Contemp. Math. 517(2010): 97-111

Congruences for Stirling Numbers of the Second Kind

O-YEAT CHAN[1] and DANTE MANNA[2]

November 9, 2009

Abstract. We characterize the Stirling numbers of the second kind $S(n,k)$ modulo prime powers in terms of binomial coefficients. Our results are surprisingly simple when k is a multiple of the modulus.

2000 AMS Classification Numbers: 11B73, 11B50.
Keywords: Stirling number, valuation, binomial coefficient.

1. Introduction

The Stirling numbers of the second kind $S(n,k)$, where n and k are nonnegative integers, are defined to be the number of ways to partition a set of n elements into k non-empty subsets. It satisfies the recurrence relation

$$S(n,k) = S(n-1,k-1) + kS(n-1,k), \tag{1.1}$$

and for fixed $k \geq 0$, has the generating function

$$\sum_{n=0}^{\infty} S(n,k)x^n = \prod_{i=1}^{k} \frac{x}{1-ix}. \tag{1.2}$$

There is also an explicit formula in terms of binomial coefficients given by

$$S(n,k) = \frac{1}{k!}\sum_{i=0}^{k}(-1)^i \binom{k}{i}(k-i)^n. \tag{1.3}$$

Local properties of Stirling numbers have been studied from a number of different perspectives. It is known, for example, that for each fixed k, the sequence $\{S(n,k) : n \geq k\}$ is periodic modulo prime powers. The length of this period has been studied by Carlitz [**4**] and Kwong [**6**]. The values $\Delta_{n,m} := \gcd\{k!S(n,k) : m \leq k \leq n\}$ arise in algebraic topology and were investigated by Lundell [**9**] using the explicit formula (1.3). Lengyel [**8**] studied the 2-adic valuations of $k!S(n,k)$ and conjectured an explicit formula for the valuation of $S(2^n,k)$. This conjecture was proved by DeWannemacker in [**5**]. Various congruences involving sums of $S(n,k)$ are also known [**12**].

Recently, the second author, with Amdeberhan and Moll [**1**], considered the sequence of 2-adic valuations of $S(n,k)$ for fixed k. They discovered a deep self-similar structure which they proved for $k \leq 5$. Other authors have looked at extensions to p-adic valuations for odd primes p [**2**], and have proved partial results in that direction. In this paper, we approach the problem from a different angle. Rather than looking for structure in the sequence $\{S(n,k)\}_{n\geq k}$, we look for reductions of $S(n,k)$ for general n and k modulo prime powers, and express them in terms of binomial coefficients, which are much easier to analyze. Unlike much of the work mentioned above, our main tool will not be the explicit formula (1.3), but rather the generating function (1.2).

The rest of the paper is organized as follows. We begin by investigating the parity of $S(n,k)$ and use our theorem to prove a surprising result on the structure of the odd central Stirling numbers

[1] Research partially supported by the NSERC PDF program.
[2] Research partially supported by the AARMS Director's Postdoctoral Fellowship.

$S(2n,n)$. Then we extend our technique to obtain explicit reductions of $S(n,k)$ modulo 4. In Section 4 we generalize our theorems to higher powers of 2, and consider the situation with odd prime powers in Section 5.

Before we continue, we remark that while not immediately evident from our presentation, many of our key results were discovered by mathematical experimentation. In particular, the correct forms of Lemmas 4.1 and 5.1 were found with the help of Maple, and Theorem 2.4 was found using a combination of computation and online resources.

Finally, let us introduce some notation. For a positive integer m, we write $x \equiv_m y$ for $x \equiv y \pmod{m}$. Also, for a prime p, let $\nu_p(n)$ be the largest exponent k such that p^k divides n, with $\nu_p(0) = \infty$ for any p. That is, for $n \neq 0$, $\nu_p(n)$ is the unique positive integer such that $p^{\nu_p(n)} \| n$. Since for any two numbers a and b, $\nu_p(ab)$ satisfies

$$\nu_p(ab) = \nu_p(a) + \nu_p(b), \tag{1.4}$$

ν_p has a natural generalization to the rationals via the identity

$$\nu_p\left(\frac{a}{b}\right) = \nu_p(a) - \nu_p(b). \tag{1.5}$$

Lastly, we define $s_p(n)$ to be the sum of the digits in the base-p representation of n.

2. The Parity of $S(n,k)$

In this section, we investigate $S(n,k) \pmod 2$. The generating function (1.2) allows us to obtain handily the next theorem, which was noted in [**13**] geometrically.

THEOREM 2.1. *For positive integers n and k, we have,*

$$S(n,k) \equiv_2 \begin{cases} 0, & \text{if } n < k, \\ \dbinom{n - \lfloor \frac{k}{2} \rfloor - 1}{n-k}, & \text{if } n \geq k. \end{cases} \tag{2.1}$$

PROOF. We reduce the generating function (1.2) modulo 2 to obtain

$$\begin{aligned} \sum_{n=0}^{\infty} S(n,k)x^n = \prod_{i=1}^{k} \frac{x}{1-ix} &\equiv_2 \frac{x^k}{(1-x)^{\lfloor (k+1)/2 \rfloor}} \\ &= x^k \sum_{n=0}^{\infty} (-1)^n \binom{-\lfloor \frac{k+1}{2} \rfloor}{n} x^n \\ &= x^k \sum_{n=0}^{\infty} \binom{\lfloor \frac{k+1}{2} \rfloor + n - 1}{n} x^n \\ &\equiv_2 \sum_{n=k}^{\infty} \binom{\lfloor \frac{k+1}{2} \rfloor + n - k - 1}{n-k} x^n. \end{aligned} \tag{2.2}$$

Equating coefficients of x^n and simplifying gives the desired result. □

Theorem 2.1 allows us to compute the parity of $S(n,k)$ very efficiently, since the parity of binomial coefficients is easy to compute. In fact, the p-adic valuations of binomial coefficients are well-known ([**3**], Ch. 1):

PROPOSITION 2.2. *Let p be a prime and n,k be non-negative integers. Then we have*

$$\nu_p(n!) = \frac{n - s_p(n)}{p-1}, \tag{2.3}$$

and thus, for all $0 \leq n \leq k$,

$$\nu_p\left(\binom{n}{k}\right) = \frac{s_p(k) + s_p(n-k) - s_p(n)}{p-1}. \tag{2.4}$$

Theorem 2.1 also tells us that the parity of Stirling numbers $S(n,k)$ matches up with the parity of binomial coefficients in a non-trivial way. Recall that $S(n,k)$ also satisfies recurrence relation (1.1), analogous to the recurrence for binomial coefficients. Indeed, (1.1) can be used to construct a "Stirling triangle" just as the binomial coefficients can be arranged in Pascal's triangle. Relations between entries in the two triangles exist, see for example [**14**], but are complicated. The simplicity of Theorem 2.1 allows us to investigate the parity of corresponding subsequences between $S(n,k)$ and $\binom{n}{k}$.

One such application is to consider the central Stirling numbers $S(2n,n)$. The corresponding central binomial coefficients $\binom{2n}{n}$ are ubiquitous in number theory and combinatorics. The Catalan numbers, $\frac{1}{n+1}\binom{2n}{n}$ are particularly important. By (2.4), it is easy to see that for any $n \geq 1$, we have

$$\nu_2\left(\binom{2n}{n}\right) = 2s_2(n) - s_2(2n) = s_2(n) \geq 1.$$

Thus there are no odd central binomial coefficients. But what about $S(2n,n)$? Using Pari/GP version 2.3.4 [**10**], we calculated the indices n for which $S(2n,n)$ is odd and looked for structure. The first 20 terms of the sequence are:

```
1, 2, 4, 5, 8, 9, 10, 16, 17, 18, 20, 21, 32, 33, 34, 36, 37, 40, 41, 42.
```

Putting this sequence into Sloane's Online Encyclopedia of Integer Sequences [**11**], we obtain a unique match: sequence A003714, the Fibbinary numbers. This is the sequence of integers whose binary representation contains no consecutive ones. We now prove this observation, and therefore completely characterize the odd central Stirling numbers. We do this in two steps: first dealing with the even indices and then the odd indices. Since multiplication by two does not change whether there are consecutive ones in the binary representation of a number, one would expect the following lemma to be true.

Lemma 2.3. *For all $n \geq 0$,*

$$S(2n,n) \equiv_2 S(4n,2n).$$

Proof. Theorem 2.1 implies that

$$S(2n,n) \equiv_2 \binom{2n - \lfloor \frac{n}{2} \rfloor - 1}{n}.$$

We split into two cases according to the parity of n. If n is odd, then let $n = 2k+1$ and write

$$S(2n,n) \equiv_2 \binom{4k+2-k-1}{2k+1} = \binom{3k+1}{2k+1}.$$

But we also know that

$$S(4n,2n) \equiv_2 \binom{3n-1}{2n} = \binom{6k+2}{4k+2} = \binom{2(3k+1)}{2(2k+1)}.$$

By (2.4), we have

$$\begin{aligned} \nu_2\left(\binom{m}{\ell}\right) &= s_2(\ell) + s_2(m-\ell) - s_2(m) \\ &= s_2(2\ell) + s_2(2(m-\ell)) - s_2(2m) = \nu_2\left(\binom{2m}{2\ell}\right) \qquad (2.5) \end{aligned}$$

for all $m, \ell \in \mathbb{N}$ with $0 \leq \ell \leq m$. The lemma for this case follows by setting $m = 3k+1$, $\ell = 2k+1$.

In the second case, where $n = 2k$, write

$$S(2n,n) \equiv_2 \binom{4k-k-1}{2k} = \binom{3k-1}{2k}.$$

Comparing to $S(4n, 2n)$, we get

$$S(4n, 2n) \equiv_2 \binom{6k-1}{4k} = \frac{6k-1}{2k-1}\binom{6k-2}{4k}.$$

We apply (1.4) and (1.5) to this formula to obtain

$$\nu_2\left(\binom{6k-1}{4k}\right) = \nu_2\left(\binom{6k-2}{4k}\right) + \nu_2(6k-1) - \nu_2(2k-1) = \nu_2\left(\binom{6k-2}{4k}\right),$$

and the desired result follows from (2.5) by letting $m = 3k-1$ and $\ell = 2k$. □

Theorem 2.4. *The central Stirling number of the second kind $S(2n, n)$ is odd if and only if n is a Fibbinary number.*

Proof. By Lemma 2.3, we only need to consider n odd, since doubling n only appends zeroes to the binary representation and hence does not affect the Fibbinary condition. Set $n = 2k+1$ and apply Theorem 2.1, as in Lemma 2.3 to find that

$$S(2n, n) = S(4k+2, 2k+1) \equiv_2 \binom{3k+1}{2k+1}.$$

Thus by equation (2.4) we see that $S(2n, n)$ is odd if and only if

$$\nu_2\left(\binom{3k+1}{2k+1}\right) = s_2(2k+1) + s_2(k) - s_2(3k+1) = 0. \tag{2.6}$$

First, we argue that for (2.6) to hold, k must be even. If not, then it is easy (via $s_2(2k+1) = s_2(k)+1$) to see that

$$s_2(2k+1) + s_2(k) - s_2(3k+1) = 2s_2(k) + 1 - s_2(3k+1).$$

Also, since k is odd then $3k$ is odd, so $s_2(3k) \geq s_2(3k+1)$ due to the carry in the units digit when adding 1 to $3k$ in binary. Thus, for k odd, we find that

$$\begin{aligned}\nu_2\left(\binom{3k+1}{2k+1}\right) &= 2s_2(k) + 1 - s_2(3k+1)\\ &\geq 2s_2(k) + 1 - s_2(3k) = 1 + \nu_2\left(\binom{3k}{k}\right) \geq 1.\end{aligned}$$

We have now reduced the problem to characterizing the even values of k such that $\binom{3k+1}{2k+1}$ is odd. In other words, even k for which

$$2s_2(k) + 1 - s_2(3k+1) = 0.$$

In this case, since k is even, $3k$ must also be even, hence

$$s_2(3k+1) = s_2(3k) + 1.$$

Therefore,

$$\nu_2\left(\binom{3k+1}{2k+1}\right) = 2s_2(k) - s_2(3k) = 2s_2(k) - s_2(2k+k).$$

This final quantity will equal zero if and only if k is such that the addition in binary of $2k$ and k has no carries, since

$$s_2(a+b) \leq s_2(a) + s_2(b)$$

with equality if and only if the addition $a+b$ has no carries. As the binary addition of $2k$ and k means shifting the digits of k to the left and then adding the result to k, a carry occurs if and only if the binary expression of k contains consecutive ones.

Putting it all together, we have proved that for odd n, $S(2n, n)$ is odd if and only if $k = (n-1)/2$ is an even Fibbinary number. It is easy to see that this is equivalent to n being an odd Fibbinary number. □

3. $S(n,k)$ Mod 4

In this section we extend our approach above to completely characterize $S(n,k)$ mod 4. We begin with an easy lemma.

Lemma 3.1. *For any n, k, $m \in \mathbb{N}$, we have*

$$S(n,km) \equiv_m S(n-1,km-1). \tag{3.1}$$

Proof. Reduce the recurrence relation (1.1) modulo m, with k replaced by km. Equation (3.1) follows immediately. □

Our next lemma completely characterizes $S(n,4) \pmod 4$, and will be the basis for the full characterization in Theorem 3.3.

Lemma 3.2. *For positive integers n, we have*

$$S(n,4) \equiv_4 \begin{cases} 0, & \text{if } n = 0,1,2,3, \\ 1, & \text{if } n \text{ is even and } n \geq 4, \\ 2, & \text{if } n \text{ is odd and } n \geq 4. \end{cases} \tag{3.2}$$

Proof. We reduce the generating function (1.2) modulo 4. We easily find that

$$\begin{aligned} \sum_{n=0}^{\infty} S(n,4)x^n &= \prod_{i=1}^{4} \frac{x}{1-ix} \equiv_4 \frac{x^4}{(1-x)(1-2x)(1+x)} \\ &= \frac{x^4}{(1-x^2)(1-2x)} = x^4 \left(\sum_{n=0}^{\infty} x^{2n}\right)\left(\sum_{n=0}^{\infty} (2x)^n\right) \\ &\equiv_4 \sum_{n=0}^{\infty} x^{2n+4} + \sum_{n=0}^{\infty} 2x^{2n+5}. \end{aligned} \tag{3.3}$$

That is,

$$\sum_{n=0}^{\infty} S(n,4)x^n \equiv \sum_{\substack{n\geq 4 \\ n \text{ even}}} x^n + \sum_{\substack{n\geq 4 \\ n \text{ odd}}} 2x^n \pmod 4,$$

from which the lemma follows immediately. □

Theorem 3.3. *For positive integers n and r, we have*

$$S(n,4r) \equiv_4 \begin{cases} 2r\binom{\frac{n-1}{2}-r-1}{r-1}, & \text{if } n \text{ is odd,} \\ \\ \binom{\frac{n}{2}-r-1}{r-1}, & \text{if } n \text{ is even;} \end{cases} \tag{3.4}$$

$$S(n,4r+1) \equiv_4 \begin{cases} (2r+1)\binom{\frac{n-1}{2}-r-1}{r} + \binom{\frac{n-1}{2}-r-1}{r-1} & \text{if } n \text{ is odd,} \\ \\ (2r+1)\binom{\frac{n}{2}-r-1}{r} & \text{if } n \text{ is even;} \end{cases} \tag{3.5}$$

$$S(n,4r+2) \equiv_4 \begin{cases} (2r-1)\binom{\frac{n-1}{2}-r-1}{r}, & \text{if } n \text{ is odd,} \\ \\ (2r+2)\binom{\frac{n}{2}-r-2}{r} + \binom{\frac{n}{2}-r-1}{r} & \text{if } n \text{ is even;} \end{cases} \tag{3.6}$$

$$S(n,4r+3) \equiv_4 \begin{cases} \binom{\frac{n+1}{2}-r-2}{r}, & \textit{if } n \textit{ is odd,} \\ \\ (2r+2)\binom{\frac{n}{2}-r-2}{r}, & \textit{if } n \textit{ is even;} \end{cases} \tag{3.7}$$

Proof. We provide a proof that contains a combinatorial flavour, although the techniques used in the next section can also be applied here. We first prove the theorem for $S(n,4r)$. The other three are deduced from this case. As before, we reduce the generating function (1.2) modulo 4. With $k=4r$, we readily find that

$$\begin{aligned} \sum_{n=0}^{\infty} S(n,4r)x^n &= \prod_{i=1}^{4r} \frac{x}{1-ix} \equiv_4 \left(\prod_{i=1}^{4} \frac{x}{1-ix}\right)^r = \left(\sum_{n=0}^{\infty} S(n,4)x^n\right)^r \\ &= \sum_{n\ge 0} \sum_{\substack{n_1,\ldots,n_r\ge 0 \\ n_1+\cdots+n_r=n}} S(n_1,4)S(n_2,4)\cdots S(n_r,4)x^n. \end{aligned} \tag{3.8}$$

By Lemma 3.2, the product $S(n_1,4)\cdots S(n_r,4)$ is $0 \pmod 4$ whenever any $n_i \le 3$, $1 \le i \le r$, or whenever any pair n_i, n_j, $1 \le i < j \le r$, are both odd. Otherwise, the value of the product $S(n_1,4)\cdots S(n_r,4)$ is 1 or 2 depending on whether all the n_i are even or if exactly one of them is odd. This means the sum of the n_i must be even in the former case and odd in the latter case. Thus,

$$\sum_{n=0}^{\infty} S(n,4r)x^n \equiv_4 \sum_{\substack{n\ge 0 \\ n \text{ even}}} \sum_{\substack{n_1,\ldots,n_r\ge 4 \\ n_1+\cdots+n_r=n \\ n_1,\ldots,n_r \text{ even}}} x^n + \sum_{\substack{n\ge 0 \\ n \text{ odd}}} \sum_{\substack{n_1,\ldots,n_r\ge 4 \\ n_1+\cdots+n_r=n \\ \text{Exactly one of } n_1,\ldots,n_r \text{ odd}}} 2x^n \tag{3.9}$$

Note that the coefficients of x^n in the first sum counts the number of solutions in non-negative even integers $(x_1,\ldots,x_r)$ to the equation $x_1+\cdots+x_r = n-4r$. Dividing both sides by 2, we find that the number of solutions is equal to the number of solutions in non-negative integers $(y_1,\ldots,y_r)$ to the equation $y_1+\cdots+y_r = (n-4r)/2$. Therefore, an elementary combinatorial formula implies that the coefficient of x^n in the first sum is $\binom{(n-4r)/2+r-1}{r-1}$.

The coefficients of x^n in the second sum counts twice the number of solutions in non-negative integers $(x_1,\ldots,x_r)$ to the equation $x_1+\cdots+x_r = n-4r$, with exactly one of $x_1,\ldots,x_r$ odd. By symmetry, this is equal to $2r$ times the number of solutions in non-negative integers $(y_1,\cdots,y_r)$ to the equation $y_1+\cdots+y_r = n-4r$ with y_1 odd and $y_2,\ldots,y_r$ even. Subtracting 1 from both sides we find that this equation is equivalent to $(y_1-1)+y_2+\cdots+y_r = (n-1)-4r$ with $y_1-1, y_2,\ldots,y_r,n$ all even. Therefore, by the same analysis used in the first sum above, the coefficient of x^n in the second sum is $2r\binom{(n-1-4r)/2+r-1}{r-1}$ for odd n and 0 for even n. Putting these values for the coefficients into (3.9) and simplifying, we arrive at the desired result.

Next, to prove the formula for $S(n,4r+1)$, we once again reduce the generating function (1.2) modulo 4 to find

$$\begin{aligned} \sum_{n=0}^{\infty} S(n,4r+1)x^n &= \prod_{i=1}^{4r+1} \frac{x}{1-ix} \equiv_4 \left(\prod_{i=1}^{4r} \frac{x}{1-ix}\right) \frac{x}{1-x} \\ &= \left(\sum_{n=0}^{\infty} S(n,4r)x^n\right)\left(\sum_{m=1}^{\infty} x^m\right) = \sum_{n=0}^{\infty}\sum_{m=0}^{n-1} S(m,4r)x^n. \end{aligned} \tag{3.10}$$

Thus,

$$S(n,4r+1) \equiv_4 \sum_{m=0}^{\lfloor (n-1)/2 \rfloor} S(2m,4r) + \sum_{m=1}^{\lfloor n/2 \rfloor} S(2m-1,4r)$$

$$\begin{aligned} &\equiv_4 \sum_{m=0}^{\lfloor (n-1)/2\rfloor} \binom{m-r-1}{r-1} + \sum_{m=1}^{\lfloor n/2\rfloor} 2r\binom{m-r-2}{r-1} \\ &= \sum_{m=0}^{\lfloor (n-1)/2\rfloor-2r} \binom{m+r-1}{m} + 2r\sum_{m=0}^{\lfloor n/2\rfloor-2r-1} \binom{m+r-1}{m}. \end{aligned}\tag{3.11}$$

Applying the identity

$$\sum_{j=0}^{r}\binom{n+j}{j} = \binom{n+r+1}{r},\tag{3.12}$$

we find that

$$\begin{aligned} S(n,4r+1) &\equiv_4 \binom{r-1+\lfloor\frac{n-1}{2}\rfloor-2r+1}{\lfloor\frac{n-1}{2}\rfloor-2r} + 2r\binom{r-1+\lfloor\frac{n}{2}\rfloor-2r-1+1}{\lfloor\frac{n}{2}\rfloor-2r-1} \\ &= \binom{\lfloor\frac{n-1}{2}\rfloor-r}{r} + 2r\binom{\lfloor\frac{n}{2}\rfloor-r-1}{r}. \end{aligned}\tag{3.13}$$

Splitting $\binom{(n-1)/2-r}{r}$ into $\binom{(n-1)/2-r-1}{r}+\binom{(n-1)/2-r-1}{r-1}$ when n is odd, we easily verify that (3.13) is equivalent to (3.5).

Proving (3.6) is much easier, since by (1.2),

$$\begin{aligned} \sum_{n=0}^{\infty} S(n,4r+2)x^n &= \left(\sum_{n=0}^{\infty} S(n,4r+1)x^n\right)\frac{x}{1-2x} \equiv_4 \left(\sum_{n=0}^{\infty} S(n,4r+1)x^n\right)(x+2x^2) \\ &= \sum_{n=0}^{\infty}(S(n-1,4r+1)+2S(n-2,4r+1))x^n. \end{aligned}\tag{3.14}$$

Combining (3.13) and (3.14) we find that

$$\begin{aligned} S(n,4r+2) &\equiv_4 S(n-1,4r+1)+2S(n-2,4r+1) \\ &\equiv_4 \binom{\lfloor\frac{n-2}{2}\rfloor-r}{r} + 2r\binom{\lfloor\frac{n-1}{2}\rfloor-r-1}{r} + 2\binom{\lfloor\frac{n-3}{2}\rfloor-r}{r} \\ &= \binom{\lfloor\frac{n-2}{2}\rfloor-r}{r} + (2r+2)\binom{\lfloor\frac{n-1}{2}\rfloor-r-1}{r}. \end{aligned}\tag{3.15}$$

Noting that $3\equiv -1 \pmod 4$ and considering the cases where n is odd or even separately, we see that (3.15) is equivalent to (3.6).

Finally, to prove (3.7), we apply (3.4) to (3.1) and simplify. □

4. Powers of 2

The success of the generating function approach in the previous sections motivates us to apply these techniques to higher powers of 2. The question we need to answer, then, is, "What happens if we try to reduce the polynomial in the denominator of (1.2) modulo 2^m, for some $m\geq 3$?" The answer lies in the following lemma.

Lemma 4.1. *Let $m\geq 3$ be a positive integer. Then we have*

$$\prod_{i=1}^{2^{m-\ell-1}}(1-2^{\ell}(2i-1)x) \equiv_{2^m} \begin{cases} (1-x^2)^{2^{m-2}}, & \text{for } \ell=0, \\ 1-2^{m-1}x^2, & \text{for } \ell=1, \\ 1, & \text{for } 2\leq \ell\leq m-2. \end{cases}\tag{4.1}$$

The $l=0$ case appears, in stronger form, as (11) in the proof of Theorem 4 in [**7**].

Lemma 4.1 allows us to write the generating function for $S(n,2^m)$ in a form from which formulas relating $S(n,2^m)$ to binomial coefficients modulo powers of 2 can be read.

Corollary 4.2.

$$
\begin{aligned}
\sum_{n\ge 0} S(n,2^m)x^n &\equiv_{2^m} \frac{x^{2^m}}{(1-x^2)^{2^{m-2}}(1-2^{m-1}x^2)(1-2^{m-1}x)} \\
&\equiv x^{2^m}\left(\sum_{k\ge 0} 2^{k(m-1)}x^{2k}\right)\left(\sum_{\ell\ge 0} 2^{\ell(m-1)}x^{\ell}\right)\left(\sum_{n\ge 0}\binom{-2^{m-2}}{n}x^{2n}\right) \\
&\equiv_{2^m} x^{2^m}(1+2^{m-1}x^2)(1+2^{m-1}x)\left(\sum_{n\ge 0}\binom{-2^{m-2}}{n}x^{2n}\right) \qquad (4.2)
\end{aligned}
$$

We now prove the lemma.

Proof. We begin by noting that for $m \ge 3$ and $0 \le \ell \le m-2$ we have

$$
\begin{aligned}
\prod_{i=1}^{2^{m-\ell}}(1-2^\ell(2i-1)x) &= \prod_{i=1}^{2^{m-\ell-1}}(1-2^\ell(2i-1)x)(1-2^\ell(2i-1+2^{m-\ell})x) \\
&= \prod_{i=1}^{2^{m-\ell-1}}\left[(1-2^\ell(2i-1)x)^2-2^m x(1-2^\ell(2i-1)x)\right] \\
&= \left(\prod_{i=1}^{2^{m-\ell-1}}(1-2^\ell(2i-1)x)\right)^2 \\
&\quad -2^m x\sum_{j=1}^{2^{m-\ell-1}}(1-2^\ell(2j-1)x)\prod_{\substack{1\le i\le 2^{m-\ell-1}\\ i\ne j}}(1-2^\ell(2i-1)x)^2 \\
&\quad + \text{terms involving factors of } 2^{2m} \text{ and higher.} \qquad (4.3)
\end{aligned}
$$

When $1 \le \ell \le m-2$, the product $(1-2^\ell(2j-1)x)\prod(1-2^\ell(2i-1)x)^2$ is congruent to $1 \pmod 2$ for all j. Thus

$$
\sum_{j=1}^{2^{m-\ell-1}}(1-2^\ell(2j-1)x)\prod_{i\ne j}(1-2^\ell(2i-1)x)^2 \equiv 2^{m-\ell-1} \equiv 0 \pmod 2,
$$

and so, since $m \ge 3$, we have

$$
\prod_{i=1}^{2^{m-\ell}}(1-2^\ell(2i-1)x) \equiv \left(\prod_{i=1}^{2^{m-\ell-1}}(1-2^\ell(2i-1)x)\right)^2 \pmod{2^{m+1}}. \qquad (4.4)
$$

Similarly, when $\ell = 0$, the product $(1-2^\ell(2j-1)x)\prod(1-2^\ell(2i-1)x)^2$ is congruent to $(1-x)^3 \pmod 2$ for all j. Therefore we have

$$
\sum_{j=1}^{2^{m-1}}(1-(2j-1)x)\prod_{i\ne j}(1-(2i-1)x)^2 \equiv 2^{m-1}(1-x)^3 \equiv 0 \pmod 2,
$$

and so (4.4) holds for $\ell = 0$ as well.

Using (4.4), we easily prove Lemma 4.1 by induction on m. For the base case, $m = 3$, it is easy to verify that

$$
\begin{aligned}
\prod_{i=1}^{4}(1-(2i-1)x) &\equiv_8 (1-x)(1-3x)(1+3x)(1+x) \\
&\equiv_8 (1-x^2)(1-9x^2) \equiv_8 (1-x^2)^2
\end{aligned}
$$

for $\ell = 0$ and

$$\prod_{i=1}^{2}(1-2(2i-1)x) \equiv_8 (1-2x)(1+2x) \equiv_8 1-4x^2$$

for $\ell = 1$.

Now suppose that for some $m \geq 3$, (4.1) is true. This means that there are polynomials $f_\ell(x), 0 \leq \ell \leq m-2$, such that

$$\prod_{i=1}^{2^{m-\ell-1}} (1-2^l(2i-1)x) = 2^m f_\ell(x) + \begin{cases} (1-x^2)^{2^{m-2}}, & \text{for } \ell = 0, \\ 1-2^{m-1}x^2, & \text{for } \ell = 1, \\ 1, & \text{for } 2 \leq \ell \leq m-2. \end{cases} \tag{4.5}$$

Now apply (4.5) to (4.4) to obtain the result for $m+1$ and $0 \leq \ell \leq m-2$. The final case for $m+1$ is $\ell = m-1$. Here note that the product contains only two factors, so

$$\begin{aligned} \prod_{i=1}^{2^{m+1-(m-1)-1}} (1-2^{m-1}(2i-1)x) &= (1-2^{m-1}x)(1-3\cdot 2^{m-1}x) \\ &\equiv (1-2^{m-1}x)(1+2^{m-1}x) \\ &\equiv 1-2^{2m-2}x^2 \equiv 1 \pmod{2^{m+1}} \end{aligned}$$

as desired. □

We are now ready to provide a characterization of $S(n,k) \pmod{2^m}$ for any $m \geq 3$.

THEOREM 4.3. *Let n, a, m be positive integers with $m \geq 3$, $a > 0$, and $n \geq a2^m + 1$. Then*

$$S(n, a2^m) \equiv_{2^m} a2^{m-1}\binom{\lfloor\frac{n-1}{2}\rfloor - a2^{m-2}-1}{\lfloor\frac{n-1}{2}\rfloor - a2^{m-1}} + \frac{1+(-1)^n}{2}\binom{n/2-a2^{m-2}-1}{n/2-a2^{m-1}} \tag{4.6}$$

PROOF. By (1.2) and Corollary 4.2, we find that

$$\begin{aligned} \sum_{n\geq 0} S(n,a2^m)x^n &\equiv x^{a2^m}\left(\sum_{n\geq 0}(-1)^n\binom{-a2^{m-2}}{n}x^{2n}\right)(1+a2^{m-1}x^2)(1+a2^{m-1}x) \\ &\equiv \left(\sum_{n\geq 0}\binom{a2^{m-2}+n-1}{n}x^{2n+a2^m}\right)(1+a2^{m-1}x+a2^{m-1}x^2). \end{aligned} \tag{4.7}$$

Collecting powers and reindexing, we obtain

$$S(n,a2^m) \equiv_{2^m} \begin{cases} a2^{m-1}\binom{\frac{n-a2^m-1}{2}+a2^{m-2}-1}{\frac{n-a2^m-1}{2}} & \text{if } n \text{ is odd,} \\ \binom{\frac{n-a2^m}{2}+a2^{m-2}-1}{\frac{n-a2^m}{2}} + a2^{m-1}\binom{\frac{n-a2^m-2}{2}+a2^{m-2}-1}{\frac{n-a2^m-2}{2}} & \text{if } n \text{ is even,} \end{cases}$$

which is equivalent to (4.6). □

Next we prove a formula for $S(n,k)$ (mod 2^m) when k is not necessarily a multiple of 2^m. We will use the notation $t_N(x_1,\ldots,x_M)$ for the *elementary symmetric polynomial* on $x_1,\ldots,x_M$ of degree N. These polynomials exist for integers N and M such that $0 \leq N \leq M$ and are generated by the formula

$$\prod_{i=1}^{M}(z-x_i) = \sum_{N=0}^{M} t_N(x_1,\ldots,x_M)z^{M-N}.$$

THEOREM 4.4. *Let n, a, b, m be positive integers with $m \geq 3$, $a > 0$, and $b, n \geq 0$. Then we have*

$$S(n, a2^m + b) \equiv \sum_{i=0}^{2^m-b-1} S(n + 2^m - b - i, (a+1)2^m) t_i(1, 2, \ldots, 2^m - b - 1) \tag{4.8}$$

$$\equiv \sum_{i=0}^{n} S(i, a2^m) S(n-i, b) \pmod{2^m}. \tag{4.9}$$

PROOF. The second congruence follows immediately from the fact that

$$\sum_{n\geq 0} S(n, a2^m + b)x^n \equiv_{2^m} \left(\prod_{i=1}^{a2^m} \frac{x}{1-ix}\right) \cdot \left(\prod_{i=1}^{b} \frac{x}{1-ix}\right) = \sum_{n\geq 0} \sum_{i+j=n} S(i, a2^m) S(j, b) x^n.$$

To obtain the first congruence, note that

$$\begin{aligned}
&\sum_{n\geq 0} S(n, a2^m + b)x^n \\
&\quad = \left(\prod_{i=1}^{(a+1)2^m} \frac{x}{1-ix}\right) \left(\prod_{i=0}^{2^m-b-1} \frac{1-((a+1)2^m - i)x}{x}\right) \\
&\quad \equiv_{2^m} \left(\sum_{n\geq 0} S(n, (a+1)2^m) x^{n-2^m+b}\right) \left(\prod_{i=1}^{2^m-b-1} (1+ix)\right) \\
&\quad \equiv_{2^m} \left(\sum_{n\geq 0} S(n + 2^m - b, (a+1)2^m) x^n\right) \left(\sum_{i=0}^{2^m-b-1} t_i(1, 2, \ldots, 2^m - b - 1) x^i\right).
\end{aligned}$$

Multiplying through and collecting like powers yields (4.8). □

REMARK 4.5. To compute a congruence formula for a Stirling number $S(n, k)$ in terms of binomial coefficients mod a power of 2, we rewrite $k = a2^m + b$ and apply the previous theorem. (Notice that the result is "tight" in the sense that it does not hold if $\equiv_{2^m}$ is replaced by $\equiv_{2^{m+1}}$.) The symmetric representation (4.8) is generally more useful for computations, since for a fixed m, all of the symmetric polynomials t_i can be precomputed and the sum on i is a short sum, the length of which is $2^m - b \leq 2^m$. Compare this to the sum in (4.9), the length of which is $n \geq a2^m$.

5. Odd Prime Powers

The ideas used in the previous sections carry over to the case where the modulus is a power of an odd prime. Thus, we obtain the following analogous version of Lemma 4.1.

LEMMA 5.1. *Let p be an odd prime and m, ℓ be integers with $0 \leq \ell < m$. Then we have*

$$\prod_{\substack{1\leq i\leq p^{m-\ell} \\ \gcd(p,i)=1}} (1 - p^\ell ix) \equiv_{p^m} \begin{cases} (1 - x^{p-1})^{p^{m-1}}, & \textit{for } \ell = 0, \\ 1, & \textit{for } 1 \leq \ell \leq m-1. \end{cases} \tag{5.1}$$

PROOF. For each fixed odd prime p, we induct on m. The base case $m = 1$ is straightforward, and is equivalent to proving that

$$(1-x)(1-2x)\cdots(1-(p-1)x) - (1-x^{p-1}) \equiv 0 \pmod{p}.$$

If the left-hand side of the above is not identically 0, then it is a polynomial of degree at most $p-1$, and thus has at most $p-1$ zeroes mod p. But $x \equiv_p 0$ is clearly a zero, and by Fermat's Little Theorem so is every non-zero congruence class mod p. Therefore the polynomial must be identically zero.

Now suppose the lemma is true for some $m \geq 1$. Then as before we find that at $m+1$ the left-hand side of (5.1) becomes

$$\begin{aligned}
&\prod_{\substack{1\leq i\leq p^{m-\ell+1}\\ \gcd(p,i)=1}} (1-p^\ell ix)\\
&\quad= \prod_{\substack{1\leq i\leq p^{m-\ell}\\ \gcd(p,i)=1}} (1-p^\ell ix)(1-(p^\ell i+p^m)x)\cdots(1-(p^\ell i+p^m(p-1))x)\\
&\quad= \prod_{\substack{1\leq i\leq p^{m-\ell}\\ \gcd(p,i)=1}} \Bigg[(1-p^\ell ix)^p - \sum_{j=1}^{p-1} p^m jx(1-p^\ell ix)^{p-1}\\
&\qquad\qquad + \text{terms involving powers of } p^{2m} \text{ and higher}\Bigg]. \qquad (5.2)
\end{aligned}$$

For $m \geq 1$, we have $2m \geq m+1$. Also, since p is odd, the sum $\sum_{j=1}^{p-1} j \equiv 0 \pmod{p}$. Thus

$$\prod_{\substack{1\leq i\leq p^{m-\ell+1}\\ \gcd(p,i)=1}} (1-p^\ell ix) \equiv \Bigg(\prod_{\substack{1\leq i\leq p^{m-\ell}\\ \gcd(p,i)=1}} (1-p^\ell ix)\Bigg)^p \pmod{p^{m+1}}. \qquad (5.3)$$

Using (5.3) with the fact that for any prime p and polynomials $r(x)$ and $s(x)$, we have $r(x) \equiv s(x) \pmod{p^m} \Rightarrow r(x)^p \equiv s(x)^p \pmod{p^{m+1}}$, we obtain the desired result for $0 \leq \ell \leq m-1$. The final piece, $\ell = m$, follows easily from the fact that

$$\begin{aligned}
&(1-p^m x)(1-2p^m x)\cdots(1-(p-1)p^m x)\\
&\quad\equiv (1-p^{2m}x^2)(1-4p^{2m}x^2)\cdots(1-[(p-1)/2]^2p^{2m}x^2) \equiv 1 \pmod{p^{m+1}}
\end{aligned}$$

whenever $m \geq 1$. □

Comparing Lemma 5.1 to Lemma 4.1, we see that the result is simpler for odd primes. We easily obtain the congruences for Stirling numbers modulo odd prime powers.

Theorem 5.2. *Let p be an odd prime and let n, a, m be positive integers with $m \geq 1$, $a > 0$, and $n \geq ap^m$. Then*

$$S(n, ap^m) \equiv_{p^m} \begin{cases} \binom{\frac{n-ap^{m-1}}{p-1} - 1}{\frac{n-ap^m}{p-1}}, & \textit{if } n \equiv a \pmod{p-1},\\ 0, & \textit{otherwise.}\end{cases} \qquad (5.4)$$

Proof. By (1.2) and Lemma 5.1, we find that

$$\begin{aligned}
\sum_{n\geq 0} S(n, ap^m)x^n &= \prod_{i=1}^{ap^m} \frac{x}{1-ix} \equiv_{p^m} \left(\prod_{i=1}^{p^m} \frac{x}{1-ix}\right)^a\\
&\equiv x^{ap^m}\left(\frac{1}{(1-x^{p-1})^{p^{m-1}}}\right)^a\\
&\equiv x^{ap^m} \sum_{n\geq 0} (-1)^n \binom{-ap^{m-1}}{n} x^{n(p-1)} \qquad (5.5)\\
&\equiv \sum_{n\geq 0} \binom{ap^{m-1}+n-1}{n} x^{n(p-1)+ap^m}. \qquad (5.6)
\end{aligned}$$

Collecting powers and reindexing, we obtain the desired result. □

Theorem 5.3. *Let p be an odd prime and n, a, b, m be positive integers with $m \geq 1$, $n > 0$, $0 \leq b \leq p^m - 1$, and $n \geq ap^m + b$. Also let $t_N(x_1, \ldots, x_M)$ be as in Theorem 4.4. Then we have*

$$
\begin{aligned}
&S(n, ap^m + b) \\
&\equiv \sum_{\substack{0 \leq i \leq p^m - b - 1 \\ i \equiv n - a - b \pmod{p-1}}} S(n + p^m - b - i, (a+1)p^m) t_i(1, 2, \ldots, p^m - b - 1) && (5.7) \\
&\equiv \sum_{\substack{0 \leq i \leq n \\ i \equiv a \pmod{p-1}}} S(i, ap^m) S(n - i, b) \pmod{p^m} && (5.8)
\end{aligned}
$$

Proof. The proofs of (5.7) and (5.8) are analogous to those of (4.8) and (4.9), respectively, with 2 replaced by p everywhere. The extra condition on the summation index i in (5.7) comes from the fact that by Theorem 5.2, $S(n+p^m-b-i, (a+1)p^m) \equiv 0 \pmod{p^m}$ unless $n+p^m-b-i \equiv a+1 \pmod{p-1}$. This implies $i \equiv n - a - b \pmod{p-1}$. The condition $i \equiv a \pmod{p-1}$ in (5.8) is also a result of Theorem 5.2. □

We have proven congruences between Stirling numbers and finite sums of binomial coefficients modulo powers of primes. The theorems are slightly different for powers of 2 than they are for powers of odd primes. Theorems 4.3 and 5.2 give us a simple form for $S(n, k)$ when k is a multiple of the modulus. Thus we can easily obtain local information on $S(n, k)$ modulo any divisor of k, by applying Theorems 4.3 and 5.2 in conjunction with the Chinese Remainder Theorem. It is worth noting that the theorems of Kwong [**6**] that give minimum periods for Stirling numbers modulo M can be recovered from here.

Although the case where the modulus does not divide k appears to be much more complicated, as shown by Theorems 4.4 and 5.3, we believe that further investigations would yield meaningful results.

References

[1] T. Amdeberhan, D. Manna, and V. H. Moll, *The 2-adic valuation of Stirling numbers*, Experiment. Math. **17** (2008), no. 1, 69–82.

[2] A. Berrizbeitia, L. A. Medina, A. C. Moll, V. H. Moll, L. Noble, *The p-adic Vaulation of Stirling Numbers*, *Preprint*, 2009.

[3] G. Boros, V. Moll, *Irresistible Integrals*, Cambridge University Press, New York, 2004.

[4] L. Carlitz, *Congruences for generalized Bell and Stirling numbers*, Duke Math. J. **22** (1955), 193–205.

[5] S. De Wannemacker, *On 2-adic orders of Stirling numbers of the second kind*, INTEGERS **5(1)** (2005), #A21.

[6] Y. H. Kwong, *Minimum periods of $S(n, k)$ modulo M*, Fibonacci Quart. **27** (1989), 217–221.

[7] T. Lengyel, *On the 2-adic order of Stirling numbers of the second kind and their differences*, FPSAC, Hagensburg, Austria, DMTCS proc. **AK** (2009), 563–574.

[8] T. Lengyel, *On the divisibility by 2 of the Stirling numbers of the second kind*, Fibonacci Quart. **32** (1994), 194–201.

[9] A. T. Lundell, *A divisibility property for Stirling numbers*, J. Number Theory **10** (1978), 35–54.

[10] PARI/GP, version `2.3.4`, Bordeaux (2008), `http://pari.math.u-bordeaux.fr/`

[11] N. J. A. Sloane, Ed. *The On-Line Encyclopedia of Integer Sequences* (2008), published electronically at `www.research.att.com/ njas/sequences/`

[12] Z.-W. Sun, *Combinatorial congruences and Stirling numbers*, Acta Arith. **126** (2007), no. 4, 387–398.

[13] M. Sved, *Divisibility—with visibility,* Math. Intelligencer 10 (1988), 56–64.

[14] S.-L. Yang and H. You, *On a connection between the Pascal, Stirling, and Vandermonde matrices*, Discrete Appl. Math. **155** (2007), 2025–2030.

School of Mathematical and Physical Sciences, University of Newcastle, Callaghan, New South Wales, 2308, Australia

E-mail address: `math@oyeat.com`

Department of Mathematics and Computer Science, Virginia Wesleyan College, 1584 Wesleyan Drive, Norfolk, Virginia, 23502, USA

E-mail address: `dmanna@vwc.edu`