DIVISIBILITY OF GENERALIZED FACTORIALS*

BENJAMIN ROSENBAUM

1. Introduction. Two different types of expression were obtained by A. M. Legendre† for $H$, the index of the highest power of the prime $p$ dividing $n!$:

\[
H = \left[ \frac{n}{p} \right] + \left[ \frac{n}{p^2} \right] + \left[ \frac{n}{p^3} \right] + \cdots ,
\]

\[
H = \frac{n - s}{p - 1},
\]

where $[a/b]$ denotes the largest integer less than or equal to $a/b$, and $s$ is the sum of the digits of $n$ to the base $p$. R. D. Carmichael‡ considered the more general problem of determining $H$ for $\prod_{x=0}^{n-1} (xa+c)$, where $a$ and $c$ are relatively prime positive integers and $a \not\equiv 0 \pmod{p}$. He obtained expressions of type (1) and upper and lower bounds for $H$. In the present paper a correction is made in the upper bound, new expressions for $H$ of types (1) and (2) are derived, and the results are extended to products where $a$ and $c$ are any positive integers.

2. Discussion of previous results. Carmichael used the following method: Set $c_0 = c$, and let $i_r$ be the smallest value of $x \geq 0$ such that $xa+c_{r-1} \equiv 0 \pmod{p}$, the quotient being $c_r$. Then $i_r \leq p - 1$. Let $e_0 = n - 1$, $e_r = \left[ \frac{(e_{r-1} - i_r)}{p} \right]$, $(r>0)$. If $\prod_{x=0}^{n-1} (xa+c_0)$ is divisible by $p$, it has $e_0 + 1$ factors of the form $(mp+i_0)a+c_0$, $(0 \leq m \leq \left[ (e_0 - i_0)/p \right])$, each divisible by $p$. The product of the quotients is $\prod_{x=0}^{e_0} (xa+c_1)$. If this product is divisible by $p$, it has $e_2 + 1$ factors of the form $(mp+i_2)a+c_1$, $(0 \leq m \leq \left[ (e_1 - i_2)/p \right])$, each divisible by $p$. Hence $e_2 + 1$ factors of $\prod_{x=0}^{n-1} (xa+c_0)$ are divisible by $p^2$. If the product of the quotients $\prod_{x=0}^{e_2} (xa+c_2)$ is divisible by $p$, $e_3 + 1$ factors of $\prod_{x=0}^{n-1} (xa+c_0)$ are divisible by $p^3$. Continue in this manner until a product $\prod_{x=0}^{e_t} (xa+c_t)$ is obtained which is not divisible by $p$. Then $e_t + 1$ factors of the original product are divisible by $p^t$ and no factors by $p^{t+1}$. Hence

\[
H = \sum_{r=1}^{t} (e_r + 1).
\]

* Presented to the Society, April 10, 1936. By a generalized factorial we mean a product of integers forming an arithmetic progression.


For certain values of $a$, $c_0$, and $p$, one has $c_0 = c_1 = \cdots = c$ and $i_1 = i_2 = \cdots = i$. In that case

$$H = \left[ \frac{n - 1 - i + p}{p} \right] + \left[ \frac{n - 1 - i - i'p + p^2}{p^2} \right] + \left[ \frac{n - 1 - i - i'p - i'p^2 + p^3}{p^3} \right] + \cdots .$$

In the case of $1 \cdot 3 \cdot 5 \cdots (2n-1)$, $i = (p-1)/2$ for $p \neq 2$ and

$$H = \left[ \frac{2n - 1 + p}{2p} \right] + \left[ \frac{2n - 1 + p^2}{2p^2} \right] + \left[ \frac{2n - 1 + p^3}{2p^3} \right] + \cdots .$$

Carmichael also obtained the expression

$$\frac{n - s}{p - 1} \leq H \leq h + \frac{n - s}{p - 1}$$

when $n$ is not a power of $p$, and $H = (n - 1)/(p - 1)$ when $n$ is a power of $p$, where $s$ is the sum of the digits of $n$ to the base $p$ and $h$ is the index of the highest power of $p \leq n$. The following examples show that these expressions are incorrect: When $a = 5$, $c_0 = 6$, $n = 3$, and $p = 2$, one has $H = 5$ while $h + (n-s)/(p-1) = 2$. When $a = 2$, $c_0 = 21$, $n = 4$, and $p = 3$, one has $H = 4$ while $h + (n-s)/(p-1) = 2$. When $a = 5$, $c_0 = 1$, $n = 4$, and $p = 2$, one has $H = 5$ while $(n-1)/(p-1) = 3$. It will be shown in §8 that the error in the first expression lies in the term $h$. The second expression was derived from a source containing a similar error. The use of (12) in the above examples gives upper bounds for $H$ of 5, 4, and 5, respectively.

I. Schur* obtained a result equivalent to (4) by the use of a different method. He found $H = \sum_{r=1}^{n}[n/p^r + 1/2]$.

E. Stridsberg,† considering the same problem as Carmichael, obtained very complicated expressions for $H$.

3. **Some relations between the letters $c$.** We shall make use of the following theorem and corollaries:

---

† Arkiv för Matematik, Astronomi och Fysik, vol. 6 (1911), no. 34; summary in Dickson, *History of the Theory of Numbers*, vol. 1, p. 264.
THEOREM. If \( c_r \) and \( c_s \) are any two of the letters \( c \), with \( s > r \), then \( c_s \) is the least integer satisfying the conditions: (1) \( c_s p^{s-r} \equiv c_r \pmod{a} \), (2) \( c_s p^{s-r} \geq c_r \).

**Proof.** The theorem is true for \( c_{r+1} \), since \( i_{r+1} \) is the least non-negative integer such that \( i_{r+1} a + c_r = 0 \pmod{p} \), the quotient being \( c_{r+1} \). Proceed by induction, assuming that \( c_s \) is the least integer such that \( c_s p^{s-r} \geq c_r \) and \( c_s p^{s-r} \equiv c_r \pmod{a} \). Now \( i_{r+1} a + c_r = c_{r+1} p \). Hence \( c_{r+1} \) is the least integer such that \( c_{r+1} p^{s+1-r} \geq c_s p^{s-r} \) and \( c_{r+1} p^{s+1-r} \equiv c_r p^{s-r} \pmod{a} \). It follows from the properties of \( c_r \) that \( c_{r+1} \) is the least integer such that \( c_{r+1} p^{s+1-r} \geq c_r \) and \( c_{r+1} p^{s+1-r} \equiv c_r \pmod{a} \). The theorem is therefore true for \( c_{r+1} \) and consequently for \( c_s \).

**Corollary 1.** If \( e \) is the least positive integer such that \( p^e \equiv 1 \pmod{a} \) and \( s > r \), then \( c_s = ma + \text{residue of } c_r p^{k+r-s} \pmod{a} \), where \( k \) is any integer such that \( ke + r - s \geq 0 \) and \( m \) is the least non-negative integer such that \( ma + \text{residue of } c_r p^{k+r-s} \geq c_r p^{s-r} \). When \( c_r < a \), \( m = 0 \).

**Proof.** The first part of the corollary follows from the theorem, which may be restated in the form: \( c_s \) is the least integer greater than or equal to \( c_r p^{s-r} \) and congruent to \( c_r p^{k+r-s} \) modulo \( a \).

To prove the second part of the corollary we make use of the congruence \( x p^{s-r} \equiv c_r \pmod{a} \), which has a unique solution \( 0 \leq x_1 < a \). When \( c_r < a \), \( x_1 p^{s-r} \geq c_r \), otherwise the positive integer \( c_r - x_1 p^{s-r} \) is less than \( a \) and is congruent to zero modulo \( a \). By the theorem, \( x_1 = c_s \). Therefore \( c_s < a \) and \( m = 0 \).

When \( p \) is large, the above corollary gives a method for calculating the letters \( c \) which is more rapid than that based on the initial determination of \( i_s \) as the least non-negative integer such that \( i_s a + c_{s-1} = 0 \pmod{p} \). This is especially true when \( c_0 < a \).

**Example.** When \( c_0 = 29 \), \( a = 7 \), and \( p = 11 \), \( e = 3 \). Then \( c_1 = 7m + \text{residue of } (29)(11)^{2+0-1} \pmod{7} = 7m + \text{residue of } (1)(4)^2 = 7m + 2 < 9 \), \( 2 < c_0 p^{-1} = 29/11 < 9 \), and \( c_2 = 7m + \text{residue of } (9)(11)^2 = 7m + 4 = 4 \).

**Corollary 2.** Necessary and sufficient conditions that \( c_r = c_s \) are (1) \( c_r \leq a \), (2) \( p^{s-r} \equiv 1 \pmod{a} \).

**Proof.** Since \( c_s \) is the least integer satisfying the conditions of the theorem, \( c_s p^{s-r} = c_r + ja \), where \( j \leq p^{s-r} - 1 \). If \( c_r > a \), then \( c_s p^{s-r} < c_r + c_r(p^{s-r} - 1) = c_r p^{s-r} \), and \( c_s < c_r \). Since \( c_r p^{s-r} \equiv c_r \pmod{a} \) and \( c_0 \) is relatively prime to \( a \), so are all the letters \( c \). Therefore when \( c_r = c_s \), we have \( p^{s-r} \equiv 1 \pmod{a} \), and the conditions are necessary.

By Corollary 1, when \( c_r < a \), \( c_r = \text{residue of } c_r p^{k+r-s} \pmod{a} \). If, in addition, \( p^{s-r} \equiv 1 \pmod{a} \), then \( c_r = \text{residue of } c_r \pmod{a} = c_s \). When \( c_r = a \), we have \( a = 1 \) and \( c_s = ma = 1 \). Hence the conditions are sufficient.
4. Expression for $H$ involving the letters $i$. Since $\prod_{x=0}^{a} (xa + c) \not\equiv 0 \pmod{p}$, and $i t a + a = c i + p$, it follows that $i t a > e i$. Also $i t a \leq p - 1$. Hence $-1 < (e i - i t a) / p < 0$ and

$$e i t a = \left[ \frac{e i - i t a}{p} \right] = -1.$$  

By induction, when $r > t$,

$$e r = \left[ \frac{e r - i r}{p} \right] = -1.$$  

Thus (3) is equivalent to

$$H = \sum_{r=1}^{\infty} (e r + 1).$$  

Using the values of $e r$ in §2, substituting that of $e 0$ in $e 1$, the resulting value of $e 1$ in $e 2$, · · · , we obtain from (5)

$$H = \left[ \frac{n - 1 - i 1 + p}{p} \right] + \left[ \frac{n - 1 - i 1 - i 2 p + p^2}{p^2} \right]$$

$$+ \left[ \frac{n - 1 - i 1 - i 2 p - i 3 p^2 + p^3}{p^3} \right] + \cdots .$$  

5. Expression for $H$ involving the letters $c$. Consider $i, a + c r - 1 = c r p$. Solving for $i r$ and substituting in (6) we obtain

$$H = \left[ \frac{l}{a p} + \frac{a - c 1}{a} \right] + \left[ \frac{l}{a p^2} + \frac{a - c 2}{a} \right]$$

$$+ \left[ \frac{l}{a p^3} + \frac{a - c 3}{a} \right] + \cdots ,$$  

where $l = a(n - 1) + c 0$ is the last factor of the product $\prod_{x=0}^{a} (xa + c 0)$. Since $e r + 1 \geq 1$ for $r \leq t$ and $e r + 1 = 0$ for $r > t$, all terms of (5), (6), and (7) are zero after the first zero term.

When $a = 1$ or 2 and $a \not\equiv 0 \pmod{p}$, we have $p \equiv 1 \pmod{a}$. By Corollary 2, when $c 0 \leq a$, $c 0 = c 1 = \cdots = c$ and (7) give (1) or (4).

When $a = 3, 4, 6$ and $a \not\equiv 0 \pmod{p}$, we have $p \equiv 1$ or $p \equiv -1 \pmod{a}$. When $c 0 < a$ and $p \equiv 1$, $c 0 = c 1 = \cdots = c$. When $c 0 < a$ and $p \equiv -1$, since $p^2 \equiv 1 \pmod{a}$, $c 0 = c 2 = c 4 = \cdots$. By Corollary 1, $c 1$ = residue of $c 0 p \pmod{a}$. Hence $c 1 = -c 0 = a - c 0 \pmod{a}$, and $c 1 = a - c 0 = c 3 = c 5 = \cdots$. 

Hence

$$\text{Residue of } c 0 p \pmod{a} = c 1 = -c 0 = a - c 0 \pmod{a},$$  

and

$$c 1 = a - c 0 = c 3 = c 5 = \cdots.$$  

Hence

$$\text{Residue of } c 0 p \pmod{a} = c 1 = -c 0 = a - c 0 \pmod{a},$$  

and

$$c 1 = a - c 0 = c 3 = c 5 = \cdots.$$  

6. Expression for $H$ involving digits of $n$ to base $p$. Let $n = d_h p^h + d_{h-1} p^{h-1} + \cdots + d_1 p + d_0$, and let $s = d_0 + d_1 + \cdots + d_h$, with $0 \leq d_r \leq p - 1$. On substituting the above value of $n$ in (6) we obtain

$$H = \sum_{r=1}^{\infty} \left[ \frac{d_h p^h + d_{h-1} p^{h-1} + \cdots + d_r p^r}{p^r} \right] + \frac{p^r + d_{r-1} p^{r-1} + \cdots + d_1 p + d_0 - \sum_{r'=1}^{s} i_{r'} p^{r'-1} - \cdots - i_2 p - i_1 - 1}{p^r}.$$

We shall designate the second term in the brackets by $F_r$. When $d_{r-1} p^{r-1} + d_{r-2} p^{r-2} + \cdots + d_0 \geq i_r p^{r-1} + i_{r-1} p^{r-2} + \cdots + i_1 + 1$, we obtain $1 \leq F_r < 2$. Since each $d$ and each $i$ is less than or equal to $p - 1$, this will occur when and only when $d_{r-1} > i_r$, or

$$d_{r-1} = i_r \quad \text{and} \quad d_{r-1-b} > i_{r-b},$$

where $r - 1 - b \geq 0$ and $d_{r-1-b}$ is the first $d$ of lower subscript than $d_{r-1}$ which is not equal to the corresponding $i$. (The letter $i_r$ corresponds to $d_{r-1}$. Though $d_{r-1} = 0$ when $u \geq 1$, it is possible to have the corresponding letter $i = 0$ and $F_{r+1} \geq 1, v \geq 1$.) When $d_{r-1} p^{r-1} + d_{r-2} p^{r-2} + \cdots + d_0 < i_r p^{r-1} + i_{r-1} p^{r-2} + \cdots + i_1 + 1$, we have $0 \leq F_r < 1$. From the above it follows that

$$H = \sum_{r=1}^{\infty} \left[ \frac{n}{p^r} \right] + \sum_{r=1}^{\infty} \left[ F_r \right]$$

and finally that

$$H = \frac{n - s}{p - 1} + g,$$

where $g$ is the number of values of $r \geq 1$ for which $d_{r-1} \geq i_r$, the equality sign being used only when the conditions of (8) are fulfilled.

In the case of $n!$, $i = p - 1$. Hence $g = 0$ and $H = (n - s)/(p - 1)$.

In the case of $1 \cdot 3 \cdot 5 \cdot \cdots \cdot (2n - 1)$, $i = (p - 1)/2$ and $g$ is the number of values of $r \geq 0$ for which $d_r \geq (p - 1)/2$, with the restriction on the equality sign.

Example. This example illustrates the use of (9). Consider the product $(22)(27)(32)(37)(42)$ with $p = 3$. From $i_r + c_{r-1} = c_r$ we obtain $i_1 = 1$, $i_2 = 0$, $i_2 = 0$, $i_4 = 1$; and $n = 5 = (1)(3) + (2)$. Hence $d_0 = 2$, $d_1 = 1; d_r = 0, r > 1$. Since $d_0 > i_1, d_1 > i_2, d_2 = i_3$, and $d_4 < i_4$, we have $g = 3$. Hence

$$H = (5 - 3)/2 + 3 = 4.$$

7. Expression for $H$ involving digits of $l = a(n-1) + c_0$ to base $p$. Let $l = \delta_0 p^h + \delta_{h-1} p^{h-1} + \cdots + \delta_0$ and $\sigma = \delta_0 + \delta_1 + \cdots + \delta_h$, with $0 \leq \delta_i \leq p - 1$. Since $l \leq p^{h+1} - 1$ and $c_r \geq 1$, all terms of (7) beyond $[l/a p^h + (a - c_0)/a]$ are zero. Hence
\[ H = \sum_{r=1}^{\lambda} \left[ \frac{a(n-1) + c_0 + p^r(a - c_r)}{a} \right] \]

\[ = \sum_{r=1}^{\lambda} \left[ \frac{N_r}{a} + \frac{D_{r-1} + a p^r - R_{r-1} p^r}{a} \right], \]

where \( D_{r-1} = \delta_{r-1} p^r + \delta_{r-2} p^{r-2} + \cdots + \delta_0. \) Here \( R_{r-1} \) is the residue \((\geq 1 \text{ and } \leq a)\) of \( p^k \text{ mod } a \) \((\mod a)\), \( k \) is the least positive exponent such that \( p^k = 1 \text{ mod } a \), \( k \) is an integer such that \( k \geq r \geq 0 \), and \( N_r = a(n-1) + c_0 - c_r p^r - D_{r-1} + R_{r-1} p^r \). By observing that \( a(n-1) + c_0 - D_{r-1} = \delta_0 p^r + \cdots + \delta_r p^r, c_r p^r - c_0 \equiv 0 \text{ mod } a \) \((\text{see the theorem of } \S 3)\), and \( R_{r-1} p^r - D_{r-1} \equiv p^{k+1} D_{r-1} p^r - D_{r-1} \equiv 0 \text{ mod } a \), we see that \( N_r \equiv 0 \text{ mod } a p^r \).

Also because \( D_{r-1} \leq p^r - 1 \) and \( 1 \leq R_{r-1} \leq a \), we see that

\[ 0 \leq \frac{D_{r-1} + a p^r - R_{r-1} p^r}{a p^r} < 1. \]

Therefore

\[ H = \sum_{r=1}^{\lambda} \frac{N_r}{a} \]

\[ = \sum_{r=1}^{\lambda} \left( \frac{\delta_0 p^r + \cdots + \delta_r + R_{r-1} - c_r}{a} \right) \]

\[ = \sum_{r=1}^{\lambda} \left( \frac{\delta_r (p^r - 1) + R_{r-1} - c_r}{a (p - 1)} \right), \]

and finally

\[ (10) \quad H = \frac{l - \sigma}{a (p - 1)} + \sum_{r=1}^{\lambda} \frac{R_{r-1} - c_r}{a}. \]

In the case of \( n! \), we have \( a = 1, c = 1, \, \epsilon = 1, \, R_{r-1} = 1, \) and \( \sum_{r=1}^{\lambda} (R_{r-1} - c_r)/a = 0. \) Therefore \( H = (n-s)/(p-1). \)

In the case of \( 1 \cdot 3 \cdot 5 \cdot \cdots \cdot (2n-1) \), we have \( a = 2, c = 1, \) and \( \epsilon = 1. \) Then \( R_{r-1} = 1 \) when \( D_{r-1} \) is odd; \( R_{r-1} = 2 \) when \( D_{r-1} \) is even. Hence \( H = (2n-s-1)/(2(p-1)) + \epsilon/2, \) where \( \epsilon \) is the number of values of \( r, (1 \leq r \leq \lambda), \) for which \( D_{r-1} \) is even. When \( l = p^\lambda, \, \sigma = 1 \) and \( e = \lambda. \) Therefore \( H = (n-1)/(p-1) + \lambda/2. \)

**Example.** This example illustrates the use of (10). Determine \( H \)
for \((22)(27)(32)(37)(42)\) with \(p = 3\). We obtain \(\epsilon = 4, \ l = 42 = (1)(3)^9 + (1)(3)^2 + (2)(3) + 0; \ D_0 = 0, \ D_1 = 6, \ D_2 = 15; \ R_0 = 5, \ R_1 = \text{residue (3)^4 \pmod 5} = 4, \ R_2 = 5.\) From \(i_a + c_{r-1} = c_r p,\) we obtain \(c_1 = 9, \ c_2 = 3, \) and \(c_3 = 1.\) Then \(H = (42 - 4)/(5)(2) + (14 - 13)/5 = 4.\)

8. Upper and lower bounds of \(H.\) The terms of (5) and (6) vanish after the \(t\)th term, where \(t\) has the same meaning as in (3). We have \(0 \leq i_r \leq p - 1.\) Substituting the limiting values of \(i_r\) in (6) we obtain

\[
\left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \cdots \leq H \leq \left\lfloor \frac{n - 1}{p} \right\rfloor + \left\lfloor \frac{n - 1}{p^2} \right\rfloor + \cdots + t.
\]

(11)

It is evident from §2 that \(t\) is the index of the highest power of \(p\) dividing any one factor of \(\prod_{x=0}^{n-1}(xa+c_0).\) Hence \(t \leq \lambda,\) the index of the highest power of \(p \leq l = a(n - 1) + c_0.\) However \(t\) may exceed \(\lambda,\) the index of the highest power of \(p \leq n.\) If \(\alpha\) is the index of the highest power of \(p\) exactly dividing \(n,\) and \(\beta\) is any integer \(\geq 0,\) then \(\left\lfloor n/p^\beta \right\rfloor = \left\lfloor (n - 1)/p^\beta \right\rfloor + 1 \quad \text{for} \quad \beta \leq \alpha,\) and \(\left\lfloor n/p^\beta \right\rfloor = \left\lfloor (n - 1)/p^\beta \right\rfloor \quad \text{for} \quad \beta > \alpha.\) Substituting these results in (11), we have

\[
\left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \cdots \leq H \leq \left\lfloor \frac{n - 1}{p} \right\rfloor + \left\lfloor \frac{n - 1}{p^2} \right\rfloor + \cdots + \lambda - \alpha,
\]

or

\[
\frac{n - s}{p - 1} \leq H \leq \frac{n - s}{p - 1} + \lambda - \alpha.
\]

(12)

9. Values of \(H\) when \(a\) and \(c_0\) are any positive integers. If \(a\) and \(c_0\) are not relatively prime let \(d\) be their greatest common divisor, with \(a = a'd\) and \(c_0 = c'd.\) Then \(\prod_{x=0}^{n-1}(xa+c_0) = d^n \prod_{x=0}^{n-1}(xa'+c').\) If \(H, \ H', \) and \(h_d\) are the indices of the highest powers of \(p\) dividing \(\prod_{x=0}^{n-1}(xa+c_0), \prod_{x=0}^{n-1}(xa'+c'),\) and \(d,\) respectively, then \(H = H' + nh_d.\)

When \(a\) and \(c_0\) are relatively prime and \(a \equiv 0 \pmod p,\) \(xa+c_0\) is not divisible by \(p\) and \(H = 0.\)

Yale University