$, where $f_1(x)$ is a smooth function satisfying certain (weak) conditions.

The case $f_1(n) = \alpha n$ was considered by G. L. Watson [6]. For all α, the positive integers n for which $(n, f(n)) = 1$ have a density, and in particular, for irrational α this is $6/\pi^2$.

Suppose now that $f(n)$ is a multiplicative function of n. We set

$$T(x) = \sum_{\substack{n \leqslant x \\ (n, f(n)) = 1}} 1.$$

P. Erdös [2] proved that for $f(n) = \varphi(n)$ or $\sigma(n)$, we have

$$T(x) \sim \frac{xe^{-\gamma}}{\log\log\log x}.$$

The case $f = \varphi$ is of particular interest since $(n, \varphi(n)) = 1$ is a necessary and sufficient condition that there is only one group of order n.

In this paper we consider an additive function, namely the sum of the distinct prime factors of n. We denote this by $g(n)$, and the result is as follows.

Theorem. *Let $T(x)$ denote the number of integers $n \leqslant x$ for which $(n, g(n)) = 1$. Then*

$$T(x) = \frac{6}{\pi^2}x + O\left(\frac{x}{(\log\log\log x)^{1/4}(\log\log\log\log x)^{3/4}}\right).$$

Thus Čebyšev's result holds in this case, as we might expect, for in general additive functions are more evenly distributed over the arithmetic progressions than multiplicative functions; moreover their prime factors, and other arithmetic properties, bear little relation to those of n itself, except when n is prime.