On the least significant 2-adic and ternary digits of certain Stirling numbers

Tamas Lengyel, Occidental College
ON THE LEAST SIGNIFICANT 2-ADIC AND TERNARY DIGITS OF CERTAIN STIRLING NUMBERS

Tamás Lengyel
Mathematics Department, Occidental College, Los Angeles, California
lengyel@oxy.edu

Received: 1/4/13, Accepted: 7/1/13, Published: 8/12/13

Abstract
Our main goal is to effectively calculate the p-ary digits of certain Stirling numbers of the second kind. We base our study on an observation regarding these numbers: as m increases, more and more p-adic digits match in $S(i(p - 1)p^m, k)$ with integer $i \geq 1$.

1. Introduction
Let $n$ and $k$ be positive integers, $p$ be a prime, $d_p(k)$ and $\nu_p(k)$ denote the sum of digits in the base $p$ representation of $k$ and the highest power of $p$ dividing $k$, i.e., the $p$-adic order of $k$, respectively. For the rational $n/k$ we set $\nu_p(n/k) = \nu_p(n) - \nu_p(k)$.

In 1808, Legendre showed

**Lemma 1.** ([2]) For any positive integer $k$, we have $\nu_p(k!) = (k - d_p(k))/(p - 1)$.

We define the 2-free part of $k$! (or unit factor of $k!$ with respect to 2), $b_k$, as $k! = 2^{k-d_2(k)}b_k,$ or more explicitly,

$$b_k = \prod_{3 \leq p \leq k \atop p \text{ prime}} p^{k-d_p(k)}/k-1.$$  

In general, $b_k$ is the $p$-free part of $k$! (or unit factor of $k!$ with respect to $p$), i.e., $k! = p^{k-d_{p'}(k)}/p' - 1$ b_k$ with

$$b_k = \prod_{p' \leq k \atop p' \text{ prime}} p^{k-d_{p'}(k)}/p' - 1.$$  

We have the identity (cf. [1]) for the Stirling numbers of the second kind

$$S(n, k) = \frac{1}{k!} \sum_{j=0}^{k} \binom{k}{j} (-1)^j (k-j)^n.$$
Our main goal is to effectively calculate the $p$-ary digits of certain Stirling numbers of the second kind. For example, if $k = 2$ then $S(m, 2) = 2^{m-1} - 1, m \geq 2$; thus, the binary representation consists of all ones. We try to find similar properties for other values of $k$. We base our study on an observation (cf. [6]) regarding these numbers: as $m$ increases, more and more $p$-adic digits match in $S(i(p - 1)p^m, k)$ with integer $i \geq 1$.

We claim the main results (cf. Theorems 2, 4, and 5) in Section 2, and illustrate and prove them in Sections 3-5. We discuss the case with $p = 2$ in Sections 3 and 4 and derive additional results (cf. Lemmas 8 and 9). A general approach is presented in Section 4. Options and limitations (cf. Theorems 12-18 based on [4] and [6]) for other primes are discussed in Section 5. Two examples are provided to demonstrate the cases of 2-adic and ternary digits.

2. Main Results

First, we deal with the binary digits and obtain

**Theorem 2.** With the above introduced notation,

\[ S(2^m, k) = \frac{1}{k!} \sum_{0 < j < k \text{ odd}} \binom{k}{j} (-1)^j (k - j)^{2^m_i} \]

\[ \equiv 2^{d_2(k) - 1} (-1)^{k-1} b_k^{2^{m-1}} \mod 2^{m+2-2k+d_2(k)} \quad \text{(2.1)} \]

for $m + 2 \geq k - d_2(k)$, $m \geq 2$, and $i \geq 1$.

**Remark 3.** Recall that (2.1) implies that $\nu_2(S(2^m, k)) = d_2(k) - 1$ if $d_2(k) - 1 < m + 2 - k + d_2(k)$, i.e., $m \geq k - 2$, cf. [5] and [7] for the generalized version.

We make the calculation more explicit in Theorem 4 and generalize it for $p = 3$ in Theorem 5, and in Theorems 12 and 17, in general.

We set $u_k = b_k \equiv b_k^{-1} \mod 4$ to be the least positive residue of the 2-free part $b_k$ of $k!$ modulo 4 which is the same as that of its inverse modulo 4,

\[ c_k = \begin{cases} -1, & \text{if } u_k = 3, \\ +1, & \text{if } u_k = 1, \end{cases} \]

and

\[ a_k = \begin{cases} \left\lfloor \frac{b_k}{4} \right\rfloor, & \text{if } u_k = 3, \\ \left\lfloor \frac{b_k}{4} \right\rfloor - 1, & \text{if } u_k = 1, \end{cases} \quad \text{(2.2)} \]

which yields that $b_k = 4a_k + c_k$. We end up with the following theorem that gives $S(2^m, k)$ explicitly, modulo a high power of two, and in terms of $k$, $m$, and $r$ ($r \geq 0$ integer).
Theorem 4. With the above introduced notation, for \( k \geq 3 \) we have
\[
S(2^m i, k) \equiv 2^{d_2(k)-1}(-1)^{k-1}c_k \sum_{j=0}^{r} (\text{mod } 2^{e(m,k,r)})
\]
with \( e(m,k,r) = \min\{m+2-k+d_2(k),(r+1)(2+\nu_2(a_k)) + d_2(k) - 1\} \).

With \( p = 3 \), we set \( u_k \equiv b_k \equiv b_k^{-1} \mod p \) to be the least positive residue of the \( p \)-free part \( b_k \) of \( k! \) modulo \( p \), which is the same that of its inverse modulo \( p \),
\[
c_k = \begin{cases} 
-1, & \text{if } u_k = p - 1, \\
+1, & \text{if } u_k = 1,
\end{cases}
\]
and
\[
a_k = \begin{cases} 
\left[ \frac{b_k}{p} \right], & \text{if } u_k = p - 1, \\
\left[ \frac{b_k}{p} \right] - 1, & \text{if } u_k = 1,
\end{cases}
\]
which yields that \( b_k = p \cdot a_k + c_k \). We get that

Theorem 5. For \( p = 3 \) and \( k \equiv 2 \) or \( 4 \) \( \pmod{6} \), we have
\[
S(i(p-1)p^m, k) \equiv \sum_{j=0}^{r} \left(\text{mod } p^{e(m,k,r)}\right)
\]
where
\[
e(m,k,r) = \min\{m+1 - \frac{k-d_2(k)}{p-1}, m+1 + v_p(a_k) + \frac{d_2(k)}{p-1} - 1, \]
\[
(r+1)(1+v_p(a_k)) + \frac{d_2(k)}{p-1} - 1\}.
\]

3. Proof of Theorem 2

We need a well-known theorem and two lemmas.

Theorem 6. (Kummer, 1852) The power of a prime \( p \) that divides the binomial coefficient \( \binom{\nu}{k} \) is given by the number of carries when we add \( k \) and \( n-k \) in base \( p \).

The first lemma is an improvement of the Fermat–Euler Theorem which claims only that \( t^{2^m+1} \equiv 1 \mod 2^{m+2} \) for \( p = 2, m \geq 0 \), and \( t \geq 1 \) odd.

Lemma 7. (Lemma 3 in [3]) For any integer \( m \geq 1 \) and any odd integer \( t \),
\[
t^{2^m} \equiv 1 \mod 2^{m+2}.
\]
This lemma can be proven by induction on \( m \) and further generalized to higher 2-power moduli (cf. [3]). The following lemma is an improvement of the well-known congruence \( \left( \frac{p^t - 1}{j} \right) \equiv (-1)^j \mod p, 0 \leq j \leq p^t - 1 \) for prime \( p \) and \( t \geq 1 \) integer.

**Lemma 8.** If \( p \) is a prime, \( (a, p) = 1 \), \( t \geq 1 \), and \( 1 \leq j \leq p^t - 1 \), then

\[
\nu_p \left( \left( \frac{ap^t}{j} \right) \right) = t - \nu_p(j)
\]

and

\[
\left( \frac{ap^t - 1}{j} \right) \equiv (-1)^j \mod p^{t - \lfloor \log_p j \rfloor}.
\]

**Proof.** Clearly, identity (3.1) is true by Theorem 6. Using the fact that \( \left( \frac{ap^t - 1}{0} \right) = 1 \) and

\[
\left( \frac{ap^t}{j} \right) = \left( \frac{ap^t - 1}{j - 1} \right) + \left( \frac{ap^t - 1}{j} \right),
\]

it implies that

\[
\left( \frac{ap^t - 1}{j} \right) \equiv (-1)^j \mod p^{t - \lfloor \log_p j \rfloor}
\]

by step-by-step increasing \( j \) from \( j = 1 \) on. \( \square \)

**Proof of Theorem 2.** The proof relies on the fact that terms with \( k - j \) even will not contribute to the congruence since \( 2^m \geq m + 2 \) as \( m \geq 2 \), and on Lemma 7, since

\[
\frac{1}{k!} \sum_{j=0}^{k} \left( \frac{k}{j} \right) (-1)^j (k-j)^{2^m} \equiv \frac{1}{k!} (-1)^{k-1} \sum_{j=0}^{k} \left( \frac{k}{j} \right) \equiv \frac{(-1)^{k-1} 2^{k-1}}{2^{k-d_2(k)} b_k} \mod 2^{m+2-k-d_2(k)}.
\]

Note that since \( b_k \) is odd, \( b_k^{-1} \equiv b_k^{2^{m-1}} \mod 2^{m+2} \) by Lemma 7. \( \square \)

We note that it is easy to see that

\[
S(n, 5) = \frac{1}{24} (5^{n-1} - 4^n + 2 \cdot 3^n - 2^{n+1} + 1)
\]

holds which yields

\[
S(2^m, 5) \equiv 2 \cdot 15^{2^{m-1}} \mod 2^{m-1}
\]

for \( i, m \geq 1 \). Indeed, we have

\[
3^{-1} \equiv 3^{2^m-1} \equiv 3^{2^{m-1}},
\]

\[
5^{-1} \equiv 5^{2^m-1} \equiv 5^{2^{m-1}} \mod 2^{m+2}.
\]
and
\[ S(2^m i, 5) = \frac{1}{8} \cdot \frac{1}{3} \cdot \left( 5^{2^m i} + 10 \cdot 3^{2^m i} + 5 \right) \equiv \frac{1}{15} \mod 2^{m-1} \]

by identity (3.2) and Lemma 7, if \( m \geq 1 \) and \( i \geq 1 \), with direct calculations and without using Theorem 2. Moreover, we get

**Lemma 9.** For any integer \( r \geq 0 \) and \( i, m \geq 1 \), we have
\[ S(2^m i, 5) \equiv -2 \sum_{j=0}^{r} 2^{4j} \mod 2^{\min\{m-1, 4r+5\}}. \tag{3.4} \]

**Proof of Lemma 9.** In fact, the statement holds if \( 2^m i < 5 \). Otherwise, we rewrite
\[ 15^{2^{m-1}} = (4^2 - 1)^{2^{m-1}} = -1 + \binom{2^{m-1}}{1}4^2 - \binom{2^{m-1}}{2}4^4 + \cdots \]
\[ \equiv - \sum_{j=0}^{r} 2^{4j} \mod 2^{\min\{m+4, 4r+4\}} \]

by Lemma 8, which already implies (3.4) by (3.3) since \( m + 2 - k + d_2(k) = m - 1 \). \( \square \)

The congruence (3.4) guarantees that the binary representation of \( S(2^m i, 5) \) ends in \((0111)^*011110\) if \( m \) is large enough. (With \( d \) being any finite word formed over the alphabet \( \{0, 1\} \), \( (d)^* \) denotes any finite number \( t, t \geq 0 \), of copies of the “word” \( d \).) If \( r = 0 \) and \( m \geq 6 \) then we have
\[ S(2^m i, 5) \equiv 30 \mod 32. \]
If \( r \geq (m - 6)/4 \) then the congruence (3.4) turns into
\[ S(2^m i, 5) \equiv -2 \sum_{j=0}^{r} 2^{4j} \mod 2^{m-1}, \]
and the terms beyond \( j = \lceil (m - 6)/4 \rceil \) effectively do not contribute to the sum.

### 4. 2-adic Digits: A General Approach for Effective Calculation and the Proof of Theorem 4

If \( k = 5 \) then we get \( d_2(5) = 2, b_5 = 15 \) and \( S(2^m i, 5) \) satisfies congruence (3.3) by Theorem 2. For larger values of \( k \), we use (4.1) below since we do not need the exact value of \( b_k \). In fact, to effectively calculate \( S(2^m i, k) \) modulo a large 2-power, it suffices to use \( b_k \) modulo that 2-power. It can be calculated by the congruence
\[ b_k = \frac{k!}{p^{\sum_{j \geq 1} \frac{k}{p^j}}} \equiv \delta \sum_{j \geq 1} \frac{k}{p^j} \prod_{j \geq 0} (K_j)_p \mod p^\delta, \tag{4.1} \]
with \( \delta = \delta(p^j) = -1 \) except if \( p = 2, q \geq 3 \) when \( \delta = 1 \), \( K_j \) is the least positive residue of \( [k/p^j] \mod p^j \), 0 \( \leq j \leq d \), if \( p^d \leq k < p^{d+1} \), and

\[
(K!)_p = \frac{K!}{p^{[k/p]!}}
\]

is the product of those positive integers not exceeding \( K \) that are not divisible by \( p \); cf. [2, Proposition 1, p8]. With \( p = 2 \), we have \( \delta = 1 \) if \( q \) is large enough. This implies that

\[b_k \equiv \prod_{j \geq 0} (K_j!)_2 \mod 2^q.\]

Now we can gain a more in-depth look at the binary digits of \( S(2^m i, k) \) by evaluating the right-hand side of (2.1) more effectively via Theorem 4.

**Proof of Theorem 4.** In a similar fashion to the case with \( k = 5 \) and depending upon \( u_k \mod 4 \), we rewrite

\[
b_k^{2^m-1} = (4a_k + c_k)^{2^m-1} = c_k + \binom{2^m-1}{1}(4a_k)c_k^2 + \binom{2^m-1}{2}(4a_k)^2(c_k)^3 + \cdots
\]

\[
\equiv c_k \sum_{j=0}^r (-4a_k c_k)^j \mod 2^{\min\{m + 2 + \nu_2(a_k) + (r + 1)(2 + \nu_2(a_k))\}}
\]

by Lemma 8, which already implies (2.3) by Theorem 2 since \( \min\{m + 2 - k + d_2(k), m + 2 + \nu_2(a_k) + d_2(k) - 1, (r + 1)(2 + \nu_2(a_k)) + d_2(k) - 1\} = \min\{m + 2 - k + d_2(k), (r + 1)(2 + \nu_2(a_k)) + d_2(k) - 1\}. \]

**Example 10.** For \( k = 3, 4, 5, \) and \( 7 \), we get \( b_3 = b_4 = 3, b_5 = 15, b_7 = 315, u_k = 3 \), \( c_k = -1, a_3 = a_4 = 1, a_5 = 4, \) and \( a_7 = 79 \), which yield that

\[
S(2^m, 3) \equiv -2 \sum_{j=0}^r 4^j \mod 2^{\min\{m + 1, 2(r + 1) + 1\}},
\]

\[
S(2^m, 4) \equiv -2 \sum_{j=0}^r 4^j \mod 2^{\min\{m - 1, 2(r + 1)\}},
\]

\[
S(2^m, 5) \equiv -2 \sum_{j=0}^r 16^j \mod 2^{\min\{m - 1, 4(r + 1) + 1\}},
\]

in agreement with (3.4), and

\[
S(2^m, 7) \equiv -2^2 \sum_{j=0}^r 316^j \mod 2^{\min\{m - 2, 2(r + 1) + 2\}}.
\]
On the other hand, if \( k = 6 \) then \( b_6 = 45, u_6 = 1, c_6 = 1, a_6 = 11, \) and
\[
S(2^m, 6) \equiv -2^2 \sum_{j=0}^r (-44)^j \mod 2^{\min\{m-2, 2(r+1)+1\}}.
\]

**Remark 11.** Note that the “best use” of the congruence (2.3) comes with values of \( a_k \) that are powers of two, e.g., if \( k = 3, 4, 5, \) etc. It will be interesting to see the general solution to this problem, i.e., find all \( k \) so that \( a_k \), which is derived from the 2-free part \( b_k \) of \( k! \) by (2.2), is a power of two. Indeed, beyond the small cases, we look for any \( k \geq 4 \), for which \( k! \) is the difference or sum of two powers of two (depending on the sign of \( c_k \)), or equivalently, whose binary representation is of the form \( 1(0)^*1(0)^*0 \) or \( 1(1)^*(0)^*0 \). This follows by the identity \( k! = 2^{k-d_2(k)}b_k = 2^{k-d_2(k)}(4k + c_k) \). (Of course, for \( k \geq 2 \), we get an even \( k! \) so it must end with a binary zero.)

5. Other primes

As \( m \) increases, more and more \( p \)-adic digits match in \( S(i(p-1)p^m, k) \). However, to effectively calculate these matching digits we need another approach. We rely on papers [4] and [6]. We need the following combination of Lemma 5 and Theorem 3 of [4]. This helps in generalizing Theorem 4 for odd primes if \( k \) is divisible by \( p-1 \).

**Theorem 12.** ([4]) For any odd prime \( p \), integer \( t \), \( n = i(p-1)p^m \), \( 1 \leq k \leq n \), and \( m > \frac{k}{p-1} - 2 \), we have
\[
(-1)^{k+1}k!S(n, k) \equiv \sum_{p|k} \binom{k}{i}(-1)^i \mod p^{m+1}
\]
and
\[
\sum_{i \equiv k \mod p} \binom{k}{i}(-1)^i \equiv \begin{cases} (-1)^{\frac{k}{p-1} - 1}p^\frac{k}{p-1} - 1 \mod p^\frac{k}{p-1}, & \text{if } k \text{ is divisible by } p-1, \\ 0 \mod p^\frac{k}{p-1}, & \text{otherwise.} \end{cases}
\]

Therefore, if \( k \) is divisible by \( p-1 \) then
\[
S(n, k) \equiv p^{\frac{d_p(k)}{p-1} - 1}(-1)^{\frac{k}{p-1}}b_k^{-1} \mod p^{\min\{m+1 - \frac{k-d_p(k)}{p-1}, \frac{d_p(k)}{p-1}\}}
\]
where \( b_k \) is the \( p \)-free part of \( k! \) as defined in the introduction and by the Fermat–Euler Theorem
\[
b_k^{-1} \equiv b_k^{(p-1)p^{m-1}} \mod p^{m+1}.
\]
Remark 13. Note that the \( p \)-adic order of \( S(i(p-1)p^m,k) \) does not depend on \( i \) and \( m \). This does not exclude the possibility that by increasing \( m \) we can get more insight into the base \( p \) representation of \( S(i(p-1)p^m,k) \). Indeed, if \( p = 2 \) then (2.1) provides us with the right tool since \( \sum_{j|i} \binom{k}{i}(-1)^i = 2^k-1, \) and it leads to Theorem 4. However, in general, increasing \( m \) does not help in getting more \( p \)-ary digits in a computationally effective way, for (5.2) cannot be significantly improved; although, according to Theorem 17, we get more and more matching digits in \( S(i(p-1)p^m,k) \) and \( S(i(p-1)p^{m+1},k) \) (starting with the least significant bit). We can avoid the use of (5.2) if a closed form exists for \( \sum_{j|i} \binom{k}{i}(-1)^i \) in (5.1), at least for some \( k \), e.g., if \( p = 3 \) or 5.

In fact, for example, if \( k \) is even and \( 3 \nmid k \), we get that \( \sum_{j|i} \binom{k}{i}(-1)^i = (-1)^{k/2+1}3^{k/2-1} \). Theorem 5 provides us with a tool to calculate the ternary digits of \( S(i(p-1)p^m,k) \) if \( k \equiv 2 \) or 4 \((\text{mod } 6)\). Its proof is a straightforward generalization of that of Theorem 4. We demonstrate its use in the next example.

Example 14. If \( p = 3 \) then \( u_k \equiv b_k \equiv b_k^{-1} \) mod 3 is the least positive residue of the 3-free part \( b_k \) of \( k! \) modulo 3 which is the same as that of its inverse modulo 3. For instance, if \( k = 4 \) we get then \( b_4 = 8, u_k = 2, c_4 = -1 \) and

\[
a_4 = \left\lfloor \frac{b_4}{3} \right\rfloor = 3,
\]

which yields that \( b_4 = 9 - 1 \). We obtain that

\[
S(2i \cdot 3^m,4) \equiv - \sum_{j=0}^r 3^{2j} \mod 3^{\nu(3,m,r)} \tag{5.3}
\]

with

\[
e(m,4,r) = \min\{m+1 - \frac{4 - d_3(4)}{2}, m+1 + \nu_3(3) + \frac{d_3(4)}{2} - 1, (r+1)(1 + \nu_3(3)) + \frac{d_3(4)}{2} - 1\}
= \min\{m, 2(r+1)\}.
\]

This implies that \( S(2i \cdot 3^m,4) \) ends in \((12)^*122\) in base 3.

Remark 15. Since \( k! = 3^{\frac{k-d_3(k)}{2}} b_k = 3^{\frac{k-d_3(k)}{2}} (3a_k + c_k) \) we get the “best use” of Theorem 5 when \( a_k \) is a power of three, i.e., when \( k! \) is the difference or sum of two powers of three. For example, in Example 14, \( 4! = 24 = 3^3 - 3 \) leads to (5.3).

Remark 16. In a similar fashion to the case with \( p = 3 \), if \( p = 5 \) then we can use the fact that \( \sum_{j|i} \binom{k}{i}(-1)^i \) can be expressed explicitly in terms of Fibonacci or Lucas numbers, with a formula depending on \( k \) modulo 20 (cf. [4]).
The idea of getting more $p$-ary digits of $S(i(p-1)p^m, k)$ by increasing $m$ is well supported and the rate of increase is made effective by the following theorem which is based on Theorems 11 and 14 of [6]. This theorem can be used in getting the digits successively although not in a direct fashion as in (2.3), (2.4), and (5.3).

**Theorem 17.** Let $p \geq 2$ be a prime, $c, n, k \in \mathbb{N}$ with $1 \leq k \leq p^n$ and $(c, p) = 1$, and $u$ be a nonnegative integer, then

$$
\nu_p(S(cp^n+1 + u, k) - S(cp^n + u, k)) \geq n - \lfloor \log_p k \rfloor + 2.
$$

It was also conjectured in Conjecture 2 in [6] that for $n, k \in \mathbb{N}$, $3 \leq k \leq 2^n$, and $c \geq 1$ odd integer, we have

$$
\nu_2(S(c2^n+1, k) - S(c2^n, k)) = n + 1 - f(k)
$$

for some function $f(k)$ which is independent of $n$ (for any sufficiently large $n$). In fact, for small values of $k$, numerical experimentation suggests that

$$
f(k) = 1 + \lfloor \log_2 k \rfloor - d_2(k) - \gamma(k),
$$

with $\gamma(4) = 2$ and otherwise it is zero except if $k$ is a power of two or one less, in which cases $\gamma(k) = 1$. This would imply that $f(k) \geq 0$, cf. [6].

In connection with Theorem 12, we note that if $k$ is divisible by $p - 1$ then $k/p$ is not an odd integer. On the other hand, if $k/p$ is an odd integer then we observe a behavior which is somewhat different from that of Theorem 12.

**Theorem 18.** (Theorem 2 in [4]) For any odd prime $p$, if $k/p$ is an odd integer then $\nu_p(k!S(i(p-1)p^m, k)) > m$.

**Acknowledgment** The author wishes to thank Gregory P. Tollisen and the referee for helpful comments that improved the presentation of the paper.

**References**


