THEOREM 3.3. *There exists an integer m_0 and a constant c, depending only on m_0 such that for all $n \geqslant m_0$:*

$$\operatorname{rank} E(K_n) \geqslant p^n - c.$$

Proof. Clearly it is enough to prove the same statement as in the theorem with $E(K_n)$ replaced by $\mathcal{E}(K_n)$. We do this by induction on n. Let m_0 be as in Theorem 3.2 and let $c = p^{m_0} - 1$. The statement is clearly true for $n = m_0$ since e_{m_0} is of infinite order. Assume that $\operatorname{rank} \mathcal{E}(K_{n-1}) \geqslant p^{n-1} - c$.

The $\operatorname{Gal}(K_n/K_0)$-module $\mathcal{E}(K_n) \otimes Q_p$ decomposes into:

$$\mathcal{E}(K_n) \otimes Q_p \approx (\mathcal{E}(K_{n-1}) \otimes Q_p) \otimes M$$

where M is a stable $\operatorname{Gal}(K_n/K_0)$-module. We make two remarks:

(1) by Theorem 3.2, $\dim M \geqslant 1$.

(2) if $v \in M$ and $v^\sigma = v$ for all $\sigma \in \operatorname{Gal}(K_n/K_{n-1})$, then $v = 0$. Let N be any non-zero, irreducible factor of M. Then we have the eigenspace decomposition: $N \otimes C = \bigoplus N^\chi$, where χ runs through the characters of $\operatorname{Gal}(K_n/K_0)$. By the second remark, $N^\chi = 0$ if χ is equal to one on $\operatorname{Gal}(K_n/K_{n-1})$. Moreover, for Galois-conjugate characters χ and χ^τ, $\dim N^{\chi^\tau} = \dim N^\chi$, therefore, we see that $\dim N = p^n - p^{n-1}$. Now it follows that

$$\begin{aligned} \operatorname{rank} \mathcal{E}(K_n) &= \operatorname{rank} \mathcal{E}(K_{n-1}) + \dim M \\ &\geqslant p^{n-1} - c + p^n - p^{n-1} \geqslant p^n - c. \end{aligned}$$

This ends the proof of Theorem 3.3.

Remark 3.4. For a different point of view on the growth of the ranks of Mordell–Weil groups, see M. Harris [2].

References

[1] B. Gross, *Heegner points on $X_0(N)$*; In R. A. Rankin (ed.): *Modular forms*, Ellis Horwood, Chichester, 1984, pp. 87–106.

[2] M. Harris, *Systematic growth of Mordell–Weil groups of Abelian varieties in towers of number fields*, Inventiones Math. 51 (1979), 123–141.

[3] P. Kurchanov, *On the rank of elliptic curves over Γ-extensions*, Mat. Sbornik 93 (1974), 460–466.

[4] S. Lang, *Elliptic Functions*, Addison-Wesley, 1973.

[5] B. Mazur, *On the arithmetic of special values of L-functions*, Inventiones Math. 55 (1979), 207–240.

[6] — *Modular curves and arithmetic*, Proceedings of Intern. Congress of Mathematicians, Warsaw 1983, Vol. 1, pp. 185–211.

[7] J. Silverman, *The Arithmetic of Elliptic Curves*, GTM 106, Springer Verlag, 1986.

DEPARTMENT OF MATHEMATICS
HOWARD UNIVERSITY
Washington, D.C. 20059
U.S.A.

Received on 10.12.1987
and in revised form on 28.7.1988 (1772)

ACTA ARITHMETICA
LV (1990)

Congruences for the Stirling numbers and associated Stirling numbers

by

F. T. HOWARD (Winston-Salem, N.C.)

1. Introduction. In [3] it is proved that if $k+n$ is odd then the Stirling number of the first kind, $s(n, k)$, is divisible by the odd part of $n-1$, and the Stirling number of the second kind, $S(n, k)$, is divisible by the odd part of k. These results can be improved; we show in this paper, for example, that if $k+n$ is odd,

$$s(n, k) \equiv 0 \left(\operatorname{mod} \binom{n}{2} \right), \tag{1.1}$$

$$S(n, k) \equiv 0 \left(\operatorname{mod} \binom{k+1}{2} \right). \tag{1.2}$$

Congruences such as (1.1) and (1.2) are apparently not well known. A few congruences for prime moduli can be found in [2], pp. 218–219, 229 and [4], p. 81. Carlitz [1] worked out a method for finding congruences for $S(n, k) \pmod p$, where p is prime, and he found the residues of $S(n, k)$ for $p = 2$, 3 and 5. Carlitz also proved some formulas for special cases such as $S(n, pk)$.

In the present paper we prove (1.1), (1.2) and other congruences for the Stirling numbers and associated Stirling numbers. In particular, we show how to find congruences (mod p) for the Stirling numbers and associated Stirling numbers, and we illustrate our method by finding the residues for $p = 2$, 3 and 5. To the writer's knowledge, these congruences, with the exception of Carlitz's results for $S(n, k)$, have not been published before.

2. Stirling numbers of the first kind. The numbers $s(n, k)$ can be defined by means of

$$x(x+1) \dots (x+n-1) = \sum_{k=0}^{n} s(n, k) x^k \tag{2.1}$$

or by the generating function

$$(-\log(1-x))^k = k! \sum_{n=k}^{\infty} s(n, k) x^n / n!. \tag{2.2}$$

It follows from (2.1) or (2.2) that

$$s(n, k) = (n-1)s(n-1, k)+s(n-1, k-1), \tag{2.3}$$

with

$$s(n, 0) = 0 \quad \text{if } n > 0, \tag{2.4}$$

$$s(n, n) = 1, \tag{2.5}$$

$$s(n, 1) = (n-1)! \quad \text{if } n > 0, \tag{2.6}$$

$$s(n, k) = 0 \quad \text{if } k > n \text{ or } k < 0. \tag{2.7}$$

Many other properties of $s(n, k)$ can be found in [2], pp. 214–219. In particular, we shall make use of the following formula:

$$ks(n, k) = \sum_{i=k-1}^{n-1} \binom{n}{i}(n-i-1)!\, s(i, k-1). \tag{2.8}$$

THEOREM 2.1. *If $n+k$ is odd, then* $s(n, k) \equiv 0 \left(\mathrm{mod} \binom{n}{2}\right)$.

Proof. Since the sets $\{0, 1, \ldots, n-1\}$ and $\{0, -1, \ldots, -(n-1)\}$ are the same (mod n) and the same (mod $(n-1)$), and since $\gcd(n, n-1) = 1$, we have

$$x(x-1)\ldots(x-(n-1)) \equiv x(x+1)\ \ldots\ (x+n-1) \pmod{n(n-1)}.$$

By (2.1) this gives

$$(-1)^{n+k}s(n, k) \equiv s(n, k) \pmod{n(n-1)}.$$

Thus if $n+k$ is odd, we have

$$2s(n, k) \equiv 0 \pmod{n(n-1)},$$

$$s(n, k) \equiv 0 \left(\mathrm{mod} \binom{n}{2}\right),$$

and the proof is complete.

We now turn to the problem of finding congruences for $s(n, k)$ (mod p) when p is prime. In (2.8) let $n = p$. Since

$$\binom{p}{i} \equiv 0 \pmod{p} \quad (i = 1, \ldots, p-1),$$

we have

$$s(p, k) \equiv 0 \pmod{p} \quad (k = 2, \ldots, p-1). \tag{2.9}$$

We note that (2.9) is a well-known result; see [2], p. 218, [4], p. 80. If we now let $n = p$ in (2.3), we see, by (2.9),

$$s(p-1, k) \equiv 1 \pmod{p} \quad (k = 1, \ldots, p-1). \tag{2.10}$$

Similarly, we can now let $n = p-1$ in (2.3). By (2.10) and induction on k, we have

$$s(p-2, k) \equiv 2^{p-k-1}-1 \pmod{p} \quad (k = 0, \ldots, p-2). \tag{2.11}$$

We can now prove our most general result.

THEOREM 2.2. *If p is a prime number, $h > 0$ and $0 \leqslant m < p$, then*

$$s(hp+m, k) = \sum_{i=0}^{h} \binom{h}{i}(-1)^{h-i}s(m, k-h-i(p-1)) \pmod{p}.$$

Proof. We first consider the case $h = 1$. That is, we want to prove, for $m \geqslant 0$,

$$s(p+m, k) \equiv -s(m, k-1)+s(m, k-p) \pmod{p}. \tag{2.12}$$

The proof of (2.12) is by induction on m. By (2.4)–(2.7), and (2.9), we see that (2.12) is true for $m = 0$. Assume it is true for $m = 0, \ldots, j-1$. Then

$$\begin{aligned} s(p+j, k) &= (p+j-1)s(p+j-1, k)+s(p+j-1, k-1) \\ &\equiv (j-1)[-s(j-1, k-1)+s(j-1, k-p)] \\ &\quad +[-s(j-1, k-2)+s(j-1, k-p-1)] \\ &\equiv -[(j-1)s(j-1, k-1)+s(j-1, k-2)] \\ &\quad +[(j-1)s(j-1, k-p)+s(j-1, k-p-1)] \\ &\equiv -s(j, k-1)+s(j, k-p) \pmod{p}, \end{aligned}$$

and the proof of (2.12) is complete. Now a simple induction argument on h completes the proof of Theorem 2.2.

It follows immediately from Theorem 2.2, (2.10) and (2.11) that if $m = 0$, 1, 2, $p-1$ or $p-2$ then for $h \geqslant 1$,

$$s(hp+m, k) \equiv 0 \pmod{p}$$

except for the following: For $i = 0, 1, \ldots, h$

$$\left.\begin{matrix} s(hp, h+(p-1)i) \\ s(hp+1, h+1+(p-1)i) \\ s(hp+2, h+1+(p-1)i) \\ s(hp+2, h+2+(p-1)i) \end{matrix}\right\} \equiv \binom{h}{i}(-1)^{h-i} \pmod{p},$$

$$s(hp+p-1, h+t+i(p-1)) \equiv \binom{h}{i}(-1)^{h-i} \pmod{p} \quad (t = 1, 2, \ldots, p-1),$$

$$s(hp+p-2, h+t+i(p-1)) \equiv \binom{h}{i}(-1)^{h-i}(2^{p-t-1}-1) \pmod{p}$$

$$(t = 1, 2, \ldots, p-2).$$

We note the following special cases. For $p = 2$, 3 or 5, and $n \geqslant p$,

$$s(n, k) \equiv 0 \pmod{p}$$

except for the following: For $h > 0$ and $i = 0, 1, \ldots, h$,

$$s(2h, h+i) \equiv s(2h+1, h+1+i) \equiv \binom{h}{i} \pmod 2,$$

$$\left.\begin{aligned} &s(3h, h+2i)\\ &s(3h+1, h+1+2i)\\ &s(3h+2, h+t+2i)\,(t = 1, 2)\end{aligned}\right\} \equiv \binom{h}{i}(-1)^{h-i} \pmod 3,$$

$$\left.\begin{aligned} &s(5h, h+4i)\\ &s(5h+1, h+1+4i)\\ &s(5h+2, h+t+4i)\,(t = 1, 2)\\ &s(5h+4, h+t+4i)\,(t = 1, 2, 3, 4)\end{aligned}\right\} \equiv \binom{h}{i}(-1)^{h-i} \pmod 5,$$

$$s(5h+3, h+t+4i)\,(t = 1, 2, 3) \equiv \binom{h}{i}(2^{4-t}-1)(-1)^{h-i} \pmod 5.$$

3. Associated Stirling numbers of the first kind. It is known that $s(n, n-k)$ is a polynomial in n of degree $2k$; in fact

$$s(n, n-k) = \sum_{j=0}^{k} d(2k-j, k-j)\binom{n}{2k-j},$$

where $d(n, k)$ is the associated Stirling number of the first kind ([2], pp. 256–257, [4], pp. 72–74). These numbers can be defined by means of the generating function

$$(-\log(1-x)-x)^k = k! \sum_{n=2k}^{\infty} d(n, k)\,x^n/n!. \tag{3.1}$$

It follows from (3.1) that

$$d(n, k) = (n-1)\,d(n-1, k)+(n-1)\,d(n-2, k-1), \tag{3.2}$$

with

$$d(0, 0) = 1, \tag{3.3}$$

$$d(n, 0) = 0 \quad \text{if } n > 0, \tag{3.4}$$

$$d(n, 1) = (n-1)! \quad \text{if } n > 1, \tag{3.5}$$

$$d(n, k) = 0 \quad \text{if } n < 2k \text{ or } k < 0. \tag{3.6}$$

We shall make use of the following formula ([4], p. 73), which follows easily from (2.2) and (3.1):

$$d(n, k) = \sum_{j=0}^{k} (-1)^j \binom{n}{j} s(n-j, k-j). \tag{3.7}$$

By (3.2) we see, trivially, that if $n > 1$

$$d(n, k) \equiv 0 \pmod{n-1}. \tag{3.8}$$

To find congruences (mod p), when p is prime, we let $n = p$ in (3.7). Then by (2.9), (3.6) and the fact that

$$\binom{p}{j} \equiv 0 \pmod p \quad (j = 1, \ldots, p-1),$$

we have

$$d(p, k) \equiv 0 \pmod p \quad (k \geqslant 2),$$

which is a known result ([2], p. 256, [4], p. 81). By (3.8) the modulus can be increased to $p(p-1)$. Thus

$$d(p, k) \equiv 0 \pmod{p(p-1)} \quad (k \geqslant 2). \tag{3.9}$$

THEOREM 3.1. *If p is a prime number, $h > 0$ and $0 \leqslant m < p$, then*

$$d(hp+m, k) \equiv (-1)^h\,d(m, k-h) \pmod p.$$

Proof. We first prove the case $h = 1$:

$$d(p+m, k) \equiv -d(m, k-1) \pmod p. \tag{3.10}$$

The proof is by induction on m. Congruence (3.10) is true for $m = 0$ by (3.4), (3.5) and (3.9), and it is true for $m = 1$ by (3.8). Assume (3.10) is true for $m = 0, 1, \ldots, j-1$. Then

$$\begin{aligned} d(p+j, k) &\equiv (j-1)\,d(p+j-1, k)+(j-1)\,d(p+j-2, k-1)\\ &\equiv (j-1)[-d(j-1, k-1)-d(j-2, k-2)]\\ &\equiv -d(j, k-1) \pmod p, \end{aligned}$$

which completes the proof of (3.10). We note that a result equivalent to (3.10) is stated in problem 4 of [4], p. 81. Now a simple induction argument on h completes the proof of Theorem 3.1.

We see from Theorem 3.1 that

$$d(hp+m, k) \equiv 0 \pmod p \quad \text{if } 2(k-h) > m,$$

$$d(hp+m, k) \equiv 0 \pmod p \quad \text{if } k \leqslant h \ (m \neq 0).$$

Also, for $m = 0, 1, 2, 3, 4$, we have, for $h \geqslant 1$,

$$d(hp+m, k) \equiv 0 \pmod p$$

except for the following cases:

$$d(hp, h) \equiv d(hp+2, h+1) \equiv (-1)^h \pmod p,$$

$$d(hp+3, h+1) \equiv 2(-1)^h \pmod p,$$

$$d(hp+4, h+1) \equiv 6(-1)^h \pmod p,$$

$$d(hp+4, h+2) \equiv 3(-1)^h \pmod p.$$

By (3.5) and Theorem 3.1, we have

$$d(hp+m, h) \equiv 0 \pmod{p} \text{ unless } m = 0,$$

$$d(hp+m, h+1) \equiv (-1)^h (m-1)! \pmod{p}.$$

We note the following special cases. For $p = 2$, 3, or 5, and $n \geqslant p$,

$$d(n, k) \equiv 0 \pmod{p}$$

except for the following: For $h = 0, 1, 2, \ldots$

$$d(2h, h) \equiv 1 \pmod 2,$$

$$d(3h, h) \equiv d(3h+2, h+1) \equiv (-1)^h \pmod 3,$$

$$\left.\begin{matrix} d(5h, h) \\ d(5h+2, h+1) \\ d(5h+4, h+1) \end{matrix}\right\} \equiv (-1)^h \pmod 5,$$

$$d(5h+3, h+1) \equiv 2(-1)^h \pmod 5,$$

$$d(5h+4, h+2) \equiv 3(-1)^h \pmod 5.$$

4. Stirling numbers of the second kind. The numbers $S(n, k)$ can be defined by means of

$$x^n = \sum_{k=0}^{n} S(n, k)\, x(x-1) \ldots (x-k+1),$$

or by the generating function

$$(e^x - 1)^k = k! \sum_{n=k}^{\infty} S(n, k)\, x^n/n!. \tag{4.1}$$

It follows from (4.1) that

$$S(n, k) = S(n-1, k-1) + kS(n-1, k), \tag{4.2}$$

with

$$S(n, 0) = 0 \quad \text{if } n > 0, \tag{4.3}$$

$$S(n, n) = 1, \tag{4.4}$$

$$S(n, 1) = 1 \quad \text{if } n > 0, \tag{4.5}$$

$$S(n, k) = 0 \quad \text{if } k > n \text{ or } k < 0. \tag{4.6}$$

In (4.1) replace x by $-x$ and then multiply both sides by e^{xk}. We get

$$(-1)^k (e^x - 1)^k = k!\, e^{xk} \sum_{n=0}^{\infty} (-1)^n S(n, k)\, x^n/n!. \tag{4.7}$$

Comparing coefficients of $x^n/n!$ in (4.7), we get the following useful formula:

$$S(n, k) = \sum_{i=k}^{n} (-1)^{k+i} \binom{n}{i} S(i, k)\, k^{n-i}. \tag{4.8}$$

If $n+k$ is odd, (4.8) gives

$$2S(n, k) = \sum_{i=k}^{n-1} (-1)^{k+i} \binom{n}{i} S(i, k)\, k^{n-i}. \tag{4.9}$$

Many other properties of $S(n, k)$ (though not (4.8)) can be found in [2], pp. 204–212.

THEOREM 4.1. *If $n+k$ is odd, then*

$$S(n, k) \equiv 0 \left(\mathrm{mod} \binom{k+1}{2}\right).$$

Proof. By (4.9) we have

$$S(n, k) \equiv 0 \pmod k \qquad (n \text{ even}, k \text{ odd}),$$

$$S(n, k) \equiv 0 \pmod{k/2} \qquad (n \text{ odd}, k \text{ even}).$$

Now in (4.2) replace n by $n+1$ and k by $k+1$ to obtain

$$S(n, k) \equiv 0 \pmod{(k+1)/2} \qquad (n \text{ even}, k \text{ odd}),$$

$$S(n, k) \equiv 0 \pmod{k+1} \qquad (n \text{ odd}, k \text{ even}).$$

Combining all these congruences, we have

$$S(n, k) \equiv 0 \left(\mathrm{mod} \binom{k+1}{2}\right) \qquad (n+k \text{ odd}),$$

and the proof is complete.

Theorem 4.1 can be refined by means of (4.9). For example, it follows from (4.9) and Theorem 4.1 that if $n+k$ is odd, then

$$S(n, k) \equiv 0 \left(\mathrm{mod}\ k\binom{k+1}{2}\right) \qquad \text{if } k \mid n,$$

$$S(n, k) \equiv 0 \left(\mathrm{mod}\ k^2\binom{k+1}{2}\right) \qquad \text{if } k^2 \mid n.$$

Let

$$A_n(t) = \sum_{r=0}^{n} S(n, r)\, t^r.$$

Touchard [5] proved that if p is prime, then

$$A_{n+p}(t) \equiv A_{n+1}(t) + t^p A_n(t) \pmod p. \tag{4.10}$$

Congruence (4.10) is also given as an exercise in [4], p. 81. By comparing coefficients of t^k, we see that (4.10) is equivalent to

(4.11) $S(p+m, k) \equiv S(m+1, k)+S(m, k-p) \pmod p \quad (m = 0, 1, \ldots).$

Congruence (4.11) can also be proved by induction on m in much the same way that (2.12) was proved. More generally, we have the following theorem, which follows from (4.11) and a simple induction argument on h.

THEOREM 4.2. *If p is a prime number, $h > 0$ and $0 \leqslant m < p$, then*

$$S(hp+m, k) \equiv \sum_{i=0}^{h} \binom{h}{i} S(m+h-i, k-ip) \pmod p.$$

It follows from Theorem 4.2 that if p is prime and $t > 0$, then

$$S(p^t, k) \equiv S(p^{t-1}, k) \pmod p \quad (k = 0, \ldots, p^t-1).$$

Thus for $t > 0$,

$$S(p^t, k) \equiv 0 \pmod p \quad \text{if } k \neq p^r,\ 0 \leqslant r < t,$$

$$S(p^t, p^r) \equiv 1 \pmod p \quad (r = 0, 1, \ldots, t).$$

In order to prove a theorem more useful than Theorem 4.2, we next generalize a result of Carlitz [1]. Let p be a fixed prime. For $n > 0, j > 0$, define $f_n(j, t)$ by

(4.12) $$f_n(j, t) = -\sum_r \binom{r}{n-(p-1)(r+1)} t^{j(n-(p-1)(r+1))}.$$

The summation on the right is over all r such that

$$(p-1)(r+1) \leqslant n \leqslant p(r+1)+1.$$

Carlitz [1] proved that

$$f_{n+p}(p, t) \equiv f_{n+1}(p, t)+t^p f_n(p, t) \pmod p.$$

It follows immediately from (4.12) that

(4.13) $$f_{n+p}(j, t) \equiv f_{n+1}(j, t)+t^j f_n(j, t) \pmod p.$$

Now suppose $a(n, k)$ is a set of numbers such that $a(0, 0) = 1$ and

(4.14) $$a(p+m, k) \equiv a(m+1, k)+a(m, k-j) \pmod p.$$

Define

(4.15) $$a_n(t) = \sum_{k=0}^{n} a(n, k) t^k.$$

By (4.14) and (4.15) we have

$$a_{n+p}(t) \equiv a_{n+1}(t)+t^j a_n(t) \pmod p.$$

THEOREM 4.3. *Define $f_n(j, t)$ and $a_n(t)$ by (4.12) and (4.15) respectively. Then*

$$a_n(t) \equiv f_n(j, t)-\sum_{r=0}^{p-1} a_{p-1-r}(t) f_{n+r}(j, t) \pmod p.$$

Proof. Let

(4.16) $$c_n(t) = f_n(j, t)-\sum_{r=0}^{p-1} a_{p-1-r}(t) f_{n+r}(j, t).$$

We will prove Theorem 4.3 by showing

$$c_n(t) \equiv a_n(t) \pmod p \quad (n = 0, 1, \ldots, p-1),$$

$$c_{n+p}(t) \equiv c_{n+1}(t)+t^j c_n(t) \pmod p.$$

By (4.12) we have

$$f_n(j, t) \equiv 0 \pmod p \quad (0 \leqslant n < p-1)(p \leqslant n < 2p-2),$$

$$f_n(j, t) \equiv -1 \pmod p \quad (n = p-1 \text{ and } n = 2p-2).$$

Thus for $0 \leqslant n < p-1$,

$$c_n(t) \equiv -a_n(t) f_{p-1}(j, t) \equiv a_n(t) \pmod p,$$

and

$$\begin{aligned} c_{p-1}(t) &\equiv -1-a_{p-1}(t) f_{p-1}(j, t)-a_0(t) f_{2p-2}(j, t) \\ &\equiv a_{p-1}(t) \pmod p. \end{aligned}$$

Now in (4.16) replace n by $n+p$ and use (4.13). After rearranging terms, we have

$$\begin{aligned} c_{n+p}(t) &\equiv f_{n+1}(j, t)-\sum_{r=0}^{p-1} a_{p-1-r}(t) f_{n+1+r}(j, t) \\ &\quad +t^j\Big[f_n(j, t)-\sum_{r=0}^{p-1} a_{p-1-r}(t) f_{n+r}(j, t)\Big] \\ &\equiv c_{n+1}(t)+t^j c_n(t) \pmod p. \end{aligned}$$

This completes the proof of Theorem 4.3.

If $j = p$, we can set $a(n, k) = S(n, k)$. A careful examination of Theorem 4.3 for $j = p$ gives us the next theorem.

THEOREM 4.4. *If p is prime and $n-(r+1)(p-1) = h$, then*

(4.17) $$S(n, hp) \equiv \binom{r}{h-1} \pmod p.$$

If $n-(p-1)r-i = h$ and $1 \leqslant m \leqslant i \leqslant p-1$, then

(4.18) $$S(n, hp+m) \equiv \binom{r}{h} S(i, m) \pmod p.$$

Carlitz [1] proved Theorem 4.3 for $j = p$. In addition to finding congruences such as (4.17), he found the residues of $S(n, k)$ for $p = 2$, 3 and 5. We will not duplicate those results here. Carlitz did not explicitly give formula (4.18).

5. Associated Stirling numbers of the second kind. The numbers $b(n, k)$ are analogous to the numbers $d(n, k)$ defined in Section 3. It is known that $S(n, n-k)$ is a polynomial in n of degree $2k$; we can write

$$S(n, n-k) = \sum_{j=0}^{k} b(2k-j, k-j)\binom{n}{2k-j},$$

where $b(n, k)$ is the associated Stirling number of the second kind ([2], pp. 221–222, [4], pp. 76–78). A generating function for these numbers is

$$(e^x - x - 1)^k = k! \sum_{n=2k}^{\infty} b(n, k)\, x^n/n!. \tag{5.1}$$

It follows from (5.1) that

$$b(n, k) = kb(n-1, k) + (n-1)b(n-2, k-1) \tag{5.2}$$

with

$$b(0, 0) = 1, \tag{5.3}$$

$$b(n, 0) = 0 \quad \text{if } n > 0, \tag{5.4}$$

$$b(n, 1) = 1 \quad \text{if } n > 1, \tag{5.5}$$

$$b(n, k) = 0 \quad \text{if } n < 2k \text{ or } k < 0. \tag{5.6}$$

Analogous to (3.7) is the following formula ([4], p. 77):

$$b(n, k) = \sum_{j=0}^{k} (-1)^j \binom{n}{j} S(n-j, k-j). \tag{5.7}$$

To find congruences (mod p), when p is prime, we let $n = p$ in (5.7). Then we have

$$b(p, k) \equiv 0 \pmod{p} \quad (k \geqslant 2). \tag{5.8}$$

By (5.2) we also have

$$b(p+1, k) \equiv 0 \pmod{p} \quad (k \geqslant 2). \tag{5.9}$$

THEOREM 5.1. *If p is a prime number, $h > 0$ and $0 \leqslant m < p$, then*

$$b(hp+m, k) \equiv \sum_{r=0}^{h} \binom{h}{r} b(m+h-r, k-r) \pmod{p}.$$

Proof. We first prove the case $h = 1$:

$$b(p+m, k) \equiv b(m+1, k) + b(m, k-1) \pmod{p}. \tag{5.10}$$

The proof is by induction on m. Congruence (5.10) is true for $m = 0$ and $m = 1$ by (5.3)–(5.6), (5.8) and (5.9); assume it is true for $m = 0, 1, \ldots, j-1$. Then

$$\begin{aligned} b(p+j, k) &\equiv kb(p+j-1, k) + (j-1)b(p+j-2, k-1) \\ &\equiv k[b(j, k) + b(j-1, k-1)] \\ &\quad + (j-1)[b(j-1, k-1) + b(j-2, k-2)] \\ &\equiv [kb(j, k) + jb(j-1, k-1)] \\ &\quad + [(k-1)b(j-1, k-1) + (j-1)b(j-2, k-2)] \\ &\equiv b(j+1, k) + b(j, k-1) \pmod{p}, \end{aligned}$$

which completes the proof of (5.10). Now a simple induction argument on h completes the proof of Theorem 5.1. We note that a result equivalent to (5.10) can be derived from a problem in [4], p. 81.

It follows from Theorem 5.1 that

$$b(hp+m, k) \equiv 0 \pmod{p} \quad \text{if } m+h < k,$$

$$b(hp+m, k) \equiv 0 \pmod{p} \quad \text{if } m+h = k \text{ and } m > 0,$$

$$b(kp, k) \equiv 1 \pmod{p}.$$

To take advantage of Theorem 4.3, we define

$$b_n(t) = \sum_{k=0}^{n} b(n, k)\, t^k. \tag{5.11}$$

It follows from (5.10) and Theorem 4.3 that if p is prime,

$$b_n(t) \equiv f_n(t) - \sum_{r=0}^{p-1} b_{p-1-r}(t) f_{n+r}(t) \pmod{p}, \tag{5.12}$$

where $f_n(t) = f_n(1, t)$ is defined by (4.12) with $j = 1$.

THEOREM 5.2. *If p is prime and $n-k = (p-1)w$, then*

$$b(n, k) \equiv \binom{w-1}{k-1} \pmod{p}. \tag{5.13}$$

If $n-k = (p-1)w + v$, $1 \leqslant v \leqslant p-2$, then

$$b(n, k) \equiv \sum_{m=0}^{p-1-v} \binom{w}{k-m} b(m+v, m) \pmod{p}. \tag{5.14}$$

If $v \leqslant (p-1)/2$, the upper limit of summation in (5.14) can be replaced by v.

Proof. If we write

$$b_{p-1-r}(t) = \sum_{i=0}^{[(p-1-r)/2]} b(p-1-r, i)\, t^i$$

and examine the sum on the right side of (5.12), we see that we can get $t^{n-(p-1)w}$, for arbitrary w, only when $i=0$, $r=p-1$ or when $i=0$, $r=0$. Taking into account the contribution from $f_n(t)$, we have (5.13). Using the same kind of reasoning, if $n-k=(p-1)w+(p-1-u)$ with $u>0$, we have

$$b(n,k) \equiv \sum_{m=0}^{u} \binom{w}{k-u+m} b(p-1-m,\, u-m) \pmod{p}. \tag{5.15}$$

In (5.15) let $u=p-1-v$ $(1 \leqslant v \leqslant p-2)$, and reverse the order of summation. Then we have (5.14), and the proof is complete.

By (5.14) we have

$$b(n,k) \equiv \binom{w}{k-1} \qquad (n-k=(p-1)w+1),$$

$$b(n,k) \equiv \binom{w}{k-1}+3\binom{w}{k-2} \qquad (n-k=(p-1)w+2,\ p>2),$$

$$b(n,k) \equiv \binom{w}{k-1} \qquad (n-k=(p-1)w+(p-2),\ p>2).$$

For $p=2,\ 3,\ 5$ we have

$$b(n,k) \equiv \binom{n-k-1}{k-1} \pmod 2,$$

$$b(n,k) \equiv \begin{cases} \binom{w-1}{k-1} \pmod 3 & \text{if } n-k=2w, \\ \binom{w}{k-1} \pmod 3 & \text{if } n-k=2w+1, \end{cases}$$

$$b(n,k) \equiv \begin{cases} \binom{w-1}{k-1} \pmod 5 & \text{if } n-k=4w, \\ \binom{w}{k-1} \pmod 5 & \text{if } n-k=4w+1, \\ 3\binom{w}{k-2}+\binom{w}{k-1} \pmod 5 & \text{if } n-k=4w+2, \\ \binom{w}{k-1} \pmod 5 & \text{if } n-k=4w+3. \end{cases}$$

References

[1] L. Carlitz, *Some partition problems related to the Stirling numbers of the second kind*, Acta Arith. 10 (1965), 409–422.

[2] L. Comtet, *Advanced Combinatorics*, Reidel, Dordrecht 1974.

[3] A. Nijenhuis and H. S. Wilf, *Periodicities of partition functions and Stirling numbers modulo p*, J. Number Theory 25 (1987), 308–312.

[4] J. Riordan, *An Introduction to Combinatorial Analysis*, Wiley, New York 1958.

[5] J. Touchard, *Propriétés arithmétiques de certains nombres recurrents*, Ann. Soc. Sci., Bruxelles, A 53 (1933), 21–31.

WAKE FOREST UNIVERSITY
Winston-Salem, NC 27109
U.S.A.

Received on 1.2.1988 (1781)