Communicated 10 January 1951 by T. NAGELL

On the highest prime-power which divides $n!$

By OVE HEMER

I

This paper deals with the following problem[1]: Let p be a given prime and consider the numbers $1 \cdot 2 \cdot 3 \ldots n = n!$ for $n = 1, 2, 3$ etc. Find the integral exponents m with the property that p^m cannot be the highest power of p dividing $n!$ for any n. We call these numbers m the exceptional exponents of p.

Put $n = \sum_{\nu=0}^{h} a_\nu p^\nu$ and $s = \sum_{\nu=0}^{h} a_\nu$, where $a_0, a_1, \ldots, a_h$ are integers such that $0 \le a_\nu \le p-1$. When $e(n)$ denotes the exponent of the highest power of p dividing $n!$, we have by Legendre's formula

$$e(n) = \sum_{i=1}^{\infty} \left[\frac{n}{p^i}\right] = \frac{n-s}{p-1}.$$

The smallest exceptional exponent is clearly $m = p$, for $e(p^2 - 1) = p - 1$ and $e(p^2) = p + 1$. As n increases, new numbers m will appear as often as n is a multiple of p^2.

$n = p^h$ gives $h - 1$ new numbers m. For simplicity we write e_h for $e(p^h)$. Since $p^h = p \cdot p^{h-1}$, this gives the recursion formula

$$e_1 = 1, \quad e_h = p\, e_{h-1} + 1.$$

Thus

$$e_h = p^{h-1} + p^{h-2} + \cdots + 1 = \frac{p_h - 1}{p - 1},$$

as can easily be shown by induction.

Hence

$$m = \frac{p^h - 1}{p - 1} - \varrho = e_h - \varrho \qquad (\varrho = 1, 2, \ldots, h - 1)$$

are the new exceptional exponents for $n = p^h$. Consider the general case

$$n = \sum_{\nu=0}^{h} a_\nu p^\nu, \quad (0 \le a_\nu \le p - 1).$$

[1] Proposed by T. NAGELL in Problem 43, p. 123 in his "Elementär talteori", Uppsala 1950.

Since $\prod_{k=p^\nu+1}^{p^\nu+q} k$ and $\prod_{k=1}^{q} k$ are divisible by the same power of p if only $p^\nu + q < p^{\nu+1}$, we have

$$e(n) = \sum_{\nu=1}^{h} a_\nu e_\nu .$$

The identity

$$\sum_{\nu=1}^{h} a_\nu e_\nu = \frac{\sum_{\nu=1}^{h} a_\nu p^\nu - \sum_{\nu=1}^{h} a_\nu}{p-1} = \frac{n-s}{p-1}$$

proves Legendre's formula.

If $n = \sum_{\nu=0}^{h} a_\nu p^\nu$, the highest multiple of $p^2 \leq n$ is $\sum_{\nu=2}^{h} a_\nu p^\nu$ and the general expression for the exceptional exponents will be

$$m = \sum_{\nu=2}^{h} a_\nu e_\nu - \varrho, \quad (\varrho = 1, 2, \ldots, r-1),$$

where $a_r \neq 0$ as the first number in the sequence $a_2, a_3, \ldots$. Of course this may also be written

$$m = e(n) - a_1 - \varrho.$$

Then the set of integers m is identical with the set

$$\sum_{\nu=2}^{h} a_\nu e_\nu - \varrho, \tag{1}$$

where $h = 2, 3, \ldots$ and the a_ν are combined in all manners with $0 \leq a_\nu \leq p-1$, $a_h \neq 0$.

Since $e_\nu = \sum_{i=0}^{\nu-1} p^i$, these sums can also be written as the polynomials

$$\sum_{\nu=0}^{h-1} b_\nu p^\nu - \varrho \quad (\varrho = 1, 2, \ldots, r-1), \tag{2}$$

where $b_\nu = \sum_{i=\nu+1}^{h} a_i$ if $0 < \nu \leq h-1$ and $b_0 = b_1$.

Hence

$$b_0 = b_1 \geq b_2 \geq \cdots \geq b_{h-1} > b_h = 0, \; b_\nu - b_{\nu+1} \leq p-1$$

$b_r \neq b_1$ as the first number in the sequence b_ν.

The first expression (1) is more practical than (2) as appears from the following table of the exceptional exponents m for $p = 3$. The table shows how the integers m can successively be determined from increasing values of h and a_ν (1) or b_ν (2). The values of n where the exceptional exponents appear and their corresponding $e(n)$ are calculated and given in the table. Since $p^\nu = \sum_{i=2}^{\nu-1}(p-1)\,p^i + p^2$ we get for n the successively increasing sequence p^2, $2\,p^2$, $3\,p^2, \ldots$.

$p = 3$ gives $e_1 = 1$, $e_2 = 3 \cdot 1 + 1 = 4$, $e_3 = 13$ and $e_4 = 40$.

Table

n	h	$a_2\ a_3\ a_4$	$b_0\ b_1\ b_2\ b_3\ b_4$	$e(n)$	m
9	2	1	1 1 0	4	3
18		2	2 2 0	8	7
27	3	0 1	1 1 1 0	13	11, 12
36		1 1	2 2 1	17	16
45		2 1	3 3 1	21	20
54		0 2	2 2 2 0	26	24, 25
63		1 2	3 3 2	30	29
72		2 2	4 4 2	34	33
81	4	0 0 1	1 1 1 1 0	40	37, 38, 39
90		1 0 1	2 2 1 1	44	43
99		2 0 1	3 3 1 1	48	47
108		0 1 1	2 2 2 1	53	51, 52
and so on.					

II

In this section we shall examine the frequency of the integers m.

Let $u(n)$ be the number of exceptional exponents m among the integers $1, 2, \ldots, e(n)$. As before we write for brevity u_h for $u(p^h)$. Then it is easy to see that we have the same recursion formula

$$u_h = p\,u_{h-1} + 1.$$

Here is

$$u_1 = 0,\quad u_2 = 1 = e_1 \quad\text{and}\quad u_h = e_{h-1}.$$

Hence for $n = \sum_{\nu=0}^{h} a_\nu p^\nu$ and $e(n) = \sum_{\nu=1}^{h} a_\nu e_\nu$

$$u(n) = \sum_{\nu=2}^{h} a_\nu u_\nu = \sum_{\nu=2}^{h} a_\nu e_{\nu-1}$$

and

$$e(n) = p\,u(n) + \sum_{\nu=1}^{h} a_\nu.$$

Since $e(n) = \dfrac{n-s}{p-1}$ we have

$$u(n) = \frac{n-s}{p(p-1)} - \frac{s-a_0}{p} = \frac{\left[\frac{n}{p}\right] - \sum_{\nu=1}^{h} a_\nu}{p-1}$$

and if we only take the numbers n which are divisible by p into consideration

$$n = p \cdot n_1$$

gives

$$u(n) = \frac{n_1 - s}{p - 1}.$$

The first of these $u(n)$ exceptional exponents m is p and the last is

$$e(n) - a_1 - 1$$

or

$$p\, u(n) + \sum_{\nu=2}^{h} a_\nu - 1.$$

Example: Let p be 5 and examine $n!$ for $n \leq 10\,365$.

$$10\,365 = 3 \cdot 5^5 + 1 \cdot 5^4 + 2 \cdot 5^3 + 4 \cdot 5^2 + 3 \cdot 5$$

and

$$s = 3 + 1 + 2 + 4 + 3 = 13.$$

Hence

$$e(10\,365) = \frac{10\,365 - 13}{4} = 2\,588$$

and

$$u(10\,365) = \frac{2\,073 - 13}{4} = 515.$$

The greatest of these 515 exceptional exponents is

$$e(n) - a_1 - 1 = 2\,588 - 3 - 1 = 2\,584.$$

Further

$$1 \leq \sum_{\nu=1}^{h} a_\nu \leq h(p-1).$$

Hence

$$\frac{e(n) - h(p-1)}{p} \leq u(n) \leq \frac{e(n) - 1}{p}.$$

Since

$$e(n) \geq e_h = \frac{p^h - 1}{p - 1}$$

we have

$$h \log p \leq \log \{1 + (p-1)\, e(n)\} < \log e(n) + 0(1).$$

Now is $\dfrac{p-1}{p \log p} < 1$ even for $p = 2$. Thus

$$\frac{h(p-1)}{p} < \log e(n) + 0(1)$$

and if n is great enough

$$\frac{1}{p} - \frac{\log e(n)}{e(n)} < \frac{u(n)}{e(n)} < \frac{1}{p}.$$

In a similar way it is easy to show that for $p > 2$ and n great enough

$$\frac{1}{p-1} - \frac{\log n}{n} < \frac{e(n)}{n} < \frac{1}{p-1}$$

and

$$\frac{1}{p(p-1)} - \frac{\log n}{n} < \frac{u(n)}{n} < \frac{1}{p(p-1)}.$$

III

It is clear that the preceding methods can be applied to determine the smallest integer $n!$ divisible by a given prime-power p^q and further by an arbitrary integer $\prod_{i=1}^{r} p_i^{q_i}$. This problem is already solved[1] but some remarks may be added.

Write

$$q = \sum_{\nu=k+1}^{h} c_\nu e_\nu + p \cdot e_k \quad (0 \leq c_\nu \leq p-1, \; e_0 = 0).$$

Since $e_\nu = p e_{\nu-1} + 1$ this expression for q is always possible and unique. $c_h, c_{h-1}, \ldots$ are determined successively as large as possible.

$k = 0$ gives $q = \sum_{\nu=1}^{h} c_\nu e_\nu = e(n)$ where $n = \sum_{\nu=1}^{h} c_\nu p^\nu$ is the smallest integer such that $n!$ is divisible by p^q but not by p^{q+1}.

Then Legendre's formula gives

$$n = (p-1) \cdot q + \sum_{\nu=1}^{h} c_\nu.$$

$k > 0$ gives $q \neq e(n)$ for any n because

$$\sum_{\nu=k+1}^{h} c_\nu e_\nu + p e_k = \sum_{\nu=1}^{h} c_\nu e_\nu + k$$

where $c_k = c_{k-1} = \cdots = c_1 = p-1$.

Hence q is one of the exceptional integers m and number k in the sequence $q-k+1, \; q-k+2, \ldots$.

If $c_r < p-1$ as the first of the numbers $c_{k+1}, c_{k+2}, \ldots$ then

$$n = \sum_{\nu=1}^{h} c_\nu p^\nu + p = \sum_{\nu=r}^{h+1} a_\nu p^\nu$$

[1] See A. J. Kempner, Amer. Math. Monthly, 25, 1918, p. 204.

where $a_r = c_r + 1$ and $a_\nu = c_\nu$ for $\nu > r$ is the smallest integer n which makes $n!$ divisible by p^q. In the special case that all the coefficients $c_{k+1}, \ldots, c_h = p - 1$ we have $c_{h+1} = 0$, $r = h + 1$ and $n = p^{h+1}$. Otherwise $a_{h+1} = 0$.

Hence $\frac{n!}{p^q}$ is divisible by p^{r-k} but by no higher power of p.

Then we also have

$$n = (p-1)(q + r - k) + \sum_{\nu=r}^{h+1} a_\nu .$$

Example 1. Let $p = 5$ and $q = 834$.

Then

$$e_1 = 1,\ e_2 = 5 \cdot 1 + 1 = 6,\ e_3 = 31,\ e_4 = 156,\ e_5 = 781.$$

Hence

$$834 = e_5 + e_3 + 3\,e_2 + 4\,e_1 .$$

$$k = 0 \text{ and } n = (p-1)\,q + \sum_{\nu=1}^{h} c_\nu = 4 \cdot 834 + 9 = 3\,345.$$

$\frac{3\,345!}{5^{834}}$ is an integer not divisible by 5.

Example 2. Let $p = 5$ and $q = 1\,716$.

Then

$$1\,716 = 2\,e_5 + 4\,e_3 + 5\,e_2 .$$

This gives $k = 2$ and $r = 4$.

Hence

$$n = 2\,p^5 + p^4 = 2 \cdot 5^5 + 5^4 = 6\,875$$

or

$$n = (p-1)(q + r - k) + \sum_{\nu=r}^{h+1} a_\nu = 4 \cdot 1\,718 + 3 = 6\,875$$

and

$\frac{6\,875!}{5^{1716}}$ is divisible by 5^2 but not by 5^3.

Tryckt den 10 mars 1951

Uppsala 1951. Almqvist & Wiksells Boktryckeri AB