Lagrange and Wilson theorems for the generalized Stirling numbers

By E. T. Bell.

(*Received* 11*th February*, 1938. *Read* 4*th March*, 1938.)

1. If m, n are integers, $m > 0$, $n > 1$, the generalized Stirling numbers[1] $S_r^{(m)}(n-1)$ are defined by the identity in x,

$$\prod_{a=1}^{n-1}(x + a^m) \equiv \sum_{r=0}^{n-1} S_r^{(m)}(n-1)\, x^{n-r-1}. \tag{1}$$

The following notation will be fixed.

p is any prime > 0; m is any integer > 0.

$\phi(m)$ is the number of positive integers $\leqq m$ and prime to m.

(a, b) is the greatest common divisor of the non-negative integers a, b; $(0, b) = b$ if $b > 0$.

$p \equiv \mu \bmod m$, $(m, \mu) = 1$, $0 < \mu \leqq m$.

$(\mu - 1, m) = g$.

$(a)_b$ is the binomial coefficient $a!/b!(a-b)!$, $a > 0$; $(a)_0 = 1$.

$S_r = S_r^{(m)}(p-1)$.

Note that as μ runs through its $\phi(m)$ values, p runs through all positive primes.

We shall consider the interdependence of the five theorems, L, F, W, L', W':

L. (Lagrange's.) $\prod_{a=1}^{p-1}(x - a) \equiv x^{p-1} - 1 \bmod p$, in which $\equiv$ is the sign of identical congruence (the coefficients of like powers of x on both sides are congruent $\bmod p$).

F. (Fermat's). $x^{p-1} - 1 \equiv 0 \bmod p$ has the $p - 1$ incongruent roots $1, \ldots, p-1$.

[1] So designated by C. Tweedie, *Proceedings Edinburgh Mathematical Society*, **37** (1918-19), p. 24.

W. (Wilson's). $1 + (p-1)! \equiv 0 \bmod p$.

L'. $\prod_{a=1}^{p-1} (x - a^m) \equiv (x^{(p-1)/g} - 1)^g \bmod p$.

W'.[1] $S_r \equiv 0 \bmod p,\ 0 \leqq r \leqq p-1,\ r \not\equiv 0 \bmod (p-1)/g;$

$$S_{t(p-1)/g} \equiv (-1)^{t(p-g-1)/g} (g)_t \bmod p,\ 0 \leqq t \leqq g.$$

If only one of these five, say A, is used in the deduction of another, say B, we shall write $A > B$; if $A > B$ and $B > A$, we write $A = B$. Hence, if A, B, C are any three of the five such that $A > B$, $B = C$, we can assert $A > C$. Obviously, if $A > B$ and $B > C$, then $A > C$. If none of the five is used in the deduction of A, we write $0 > A$. In this symbolism we shall prove

(2) $0 > L$; (3) $L > F$; (4) $L > W$; (5) $L' = W'$; (6) $L = L'$.

2. As in the usual proofs, (3), (4) are immediate consequences of (2), and (5) is obvious. To recall a proof of (2), we let n in (1) be an odd prime and take $m = 1$. In the resulting identity x is replaced by $x + 1$, and the new identity is multiplied throughout by $x + 1$. Comparison of like powers of x then gives $S_1^{(1)}(n-1) = \frac{1}{2}n(n-1)$, $\equiv 0 \bmod n$. From this the successive equations for $S_r^{(1)}(n-1)$, $r > 1$, give W' in the case $p = n$, $m = 1$, and from this L follows for the same p, m. Since L holds for $p = 2$, the proof of (2) is complete.

Again, (6) is $L > L'$ and $L' > L$, the second of which follows on taking $m = 1$ in L'. For then $\phi(m) = 1$, and $\mu = 1$ is the only value of μ, so that $g = 1$, and hence $L' > L$. We shall give a proof of $L > L'$ in § 3.

A shorter proof of L', which however is essentially less simple than the proof by $0 > L$, $L > L'$, in that it tacitly uses several known theorems which require longer proofs, is as follows. In L' replace $1^m, \ldots, (p-1)^m$, as permissible, by their least positive residues mod p. Among these residues each of the $(p-1)/g$ m—ic residues of p, which are the incongruent roots of $x^{(p-1)/g} - 1 \equiv 0 \bmod p$, occurs g times. Hence we have L'.

3. Let $\theta = e^{2\pi i/m}$, and in the statement of L replace x by $\theta^s x$. A short reduction gives

$$\prod_{a=1}^{p-1} (x - a\,\theta^s) \equiv x^{p-1} - \theta^{(p-1)s} \bmod p.$$

[1] The case $m = 2$ of W' was given by Glaisher, *Quarterly Journal*, 31 (1900), 34. His method differs from that used here to obtain the general result, and would probably be troublesome to extend.

In this we take $s = 0, \ldots, m-1$ and form the products of corresponding members of the resulting m congruences. Then

$$\prod_{a=1}^{p-1} (x^m - a^m) \equiv \prod_{s=0}^{m} (x^{p-1} - \theta^{(p-1s)}) \bmod p.$$

Referring to the notation in §1, we write $p = km + \mu$, $(\mu - 1, m) = g$, $\mu - 1 = g\sigma$, $m = gn$, $(n, \sigma) = 1$. Hence $p - 1 = g(kn + \sigma)$, and we have

$$\prod_{a=1}^{p-1} (x^n - a^m) \equiv \prod_{s=0}^{gn} (x^{(p-1)/g} - e^{2s\sigma\pi i/n}) \bmod p.$$

If $s_1 \neq s_2$ and $s_1 < n$, $s_2 < n$, the congruence $s_1 \sigma \equiv s_2 \sigma \bmod n$ is impossible, since $(n, \sigma) = 1$. Hence

$$\prod_{s=0}^{gn} (x^{(p-1)/g} - e^{2s\sigma\pi i/n}) = (x^{n(p-1)/g} - 1)^g,$$

and we have

$$\prod_{a=1}^{p-1} (x^n - a^m) \equiv (x^{n(p-1)/g} - 1)^g \bmod p.$$

The last, with x replaced by $x^{1/n}$, is L'. Hence $L > L'$.

CALIFORNIA INSTITUTE OF TECHNOLOGY,
PASADENA, CALIFORNIA, U.S.A.