Stirling Numbers of the Second Kind and Primality

Joe DeMaio
Department of Mathematics and Statistics
Kennesaw State University, Kennesaw, Georgia, 30144, USA
jdemaio@kennesaw.edu
770 423-6568

Stephen Touset
stephen@touset.org

April 21, 2008

Abstract

A Stirling number of the second kind is a combinatorial function which yields interesting number theoretic properties with regard to primality. The Stirling number of the second kind, $S(n,k) = \frac{1}{k!}\sum_{i=0}^{k}(-1)^i\binom{k}{i}(k-i)^n$, counts the number of partitions of an n-element set into k non-empty subsets. A Stirling prime (of the second kind) is a prime p such that $p = S(n,k)$ for some integers n and k. The relationship between Mersenne primes and Stirling primes will be shown. Divisibility theorems with regard to primality will be stated and used to devise algorithms for accelerated searching of Stirling primes. Search results for $1 \leq n \leq 100000$ and $1 \leq k \leq 6$ will be presented.

Keywords: Number Theory, Stirling Numbers of the Second Kind, Primality

1 Introduction

Stirling numbers of the second kind are combinatorial functions similar to Bell numbers. The Bell number, B_n, enumerates the number of partitions of n elements into non-empty subsets. The Stirling number of the second kind, $\left\{ n \atop k \right\}$ or $S(n,k)$ [1] , is the number of partitions of an n-element set into k non-empty

[1] For the purposes of this paper, the more descriptive notation for Stirling numbers of the second kind, $\left\{ n \atop k \right\}$, will be utilized. Stirling numbers of the second kind count the number of partitions of an n-element set into k non-empty subsets. Stirling numbers of the first kind count the number of different permutations of n elements into k disjoint cycles. First devised by Karamata [1] and practiced by Knuth [2], $\left\{ n \atop k \right\}$, provides a visual cue to differentiate

subsets. Thus, $B_n = \sum\limits_{k=1}^{n} \left\{ {n \atop k} \right\}$. The symbol, $\left\{ {n \atop k} \right\}$, is read as 'n subset k.' For example, $\left\{ {4 \atop 2} \right\} = 7$ since there exist seven different ways to partition the set $S = \{1, 2, 3, 4\}$ into two non-empty subsets.

{{1,2,3},{4}}	{{1,2,4},{3}}	{{1,3,4},{2}}	{{2,3,4},{1}}
{{1,2},{3,4}}	{{1,3},{2,4}}	{{1,4},{2,3}}	

All Partitions of $S = \{1, 2, 3, 4\}$ into Two Non-empty Subsets

The general formula for computing the Stirling number of the second kind is

$$\left\{ {n \atop k} \right\} = \frac{1}{k!} \sum_{i=0}^{k} (-1)^i \binom{k}{i} (k-i)^n \tag{1}$$

and a very frequently used recursive identity is

$$\left\{ {n \atop k} \right\} = \left\{ {n-1 \atop k-1} \right\} + k \left\{ {n-1 \atop k} \right\}. \tag{2}$$

$\left\{ {n \atop k} \right\}$	1	2	3	4	5	6	7	8	9	10	11	12
1	1											
2	1	1										
3	1	3	1									
4	1	7	6	1								
5	1	15	25	10	1							
6	1	31	90	65	15	1						
7	1	63	301	350	140	21	1					
8	1	127	966	1701	1050	266	28	1				
9	1	255	3025	7770	6951	2646	462	36	1			
10	1	511	9330	34105	42525	22827	5880	750	45	1		
11	1	1023	28501	145750	246730	179487	63987	11880	1155	55	1	
12	1	2047	86526	611501	1379400	1323652	627396	159027	22275	1705	66	1

Some Initial Values of $\left\{ {n \atop k} \right\}$

The sequence of Bell numbers has been searched for primes [7].[2] How about searching Stirling numbers of the second kind for primes? A cursory glance at a table of Stirling numbers of the second kind quickly yields some prime numbers

between itself and Stirling numbers of the first kind, $\left[{n \atop k} \right]$. This notation is much more distinct and easier to remember than the standard $S(n, k)$ and $s(n, k)$.

[2] The Bell number, B_n, is known to be prime for $n = 2, 3, 7, 13, 42, 55, 2841$. The 6531 digit integer B_{2841} was discovered as a probable prime in 2002 and proven prime in 2004.

and a search does not seem to be a pointless exercise. A Stirling prime (of the second kind) is a prime p such that $p = S(n,k)$ for some integers n and k. Thus, $\left\{{6 \atop 2}\right\} = 31$ and $\left\{{16 \atop 4}\right\} = 171798901$ are both examples of Stirling primes (of the second kind).

How might we reasonably search through the sequence? We'll use the time honored technique of throwing out as many known composites as possible.

2 Divisibility of $\left\{{n \atop k}\right\}$ by primes

In order to show that $\left\{{n \atop k}\right\}$ is composite it is unnecessary to determine the complete prime factorization of $\left\{{n \atop k}\right\}$. Just knowing that a single small (relative to the size of $\left\{{n \atop k}\right\}$) prime p divides $\left\{{n \atop k}\right\}$ will be sufficient to disprove primality. The rate of growth of $\left\{{n \atop k}\right\}$ quickly precludes us from concern that $\left\{{n \atop k}\right\} = p$ for some small prime p for $k \geq 3$ as in the case of $\left\{{3 \atop 2}\right\} = \binom{3}{2} = 3$.

Theorem 1 *If p is prime then $p | \left\{{p \atop k}\right\}$ for all $2 \leq k \leq p-1$. Furthermore, $p \nmid \left\{{p \atop 1}\right\}, \left\{{p \atop p}\right\}$.*

Proof. We wish to show that $\left\{{p \atop k}\right\} \equiv 0 \mod p$ for any prime p and $2 \leq k \leq p-1$. Since $k \leq p-1$, $p \nmid k!$ and it will suffice to show that $\sum\limits_{i=0}^{k} (-1)^i \binom{k}{i} (k-i)^p \equiv 0$. By Fermat's Little Theorem, $a^{p-1} \equiv 1 \mod p$ and $a^p \equiv a \mod p$ for all a and prime p. Thus $\sum\limits_{i=0}^{k} (-1)^i \binom{k}{i} (k-i)^p \equiv \sum\limits_{i=0}^{k} (-1)^i \binom{k}{i} (k-i) \mod p$. Note that $\binom{k}{i}(k-i) = k\binom{k-1}{i}$ and $\sum\limits_{i=0}^{k} (-1)^i \binom{k}{i} (k-i) \equiv \sum\limits_{i=0}^{k} (-1)^i k\binom{k-1}{i} \equiv k \sum\limits_{i=0}^{k} (-1)^i \binom{k-1}{i} \mod p$. Since $\binom{k-1}{k} = 0$ the last term can be dropped and rewritten as $k \sum\limits_{i=0}^{k-1} (-1)^i \binom{k-1}{i}$. This sum $\sum\limits_{i=0}^{k-1} (-1)^i \binom{k-1}{i} = 0$ by the binomial theorem. Finally, since $\left\{{p \atop 1}\right\} = \left\{{p \atop p}\right\} = 1$, it is clear that p divides neither. ■

Theorem 1 shows that 5 divides $\left\{{5 \atop 2}\right\}$, $\left\{{5 \atop 3}\right\}$ and $\left\{{5 \atop 4}\right\}$ but not $\left\{{5 \atop 1}\right\}$, $\left\{{5 \atop 5}\right\}$. In fact, divisibility by 5 can be extended further past row five in our table by making iterated applications of Equation 2.

Theorem 2 *If p is prime then $p | \left\{{p+1 \atop k+1}\right\}$ for all $2 \leq k \leq p-1$. Furthermore $\left\{{p+1 \atop 2}\right\} \equiv 1 \mod p$.*

Proof. Since $p | \left\{{p \atop k}\right\}$ for all $2 \leq k \leq p-1$ then $p | \left\{{p+1 \atop k+1}\right\} = \left\{{p \atop k}\right\} + (k+1)\left\{{p \atop k+1}\right\}$ for $2 \leq k \leq p-2$. For $k = p-1$, $p | \left\{{p+1 \atop k+1}\right\}$ since $p | \left\{{p \atop k}\right\}$ and $p | (k+1)$. Finally, $\left\{{p+1 \atop 2}\right\} = \left\{{p \atop 1}\right\} + 2\left\{{p \atop 2}\right\} = 1 + 2\left\{{p \atop 2}\right\}$. Since $p | \left\{{p \atop 2}\right\}$ then $\left\{{p+1 \atop 2}\right\} \equiv 1 \mod p$. ■

Theorem 2 now shows that 5 divides $\left\{ {6 \atop 3} \right\}$, $\left\{ {6 \atop 4} \right\}$ and $\left\{ {6 \atop 5} \right\}$ but $5 \nmid \left\{ {6 \atop 2} \right\}$. Of course the same recursive Equation 2 can be applied not just to $\left\{ {p+1 \atop k} \right\}$ but to $\left\{ {p+j \atop k} \right\}$ for $j \geq 2$. Now, however, for each increase in the size of j, one fewer of $\left\{ {p+j \atop k+j} \right\}$ is divisible by p due to the fact that two previous terms divisible by p are needed for each successive term divisible by p. Extending Theorem 2 and its proof technique yields the next theorem.

Theorem 3 *If p is prime then $p | \left\{ {p+j \atop k+j} \right\}$ for all $1 \leq j \leq p-2$ and $2 \leq k \leq p-j$. Furthermore $\left\{ {p+j \atop j+1} \right\} \equiv 1 \mod p$ for all $2 \leq j \leq p-2$.*

Proof of Theorem 3 is similar to the proof of Theorem 2 and yields no new insight. Theorem 3 iteratively shows that 5 divides $\left\{ {6 \atop 3} \right\}$, $\left\{ {6 \atop 4} \right\}$, $\left\{ {6 \atop 5} \right\}$, $\left\{ {7 \atop 4} \right\}$, $\left\{ {7 \atop 5} \right\}$ and $\left\{ {8 \atop 5} \right\}$ but $5 \nmid \left\{ {6 \atop 2} \right\}$, $\left\{ {7 \atop 3} \right\}$ and $\left\{ {8 \atop 4} \right\}$. Divisibility by 5 does not stop here. The same pattern now repeats itself again and again.

Corollary 1 *If p is prime then $p | \left\{ {p+i(p-1) \atop k} \right\}$ for all $2 \leq k \leq p-1$ and $i \in \mathbb{Z}^+$.*

Proof. Note that $(k-1)^{p+i(p-1)} \equiv (k-1)^p (k-1)^{(p-1)^i} \equiv (k-1)^p \mod p$ by Fermat's Little Theorem and the proof is now reduced to that of Theorem 1. ■

Theorem 1 shows that 5 divides $\left\{ {5 \atop 2} \right\}$, $\left\{ {5 \atop 3} \right\}$ and $\left\{ {5 \atop 4} \right\}$. Corollary 1 extends the result to show that 5 also divides $\left\{ {9 \atop 2} \right\}$, $\left\{ {9 \atop 3} \right\}$ and $\left\{ {9 \atop 4} \right\}$, and $\left\{ {13 \atop 2} \right\}$, $\left\{ {13 \atop 3} \right\}$ and $\left\{ {13 \atop 4} \right\}$ and so on. Continued applications of Equation 2 and slight modifications of Theorems 2 and 3 show that the entire pattern is replicated infinitely many times.

Corollary 2 *If n is a composite number then there exists k, $2 \leq k \leq n-1$ such that $n \nmid \left\{ {n \atop k} \right\}$.*

Proof. *Let p be any prime factor of n and let $j = n-p$. Since n is composite, $2 \leq n-p \leq n-2$. Thus, by Theorem 3, $1 \equiv \left\{ {p+j \atop j+1} \right\} = \left\{ {p+(n-p) \atop (n-p)+1} \right\} = \left\{ {n \atop k} \right\} \mod p$. Hence $p \nmid \left\{ {n \atop k} \right\}$. Since $p|n$, it quickly follows that $n \nmid \left\{ {n \atop k} \right\}$. Furthermore, since $n-p \leq n-2$ then $2 \leq k = (n-p)+1 \leq n-1$.* ■

Due to Corollary 2 Theorem 1 can now be improved.

Theorem 4 *The positive integer n is a prime number if and only if $n | \left\{ {n \atop k} \right\}$ for all $2 \leq k \leq n-1$.*

3 Primality of $\left\{ {n \atop k} \right\}$

In light of all this divisibility it might appear that $\left\{ {n \atop k} \right\}$ is always composite. This is certainly not true. In fact the collection of values of n such that $\left\{ {n \atop 2} \right\}$ is prime is closely related to a quite well known collection of primes. For all n, $\left\{ {n \atop 2} \right\} = 2^{n-1} - 1$. Hence, for any Mersenne prime M_p, $\left\{ {p+1 \atop 2} \right\} = M_p$ and $\left\{ {n \atop 2} \right\}$ is composite for all other values. This immediately demonstrates the existence[3] of 44 different Stirling Numbers of the Second Kind that are prime. The search for Mersenne primes has an extensive mathematical history and does not need to be discussed here.

Are there other prime Stirling Numbers of the second kind? A Brute force search yields the aforementioned $\left\{ {16 \atop 4} \right\}$. However, brute force quickly stops yielding results. Clearly there is no need to check $\left\{ {n \atop 1} \right\} = \left\{ {n \atop n} \right\} = 1$. Furthermore $\left\{ {n \atop n-1} \right\} = \binom{n}{2} = \frac{n(n-1)}{2}$ which is clearly composite except at $n = 3$. Turning our attention to the theorems of the previous section yields a sieve technique to cast out composites. With very little computational effort we know many $\left\{ {n \atop k} \right\}$ that must be divisible by each small prime p and can remove such $\left\{ {n \atop k} \right\}$ from consideration for primality testing. For example for $p = 5$ we cast out the following values in bold.

$\left\{ {n \atop k} \right\}$	1	2	3	4	5	6	7	8	9	10	11	12
1	1											
2	1	1										
3	1	3	1									
4	1	7	6	1								
5	1	**15**	**25**	**10**	1							
6	1	31	**90**	**65**	**15**	1						
7	1	63	301	**350**	**140**	21	1					
8	1	127	966	1701	**1050**	266	28	1				
9	1	**255**	**3025**	**7770**	6951	2646	462	36	1			
10	1	511	**9330**	**34105**	**42525**	22827	5880	750	45	1		
11	1	1023	28501	**145750**	**246730**	179487	63987	11880	1155	55	1	
12	1	2047	86526	611501	**1379400**	1323652	627396	159027	22275	1705	66	1

Values of $\left\{ {n \atop k} \right\}$ Relative to Divisibilty by 5

Not every $\left\{ {n \atop k} \right\}$ divisible by 5 is cast out with this process but we can rid ourselves of many composite $\left\{ {n \atop k} \right\}$. Repeating this process for numerous small primes significantly reduces the number of $\left\{ {n \atop k} \right\}$ to check for primality. A quick sieve of $\left\{ {n \atop k} \right\}$ up to $n = 24$ yields the table below. If $\left\{ {n \atop k} \right\}$ has multiple prime divisors, only the largest prime is entered into its cell in the table. The character M represents a Mersenne prime that need not be checked. The character B represents the Stirling number $\left\{ {n \atop n-1} \right\} = \binom{n}{2} = \frac{n(n-1)}{2}$ which need not be checked. Of the 300 entries in this table, we are left with only 9 candidates to check for primality for $3 \le k \le n-2$. Of those 9 candidates, only $\left\{ {16 \atop 4} \right\}$ is prime.

[3] As of February 12, 2008

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
1	1																							
2	1	1																						
3	1	3	1																					
4	1	M	3	1																				
5	1	5	5	5	1																			
6	1	M	5	5	5	1																		
7	1	7	7	5	5	7	1																	
8	1	M	7	7	5	7	7	1																
9	1	M		7	7	7	7	B	1															
10	1	M	E		7	7	7		B	1														
11	1	11	11	11	11	7	7	11	11	11	1													
12	1	M	11	11	11	11	7	11	11	11	11	1												
13	1	13	13	11	11	11	11	11	11	11	11	13	1											
14	1	M	13	13	11	11	11	11	11	11	11	13	13	1										
15	1	M		13	13	11	11	11	11	11	11	13	13	B	1									
16	1	M	E		13	13	11	11	11	11	11	13	13		B	1								
17	1	17	17	17	17	13	13	11	11	11	11	13	13	17	17	17	1							
18	1	M	17	17	17	17	13	13	11	11	11	13	13	17	17	17	17	1						
19	1	19	19	17	17	17	17	13	13	11	11	13	13	17	17	17	17	19	1					
20	1	M	19	19	17	17	17	17	13	13	11	13	13	17	17	17	17	19	19	1				
21	1	M		19	19	17	17	17	17	13	13	13	13	17	17	17	17	19	19	B	1			
22	1	M	E		19	19	17	17	17	17	13	13	13	17	17	17	17	19	19		B	1		
23	1	23	23	23	23	19	19	17	17	17	17	13	13	17	17	17	17	19	19	23	23	23	1	
24	1	M	23	23	23	23	19	19	17	17	17	17	13	17	17	17	17	19	19	23	23	23	23	1

Known Composite Values of $\left\{{n \atop k}\right\}$

After sieving out known composites, an exhaustive search of $\left\{{n \atop k}\right\}$ for $1 \leq n \leq 100000$ and $1 \leq k \leq 6$ yielded three additional primes: $\left\{{40 \atop 4}\right\}$, $\left\{{1416 \atop 4}\right\}$ and $\left\{{10780 \atop 4}\right\}$.

4 Future Work

It seems unusual that we found Stirling primes of the form $\left\{{n \atop 2}\right\}$ and $\left\{{n \atop 4}\right\}$ but not $\left\{{n \atop 3}\right\}$. Is there perhaps some reason that $\left\{{n \atop 3}\right\}$ is always composite? By Equation 2, $\left\{{n \atop 3}\right\} = 5 * 2^{n-3} - 4 + 9\left\{{n-2 \atop 3}\right\}$ and since $\left\{{4 \atop 3}\right\} = 6$ then $\left\{{n \atop 3}\right\}$ is always even for all even $n \geq 4$. Similarly $\left\{{n \atop 3}\right\} = 65 * 2^{n-5} - 40 + 81\left\{{n-4 \atop 3}\right\}$ and $\left\{{5 \atop 3}\right\} = 25$ shows that $\left\{{n \atop 3}\right\} \equiv 0 \mod 5$ for $n \equiv 1 \mod 4$. Hence, $\left\{{n \atop 3}\right\}$ can be prime only for $n \equiv 3 \mod 4$. But so far, no prime values of $\left\{{n \atop 3}\right\}$ have been located. Nor does an obvious divisor pattern for $\left\{{n \atop 3}\right\}$ jump out for $n \equiv 3 \mod 4$. The factoring of $\left\{{15 \atop 3}\right\} = 227 * 10463$ and $\left\{{95 \atop 3}\right\} = 12707273 * 295097034961 * 94265058593107474994927717$ gives a glimmer of hope that $\left\{{n \atop 3}\right\}$ may be prime for some value of n.

Can we extend the divisibility pattern of Theorems 1, 2 and 3 widthwise across the table of Stirling numbers also? Perhaps. But it will not be as simple as extending this pattern lengthwise to an if and only if result as we did with Corollary 1. Such theorems would allow us to throw out more known composite values of $\left\{{n \atop k}\right\}$ extend a search with larger values of k.

References

[1] J. Karamata, "Theoremes sur la sommabilite exponentielle et d'autres sommabilites rattachant," Mathematica (Cluj) 9, 1935, 164-178.

[2] Graham, Knuth, Patashnik, Concrete Mathematics, Addison Wesley (Second Edition), Massachusetts 1994.

[3] F. Roberts, Applied Combinatorics, Prentice-Hall, New Jersey 1984.

[4] Roman, S. The Umbral Calculus, New York: Academic Press, pp. 59-63, 1984.

[5] K. Rosen, Elementary Number Theory, Addison Wesley (Third Edition), Massachusetts 1993.

[6] N. J. A. Sloane, (2007), The On-Line Encyclopedia of Integer Sequences, www.research.att.com/~njas/sequences/.

[7] http://www.research.att.com/~njas/sequences/A051130

[8] Weisstein, Eric W. "Bell Number." From MathWorld–A Wolfram Web Resource. http://mathworld.wolfram.com/BellNumber.html