7. Implementation, Statistics, and Questions

Since, we required divisors of integers in the interval $[1, 2P-1]$, the goal was to invoke these tabulation methods for all admissible $P < X$. One possible option was to have a precomputed factor-table of all integers less than $2X$. This single table could be used to check the admissibility of P and find the factors of $P - \delta_P$ and $\delta_q P - \delta_r D$ for any $P < X$. However, this table would be very space intensive. Instead, we opted for two incremental sieves and this uses only $O(\sqrt{P})$ space. If X is chosen using the cross-over method, this is $O(B^{1/6})$ space. One sieve was used to find admissible P and it always stored the factors of $P-1$ and $P+1$ so that the factors of $P - \delta_P$ would be accessible. For any admissible P, another incremental sieve was instantiated to factor integers in $[1, 2P-1]$ for the $\delta_q P - \delta_r D$ term. We used MPI to have this run in parallel, and striped the work by counting admissible P.

For the tabulations, we chose $X = 6 \cdot 10^6$. For every $P < X$, we used a hybrid approach combining both the CD method and the $D\Delta$ method; that is, for a given D we choose the inner-loop that would create fewer candidate values. The program computed all possible $n = Pqr$ and we used post-processing to eliminate $n > 2^{64}$. Our choice of X means that there are no cases for $k = 3$ that need to be accounted as large. We wrote 9 distinct programs for the large case (one for each $3 < k < 13$). There are two obvious ways to implement these programs. The first is to have k incremental sieves. Each sieve is instantiated to find primes starting at the prior incremental sieve's prime and going as large as $(B/P_j)^{1/(k-j)}$. While this is very space efficient, it seemed like there would be a lot of overhead. Instead, we used a precomputed list of primes in the interval $[1, \sqrt{B/X})$. If $X > B^{1/3}$, this requires $O(B^{1/3})$ storage. For each $k > 3$, we keep track of $k-1$ pointers in the array. At each level, we make sure that the implied product is bounds admissible. And at the $k-2$ level, we also insure that the product exceeds X. The code may be found at `https://github.com/Chelmreich/Absolute-Lucas-Pseudoprimes`.

7.1. Timing information for "small" preproducts

We implemented the $D\Delta$ method, the CD method, and a hybrid approach. All three programs were run on a single thread of a Xeon Phi 7210 1.30 GHz co-processor. The timing considered two different cases to highlight the strengths of each approach. The first case was $P < X$ and P is admissible. The second case limited P to being prime. As expected, the CD method is superior on prime inputs. For the admissible preproducts, the timing information seems to confirm that the CD method does not scale as well which would be expected.

The hybrid approach appears to not offer an advantage on the prime preproducts. The overhead of updating the sieve and divisor list is more expensive than the CD

method when D was large (relative to P). If this overhead could be avoided[4], we believe that the hybrid method would be better. But, due to our specific implementation, it was not possible to dynamically turn off the incremental sieve. A novel variant of the incremental sieve that increments in a backwards direction would be required. With these two sieves running simultaneously (one for the interval $[P+1, 2P-1]$ that runs forward and one for $[1, P-1]$ that runs backwards), it would have been possible to detect when the divisor counts were consistently larger than number of C values. At which point, we could turn off the incremental sieve and finish the computation with only the CD method.

Tables for timing data for the $D\Delta$, CD, and hybrid methods for all pre-products and prime preproducts up to varying bounds can be seen below.

We also implemented the small case to run only on bound admissible pre-products. For example, let $B = 10^{15}$. Then, it took 196 seconds to find the completions for preproducts in $[10^5 - 10^3, 10^5]$. And it only took 150 seconds for the interval $[10^5, 10^5 + 10^3]$. Even though the inputs on the first interval are smaller than the inputs on the second interval, the number of bound admissible preproducts decreases and so the computation finishes noticeably quicker.

7.2. Timing information for "large" preproducts

Tables 3 and 4 found below show the timing data on the same machine for finding absolute Lucas pseudoprimes. As expected, the timing impact of having a cross-over is seen more clearly in the smaller k values than the larger k values. As k gets larger, it becomes very rare that a product of $k-2$ primes will be less than X. Having the cross-over, as noted above, has an impact on the memory requirements if the computation assumes the existence of a look-up table. We did not measure the impact that storage might have for these relatively small bounds (in comparison to 2^{64}). One would probably need to abandon a look-up table approach if a cross-over was not used.

Tables 1 and 2 show the timing data for the $D\Delta$, CD, and hybrid methods for all pre-products and prime preproducts up to varying bounds.

The first table shows the timings for finding all such numbers with a fixed number of prime factors and the second table shows the timings when a cross-over of $X = B^{.35}$ is chosen.

7.3. Comparison to Carmichael numbers

We let $C_d(k, B)$ be the function that counts the number of absolute Lucas pseudoprimes less than B, where d is the discriminant of the family of Lucas sequences and k is the number of prime factors. There seems to be more absolute Lucas pseu-

[4]If a global look-up table had been employed, then the overhead is the look-up. We need the ability to dynamically turn off the incremental sieve.

Admissible pre-product bound	$D\Delta$	CD	Hybrid
$1 \cdot 10^3$	2	5	1
$2 \cdot 10^3$	7	32	6
$3 \cdot 10^3$	17	96	14
$4 \cdot 10^3$	33	213	25
$5 \cdot 10^3$	52	399	40
$6 \cdot 10^3$	77	653	59
$7 \cdot 10^3$	107	981	82
$8 \cdot 10^3$	142	1433	109
$9 \cdot 10^3$	183	1968	141
$10 \cdot 10^3$	231	2646	176

Table 1: (in seconds)

doprimes than Carmichael numbers. The presence of the product of twin primes plays a significant role in this count. Letting α be the least order of magnitude for which $\alpha > 1/3$ is 15 for Carmichael numbers. But for the other discriminants this threshold is crossed at $13, 8, 9$, and 11 (ordered by discriminant). We are not entirely sure why this is; our expectations was that the exclusion of primes dividing d from admissible preproducts would cause there to be fewer of these numbers. Since the actual asymptotic behavior of Carmichael number is still subject to many open questions (e.g. [11]), we believe the asymptotic counts of these numbers would be subject to the same problems. In a follow-up report on tabulating Carmichael numbers to 10^{21}, Richard Pinch provided comparable information to our Tables (see Tables 5-8) in his report[16]. We have provided his table as our Table 9.

Prime pre-product bound	$D\Delta$	CD	Hybrid
$1 \cdot 10^3$	1	.4	1
$2 \cdot 10^3$	3	1	2
$3 \cdot 10^3$	7	3	4
$4 \cdot 10^3$	13	5	7
$5 \cdot 10^3$	20	8	10
$6 \cdot 10^3$	29	12	14
$7 \cdot 10^3$	40	17	19
$8 \cdot 10^3$	52	21	24
$9 \cdot 10^3$	67	27	31
$10 \cdot 10^3$	84	33	38

Table 2: (in seconds)

Table 3: Timing without a Crossover

Bound	$k = 4$	$k = 5$	$k = 6$	$k = 7$
10^{10}	0.2	40.2	0.01	-
10^{11}	1.1	0.8	0.2	0.01
10^{12}	5.4	4.9	1.4	0.2
10^{13}	27.7	30.5	12.3	2.3
10^{14}	140.6	200.2	84.8	20
10^{15}	664.1	1122.1	611.7	185

Table 4: Timing with a cross-over chosen as $X = B^{.35}$

Bound	$k = 4$	$k = 5$	$k = 6$	$k = 7$
10^{10}	0.1	0.1	0.02	-
10^{11}	0.6	0.7	0.2	0.01
10^{12}	3.2	4.7	1.4	0.2
10^{13}	17.2	29.5	11.7	1.9
10^{14}	92.5	173.3	91.6	20
10^{15}	496.7	964.6	681.8	184.6

Table 5: Values of $C_5(B)$ and $C_5(k, B)$

B	$k=2$	3	4	5	6	7	8	9	10	11	12	$C_5(B)$	α
10^3	1	0	0	0	0	0	0	0	0	0	0	1	0
10^4	1	2	0	0	0	0	0	0	0	0	0	3	0.1193
10^5	1	7	0	0	0	0	0	0	0	0	0	8	0.1806
10^6	9	22	3	0	0	0	0	0	0	0	0	34	0.2552
10^7	24	50	24	2	0	0	0	0	0	0	0	100	0.2857
10^8	64	102	89	18	1	0	0	0	0	0	0	274	0.3047
10^9	159	189	249	106	7	0	0	0	0	0	0	710	0.3168
10^{10}	414	356	512	358	71	0	0	0	0	0	0	1711	0.3233
10^{11}	1053	633	1008	1040	316	17	0	0	0	0	0	4067	0.3281
10^{12}	2734	1110	1857	2703	1268	180	3	0	0	0	0	9855	0.3328
10^{13}	7301	2038	3344	6226	4174	966	59	0	0	0	0	24108	0.3371
10^{14}	19674	3737	5649	13287	12078	4288	490	6	0	0	0	59209	0.3409
10^{15}	53561	6754	9462	26821	31472	15721	2844	138	1	0	0	146774	0.3444
10^{16}	146953	12215	15639	51121	76397	50690	13280	1201	22	0	0	367518	0.3478
10^{17}	407779	22004	25186	94748	173721	148482	53529	7338	287	0	0	933074	0.3512
10^{18}	1142128	39974	40155	169243	376784	404815	191645	37528	2501	37	0	2404810	0.3545
10^{19}	3220913	73298	62991	293565	783905	1033279	621182	165609	17013	526	5	6272286	0.3578
2^{64}	4247414	86227	70917	338435	946862	1313728	839626	240258	27437	1004	10	8111918	0.3586

Table 6: Values of $C_{-7}(B)$ and $C_{-7}(k, B)$

B	2	3	4	5	6	7	8	9	10	11	12	$C_{-7}(B)$	α
10^3	0	0	0	0	0	0	0	0	0	0	0	0	0
10^4	1	4	0	0	0	0	0	0	0	0	0	5	0.1747
10^5	1	17	0	0	0	0	0	0	0	0	0	18	0.2511
10^6	4	53	10	0	0	0	0	0	0	0	0	67	0.3043
10^7	15	115	74	8	0	0	0	0	0	0	0	212	0.3323
10^8	37	249	267	61	0	0	0	0	0	0	0	614	0.3485
10^9	94	509	746	316	16	0	0	0	0	0	0	1684	0.3585
10^{10}	239	965	1770	1272	168	0	0	0	0	0	0	4414	0.3645
10^{11}	623	1773	3777	4565	1128	70	0	0	0	0	0	11936	0.3706
10^{12}	1595	3248	7458	14516	5260	602	5	0	0	0	0	32684	0.3762
10^{13}	4320	5863	14052	41215	19405	3696	138	0	0	0	0	88689	0.3806
10^{14}	11756	10490	25389	99562	61541	18690	1568	24	0	0	0	229020	0.3828
10^{15}	32071	19211	44127	207979	175819	79626	11676	392	2	0	0	570903	0.3838
10^{16}	88111	34589	75146	390112	459693	291488	67197	4544	47	0	0	1410927	0.3843
10^{17}	243992	62833	124996	684936	1127659	958164	318930	36532	999	1	0	3559042	0.3854
10^{18}	684583	115274	203560	1154665	2609781	2870274	1304962	227523	12309	113	0	9183044	0.3868
10^{19}	1930996	211336	326436	1902266	5763746	7969591	4752342	1173485	104118	2324	7	24136647	0.3686
2^{64}	2546823	248473	369654	2167587	7063176	10340609	6595966	1770773	175859	4753	16	31283689	0.3890

Table 7: Values of $C_{-11}(B)$ and $C_{-11}(k, B)$

B	2	3	4	5	6	7	8	9	10	11	12	$C_{-11}(B)$	
10^3	1	1	0	0	0	0	0	0	0	0	0	2	0.1903
10^4	3	3	0	0	0	0	0	0	0	0	0	6	0.1945
10^5	6	6	3	0	0	0	0	0	0	0	0	15	0.2352
10^6	8	25	14	1	0	0	0	0	0	0	0	48	0.2802
10^7	15	63	51	7	1	0	0	0	0	0	0	137	0.3052
10^8	41	157	156	27	1	0	0	0	0	0	0	382	0.3228
10^9	108	317	421	155	15	0	0	0	0	0	0	1016	0.3341
10^{10}	276	617	990	693	80	0	0	0	0	0	0	2656	0.3424
10^{11}	694	1215	2157	2452	516	16	0	0	0	0	0	7050	0.3498
10^{12}	1795	2292	4373	7798	2493	230	0	0	0	0	0	18981	0.3565
10^{13}	4899	4171	8535	22623	9547	1575	31	0	0	0	0	51381	0.3624
10^{14}	13183	7514	15701	56048	31758	8307	520	5	0	0	0	133036	0.3660
10^{15}	35654	13667	27741	119135	92145	37187	4299	97	0	0	0	329925	0.3679
10^{16}	97750	24427	47899	226410	247963	143068	27953	1426	5	0	0	816901	0.3695
10^{17}	271562	44398	80166	402574	618647	485980	142421	13079	221	0	0	2059048	0.3714
10^{18}	760653	80786	131666	684709	1456771	1498393	614240	90839	3524	18	0	5321599	0.3737
10^{19}	2147345	149154	212589	1141736	3259866	4257511	2332830	507737	35554	494	0	14044816	0.3762
2^{64}	2831298	175235	241194	1305333	4007294	5554172	3268653	778688	62510	1132	2	18225511	0.3767

Table 8: Values of $C_{13}(B)$ and $C_{13}(k, B)$

B	2	3	4	5	6	7	8	9	10	11	12	$C_{13}(B)$	α
10^3	2	0	0	0	0	0	0	0	0	0	0	2	0.1003
10^4	2	0	0	0	0	0	0	0	0	0	0	2	0.0753
10^5	5	4	1	0	0	0	0	0	0	0	0	10	0.2
10^6	10	16	8	0	0	0	0	0	0	0	0	34	0.2552
10^7	18	39	30	1	0	0	0	0	0	0	0	88	0.2778
10^8	59	87	95	20	0	0	0	0	0	0	0	261	0.3021
10^9	135	182	230	106	8	0	0	0	0	0	0	661	0.3134
10^{10}	335	360	494	359	121	4	0	0	0	0	0	1673	0.3223
10^{11}	861	669	1012	1175	2115	22	0	0	0	0	0	5854	0.3425
10^{12}	2218	1213	1892	3358	12776	133	0	0	0	0	0	21590	0.3612
10^{13}	5972	2190	3349	8860	44394	727	0	0	0	0	0	65492	0.3705
10^{14}	15996	3921	5722	20351	116366	3207	10	0	0	0	0	165573	0.3728
10^{15}	43387	7065	9512	40233	252535	12101	106	34	0	0	0	364973	0.3708
10^{16}	119760	12767	15772	71695	483640	40779	587	469	2	0	0	745471	0.3670
10^{17}	333122	22825	25616	119960	857358	125490	2782	3858	67	0	0	1491078	0.3631
10^{18}	933600	41533	40764	191781	1434794	351699	11463	23179	932	3	0	3029748	0.3601
10^{19}	2634300	76327	63903	300111	2326807	920304	43598	113433	8493	113	0	6487389	0.3585
2^{64}	3473895	89688	71861	337321	2633462	1177125	61566	168929	14437	254	0	8028538	0.3584

Table 9: Values of $C_1(B)$ and $C_1(k, B)$ - Carmichael numbers (Pinch's table)

B	3	4	5	6	7	8	9	10	11	12	Total
10^3	1	0	0	0	0	0	0	0	0	0	1
10^4	7	0	0	0	0	0	0	0	0	0	7
10^5	12	4	0	0	0	0	0	0	0	0	16
10^6	23	19	1	0	0	0	0	0	0	0	43
10^7	47	55	3	0	0	0	0	0	0	0	105
10^8	84	144	27	0	0	0	0	0	0	0	255
10^9	172	314	146	14	0	0	0	0	0	0	646
10^{10}	335	619	492	99	2	0	0	0	0	0	1547
10^{11}	590	1179	1336	459	41	0	0	0	0	0	3605
10^{12}	1000	2102	3156	1714	262	7	0	0	0	0	8241
10^{13}	1858	3639	7082	5270	1340	89	1	0	0	0	19279
10^{14}	3284	6042	14938	14401	5359	655	27	0	0	0	44706
10^{15}	6083	9938	29282	36907	19210	3622	170	0	0	0	105212
10^{16}	10816	16202	55012	86696	60150	16348	1436	23	0	0	246683
10^{17}	19539	25758	100707	194306	172234	63635	8835	340	1	0	585355
10^{18}	35586	40685	178063	414660	460553	223997	44993	3058	49	0	1401644
10^{19}	65309	63343	306310	849564	1159167	720406	196391	20738	576	2	3381806

7.4. Distribution of Jacobi Symbols

After completing the four tabulations, we were curious if the distribution of the possible Jacobi symbols of a particular k value was uniform. Our expectation was the distribution would be approximately uniform. We first looked at the eight cases for $k = 3$ with $d = 5$ and found that the count is not uniformly distributed among the 8 possibilities. In Figure 1, we see the largest count being 32227 which corresponded to $\delta_{p_1} = \delta_{p_2} = \delta_{p_3} = 1$, which are also Carmichael numbers. The smallest count was 1146 which corresponded to $\delta_{p_1} = \delta_{p_2} = -\delta_{p_3} = 1$. We repeated this for all four of our tabulations using $k = 3$ and found that $d = 5$ (Figure 1) and $d = 13$ have extremely different distributions of the 8 possible cases of Jacobi symbols. It should be noted that for $k = 3$ and $d = -7$, the Carmichael numbers represent the smallest count of the eight possible cases (see Figure 2).

Since the product of twin primes plays a special role for absolute Lucas pseudoprimes, we thought that their presence might play a unique role even when $k > 2$. So, we analyzed the counts when we removed numbers that have a product of twin primes dividing them to see if there was more uniformity across cases. When we do this for $d = 5$, we see no significant change in the distribution. However, when we do this for $d = -7$, we can clearly see the distribution becomes more uniform. Compare Figure 1 to Figure 3 and Figure 2 to Figure 4.

We also looked at the Jacobi symbol for n for each discriminant from $k = 3$ to $k = 9$ and put these counts in graphs. For $d = 5$, the count was greatly skewed towards the Jacobi symbol being 1, as seen in Figure 5. Similarly, $d = 13$ was largely skewed toward 1 as seen in Figure 6, but not as dramatically as $d = 5$. Discriminants -7 and -11 were almost even among their symbols of n. The graphs show the percentage of symbol -1 and 1 for each k case of the positive discriminants.

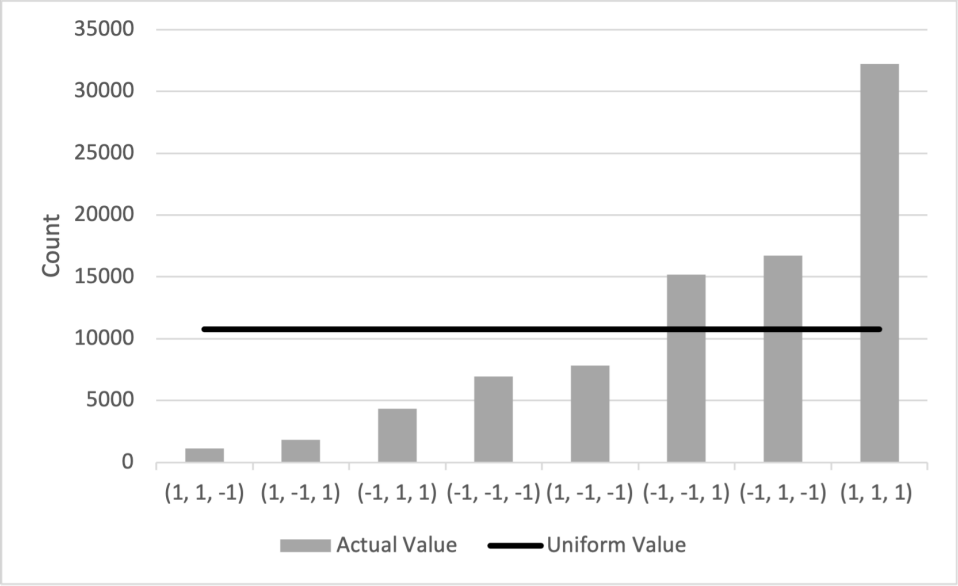

Figure 1: Jacobi Symbol Distribution for $k = 3$ and $d = 5$

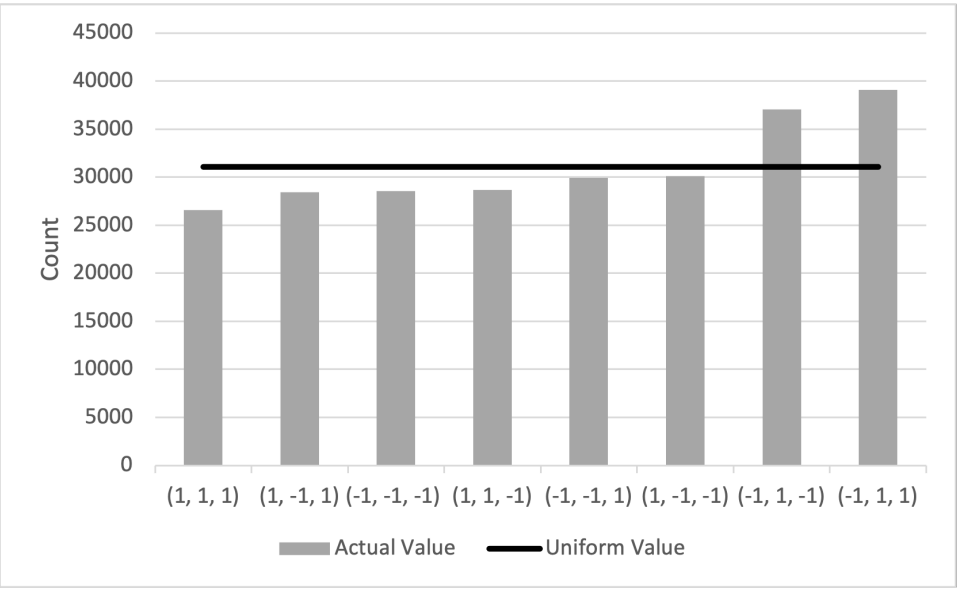

Figure 2: Jacobi Symbol Distribution for $k = 3$ and $d = -7$

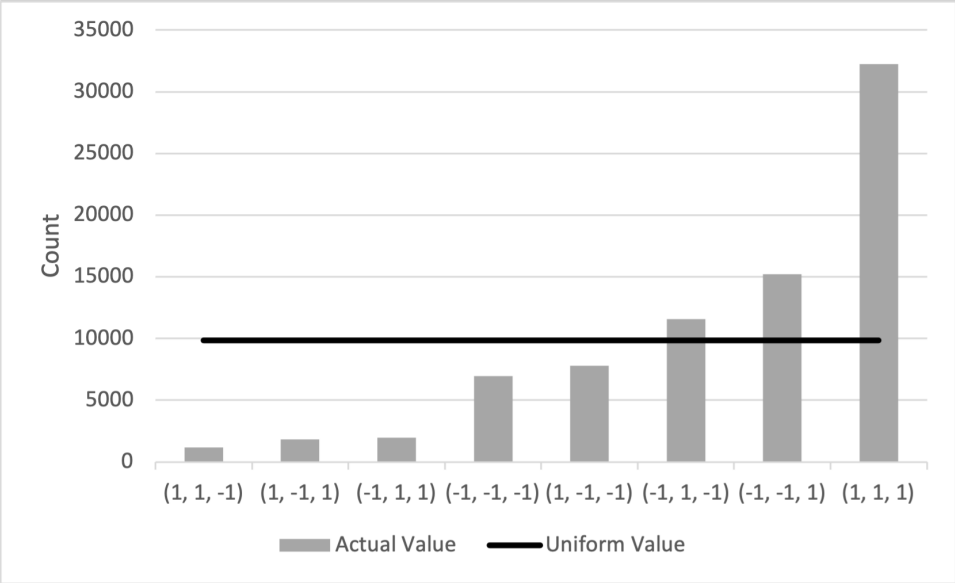

Figure 3: Jacobi Symbol Distribution for $k = 3$ and $d = 5$ with twin primes removed

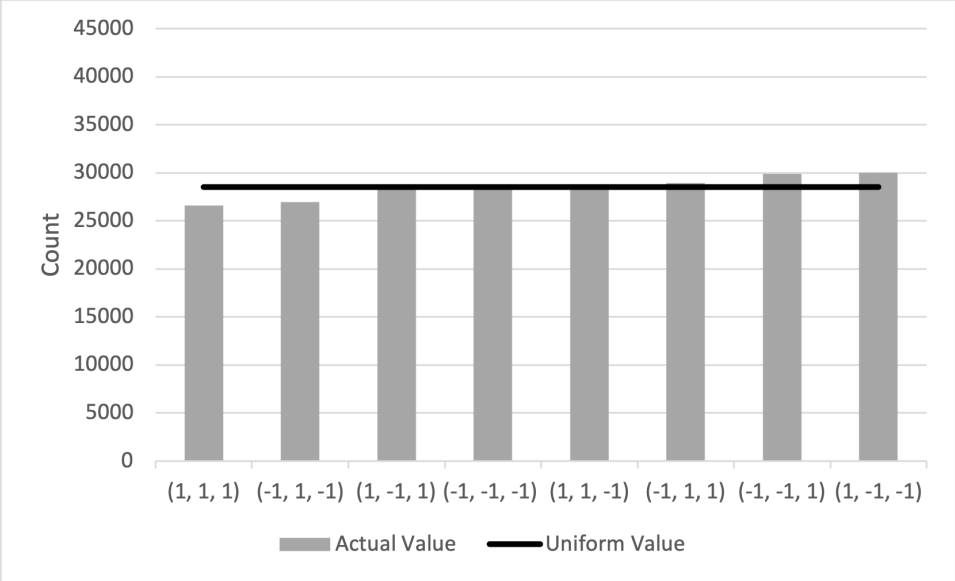

Figure 4: Jacobi Symbol Distribution for $k = 3$ and $d = -7$ with twin primes removed

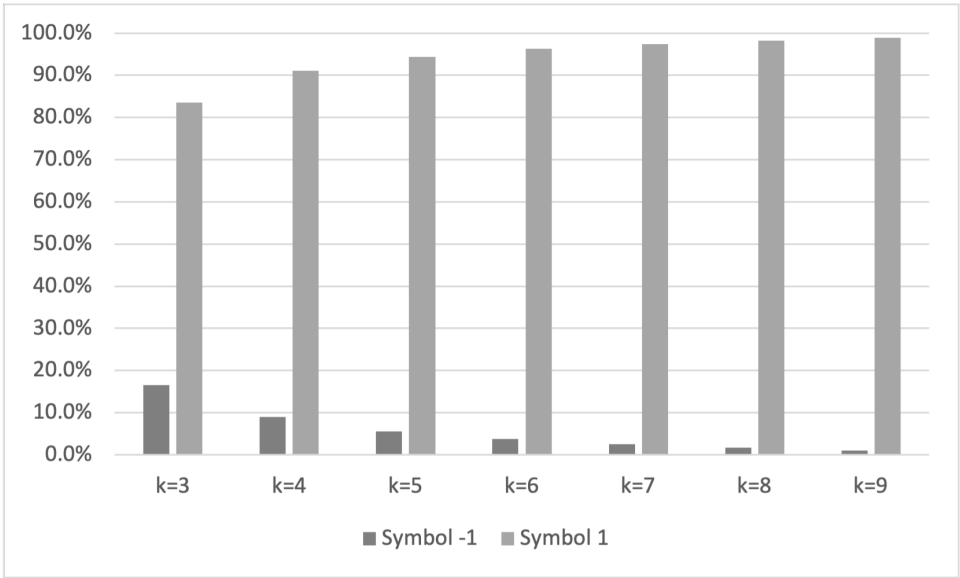

Figure 5: Discriminant 5 Jacobi Symbol of n

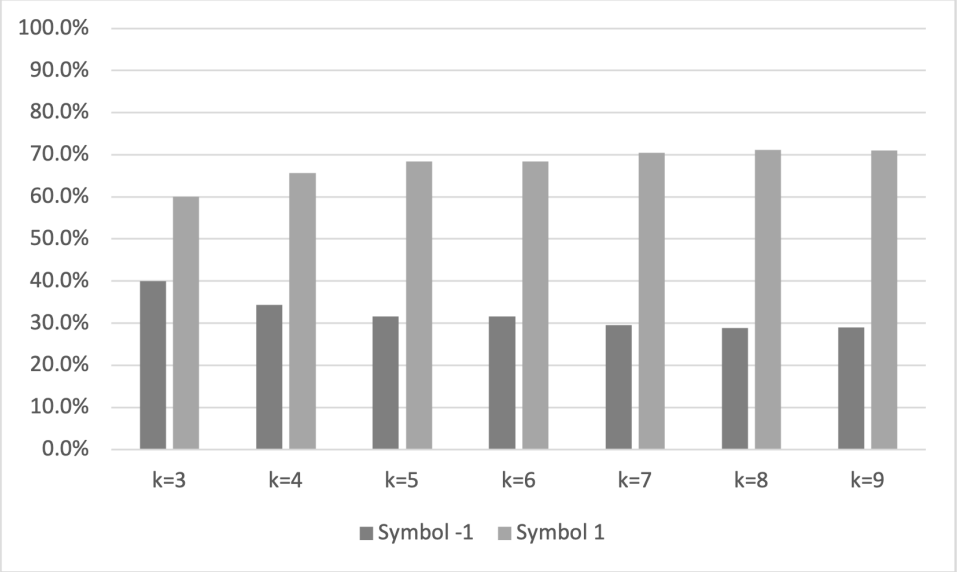

Figure 6: Discriminant 13 Jacobi Symbol of n

Acknowledgements. We both thank Anthony Gurovski for his initial contribu-

tions, which included a tabulation up to 10^{17} for $d = 5$. We are grateful to Hugh Williams' encouragement and his comments on a preliminary draft of this work. We are also thankful to the anonymous referee.

References

[1] R. Baillie, A. Fiori, and S. Wagstaff, Strengthening the Baillie-PSW primality test, *Math. Comp.* **90** (330), 1931-1955, (2021).

[2] R. Baillie, and S. Wagstaff, Lucas Pseudoprimes, *Math. Comp.* **35** (152), 1391-1417, (1980).

[3] R. Crandall and C. Pomerance, *Prime numbers: A computational perspective*, Springer, New York, (2005).

[4] H.G.W.H. Beeger, On composite numbers n for which $a^{n-1} \equiv 1 \pmod{n}$ for every a prime to n. *Scripta Math.* **16**, 133-135, (1950).

[5] H.J.A. Duparc, On Carmichael numbers. *Simon Stevin* **29**, 21-24, (1952).

[6] P. Erdős, Some asymptotic formulas in number theory. *J. Indian Math. Soc.* **12**, 75-78, (1948).

[7] P. Erdős, C. Pomerance, and E. Schmutz, Carmichael's lambda function. *Acta Arithmetica*, **58** no. 4, 365-385, (1991).

[8] J. Friedlander, C. Pomerance, and I. Shparlinski, Period of the power generator and small values of the Carmichael function. *Math. Comp.* **70** (236), 1591–1605, (2001).

[9] T. Granlund and the GMP development team, *GNU MP: The GNU Multiple Precision Arithmetic Library.* `http://gmplib.org/` (2023).

[10] J. Grantham, Frobenius pseudoprimes, *Math. Comp.* **70** , no. 234, 873–891, (2000).

[11] A. Granville and C. Pomerance, Two contradictory conjectures concerning Carmichael numbers, *Math. Comp.* **71** (238), 883-908, (2001).

[12] G. Jaeschke, On strong pseudoprimes to several bases, *Math. Comp.* **61** , no. 204, 915–926, (1993).

[13] M. Joye and J.-J. Quisquater, Efficient computation of full Lucas sequences, *Electron. Lett.* **32**, no. 6, 537-538, (1996).

[14] D.H. Lehmer, An extended theory of Lucas' functions, *Ann. of Math.* (2) **31**, no. 1, 80-85, (1930).

[15] R. G. E. Pinch, The Carmichael numbers up to 10^{15}, *Math. Comp.* **61** (203), 381-391, (1993).

[16] R. G. E. Pinch, The Carmichael numbers up to 10^{21}, `https://tinyurl.com/45w4ec2w`, (2007).

[17] M. Rabin, Probabilistic algorithm for testing primality, *Journal of Number Theory* **12**, 128-138, (1980).

[18] A. Shallue and J. Webster, Tabulating Carmichael numbers $n = Pqr$ with small P, *Res. Number Theory*, **8** (4), Paper No. 84, 11, (2022).

[19] J. Sorenson and J. Webster, Two algorithms to find primes in patterns, *Math. Comp.* **89** (324), 1953-1968, (2020).

[20] H. C. Williams, *Édouard Lucas and primality testing*, Wiley, New York, (1998).

[21] H. C. Williams, On numbers analogous to the Carmichael numbers, *Canad. Math. Bull.* **20** (1), 133-143, (1977).