

COMPUTATION OF JACOBSTHAL'S FUNCTION $h(n)$ FOR
 $n < 50$.

THOMAS R. HAGEDORN

ABSTRACT. Let $j(n)$ denote the smallest positive integer m such that every sequence of m consecutive integers contains an integer prime to n . Let P_n be the product of the first n primes and define $h(n) = j(P_n)$. Presently, $h(n)$ is only known for $n \leq 24$. In this paper, we describe an algorithm that enabled the calculation of $h(n)$ for $n < 50$.

0.1. Introduction. Let n be a positive integer. Every sequence of n consecutive integers contains an a with $(a, n) = 1$. In [7], Jacobsthal raised the question: For a given n , what is the smallest number m with the property that every sequence of m consecutive integers contains an a with $(a, n) = 1$? The Jacobsthal function $j(n)$ is defined to be the smallest m with this property. Equivalently, it is the largest difference between consecutive terms in the sequence of integers relatively prime to n . For example, we have $j(6) = 4$, $j(30) = 6$. Trivially, one has $j(n) \leq n$ and Jacobsthal conjectured

$$j(n) \ll \left(\frac{\log n}{\log_2 n} \right)^2,$$

where $f(x) \ll g(x)$ is understood to mean that there is a constant C such that $|f(x)| \leq Cg(x)$ for all x and $\log_k x$ is the iterated logarithm defined by

$$\log_k x = \begin{cases} \log x, & \text{if } k = 1, \\ \log(\log_{k-1} x), & \text{if } k > 1. \end{cases}$$

The best known upper bound:

$$(0.1) \quad j(n) \ll \log^2 n$$

is due to Iwaniec [6].

If m, n are both divisible by the same primes, then $j(m) = j(n)$. Hence, in studying $j(n)$, we can restrict our attention to n that are the product of distinct primes. In this paper, we consider the particular case when n is the product of the first k primes. Let P_n denote the product of the first n primes and define

$$h(n) = j(P_n).$$

Jacobsthal [7], Kanold [9], and Stevens [15] established upper bounds for $h(n)$; Maier and Pomerance [11] and Pintz [12] have established lower bounds for $h(n)$. Exact values for $h(n)$ have been previously calculated for $n \leq 24$ [8] and are the

Received by the editor April 3, 2008.
2000 *Mathematics Subject Classification.* 11N25, 11Y55.
Key words and phrases. Jacobsthal function, killing sieve.

n	$h(n)$	n	$h(n)$	n	$h(n)$	n	$h(n)$	n	$h(n)$
1	2	11	58	21	190	31	354	41	550
2	4	12	66	22	200	32	378	42	574
3	6	13	74	23	216	33	388	43	600
4	10	14	90	24	234	34	414	44	616
5	14	15	100	25	258	35	432	45	642
6	22	16	106	26	264	36	450	46	660
7	26	17	118	27	282	37	476	47	686
8	34	18	132	28	300	38	492	48	718
9	40	19	152	29	312	39	510	49	742
10	46	20	174	30	330	40	538		

TABLE 1. Values of $h(n)$ for $n \leq 49$

unshaded entries in Table 1. In this paper, we present an algorithm that enabled us to calculate $h(n)$ for $25 \leq k \leq 49$. These values appear as the shaded entries in Table 1. In Figure 1, we graph the exact values for $h(n)$ versus $A(n)$ (see (1.4)), the main term of the best known asymptotic lower bound for $h(n)$. In Figure 2, we graph the ratio $h(n)/A(n)$.

In Section 1, we review the upper and lower bounds that have been established for $h(n)$ and present the connection between $h(n)$ and the problem of determining large gaps between consecutive primes. In Section 2, we introduce killing sieves and relate them to $h(n)$. In Section 3, we describe a bound that reduces the search space for finding a maximal (S_n, k) -killing sieve. In Section 4, we describe the algorithm that permits an efficient calculation of $h(n)$ using killing sieves. Upon first reading this section, one should follow the example in Section 5. In Section 6, we discuss our use of distributed computing and the technical details of our computation. At the end of the paper, we include data tables that determine a sequence of $h(n) - 1$ consecutive integers, each of which is divisible by one of the first n primes.

The author wishes to express his thanks to R. Murty and Q. Zheng for introducing him to the Jacobsthal function, to J. Haugland for explaining his computational work on $h(n)$, to M. Pulimood and her students for their work in grid computing that enabled the calculation of the larger values of $h(n)$, and to M. Kobayashi and the referee for their helpful comments and careful reading of this manuscript. The author also wishes to thank The College of New Jersey for a SOSA award that supported this work.

Notation. Finally, we list the following notations that are used throughout the paper: $[1, z]$ = the set of positive integers $\leq z$.

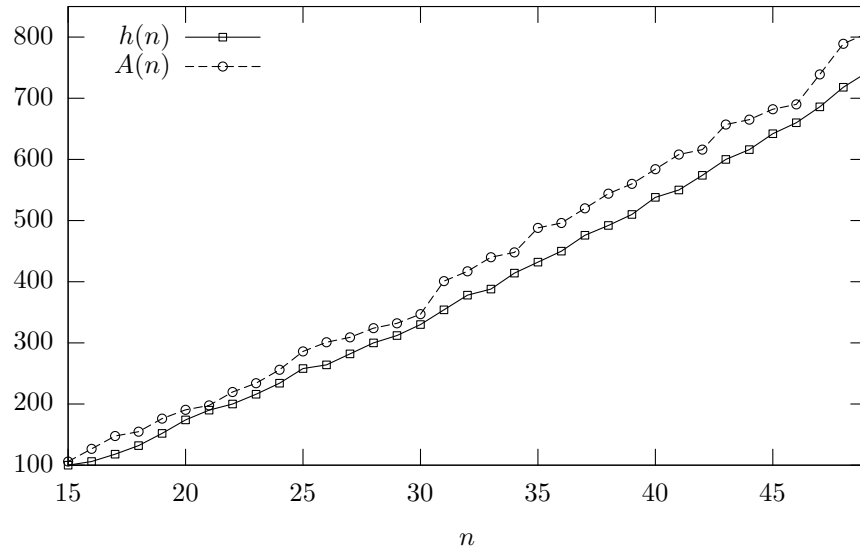
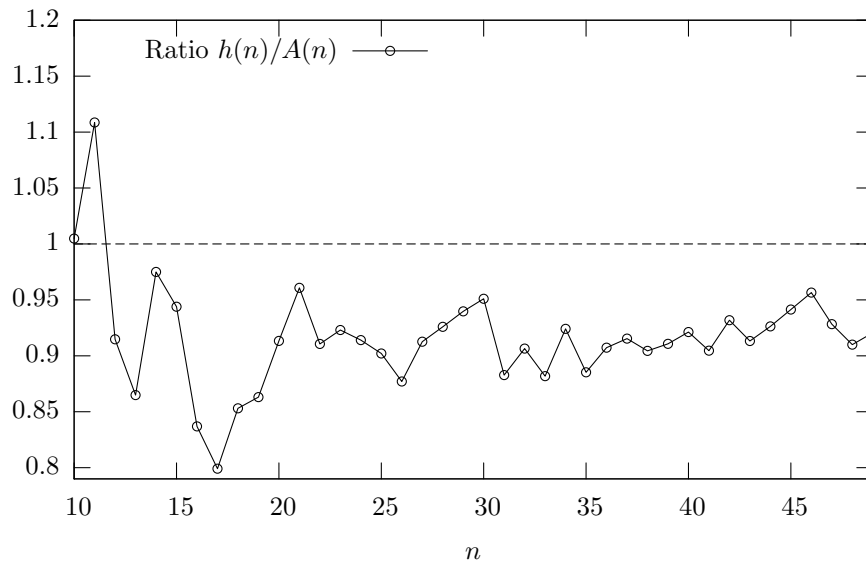
p_i denotes the i th prime.

q_i denotes the i th odd prime.

$S_n = \{q_1, \dots, q_n\}$ is the set of the first n odd primes.

$P(x)$ is the product of the primes $p \leq x$

P_n is the product of the first n primes

FIGURE 1. Comparison of $h(n)$ with the asymptotic lower bound $A(n)$ FIGURE 2. Ratio of $h(n)$ to the asymptotic lower bound $A(n)$

1. BOUNDS ON $h(n)$

Though exact values for $h(n)$ are difficult to compute, there has been extensive work done on establishing upper and lower bounds for $h(n)$. Previous to the

estimate in (0.1), Iwaniec [5] showed

$$(1.1) \quad h(n) \ll n^2 \log^2 n.$$

Iwaniec's bound is proved using sieve theory. Using very elementary arguments, Kanold [9] proved

$$h(n) \leq 2^n$$

for all n and $h(n) \leq 2\sqrt{n}$, if $n \geq e^{50}$. By elementary means, Stevens [15] proved for $n \geq 15$ the stronger (for $n > 4,000,000$) bound

$$(1.2) \quad h(n) \leq 2n^{2+2e \log n}.$$

While considerably weaker asymptotically than (1.1), (1.2) provides an explicit constant.

The best lower bound for $h(n)$ is due to Pintz [12], improving on previous work of Maier and Pomerance [11]. Define $P(x)$ to be the product of the primes less than or equal to x . Pintz proved

$$j(P(x)) \geq (2e^\gamma + o(1)) \frac{x \log x \log_3 x}{\log_2^2 x},$$

where $\gamma \approx .577216$ is Euler's constant. Letting $x = p_n$, the n th prime, we obtain

$$(1.3) \quad h(n) \geq (2e^\gamma + o(1)) \frac{p_n \log p_n \log_3 p_n}{\log_2^2 p_n}.$$

We define

$$(1.4) \quad A(n) = 2e^\gamma \frac{p_n \log p_n \log_3 p_n}{\log_2^2 p_n}.$$

$A(n)$ represents the asymptotic lower bound function for $h(n)$. We compare its values with those of $h(n)$ in Figures 1 and 2.

Let $J(x) = \max_{n \leq x} j(n)$. Combining (1.3) with the approximation $P(\log x) \approx x$, [11, 12] established a similar lower bound for $J(x)$. [12] showed that

$$(1.5) \quad J(x) \geq (2e^\gamma + o(1)) \frac{\log x \log_2 x \log_4 x}{\log_3^2 x}.$$

For completeness, we mention that Maier and Pomerance have conjectured that

$$J(x) = O\left(\log x (\log_2 x)^{2+o(1)}\right).$$

Lastly, we note that estimate (1.5) is then used by [11, 12] to establish the same lower bound as in (1.5) for the function

$$G(x) = \max_{p_n \leq x} (p_{n+1} - p_n),$$

which measures the maximal gap between two consecutive primes with the smaller prime $\leq x$. This connection with the maximal gaps between consecutive primes is a major motivation for the study of lower bounds for the Jacobsthal function.

The lower bounds for $h(n)$ established above are all based upon sieve methods. In contrast, the strongest result proved algebraically without sieve methods is the much weaker result:

Proposition 1.1. *For $n > 1$, $h(n) \geq 2p_{n-1}$.*

Proof. Let $N = p_1 \cdots p_{n-2}$ and $\epsilon = \pm 1$. By the Chinese Remainder Theorem, we can find an integer x such that

$$x \equiv 0 \pmod{N}, \quad x \equiv \epsilon \pmod{p_{n-1}}, \quad \text{and} \quad x \equiv -\epsilon \pmod{p_n}.$$

Then $x - p_{n-1}, x + p_{n-1}$ are consecutive terms in $\mathbb{Z}_{p_1 \cdots p_n}^*$ with a gap of length $2p_{n-1}$. \square

2. KILLING SIEVES

We use the same notations as described at the end of the Introduction. Because P_n , the product of the first n primes, grows exponentially as a function of n , it is impractical to determine $h(n)$ for $n > 20$ by a brute-force search of the gaps between elements of $\mathbb{Z}_{P_n}^*$. To compute $h(n)$ for $n < 50$, we employ a reduction, based upon a generalization of an idea of J. Haugland [4], that uses killing sieves. We note that algorithms similar in spirit were used by Gordon and Rodemich [3] to study admissible sets for the Prime k -tuples Conjecture. In this section, we define killing sieves and relate them to the function $h(n)$.

Definition 2.1. Let $r \geq k \geq 0$ be integers and let $S = \{t_1, \dots, t_r\}$ be a set of primes. A S -sieve with k elements is a set T , where

$$(2.1) \quad T = \{(i_1, c_1), \dots, (i_k, c_k)\}, \text{ with integers } 1 \leq i_1 < i_2 < \dots < i_k \leq r,$$

and $c_j \in \mathbb{Z}_{t_{i_j}}$ is an equivalence class mod t_{i_j} , for $j = 1, \dots, k$.

Definition 2.2. Let $r \geq k \geq 0$ be integers, let $S = \{t_1, \dots, t_r\}$ be a set of primes, and let $z \geq 1$. Let $T = \{(i_j, c_j)\}_{1 \leq j \leq r-k}$ be a S -sieve with $r - k$ elements. T is called a (S, k) -killing sieve of length z if there exists a set $I \subset [1, z]$ of k distinct integers with the property that for all $x \in [1, z] \setminus I$, there exists $j \in [1, r - k]$ such that $x \equiv c_j \pmod{t_{i_j}}$. We say that a (S, k) -killing sieve T has maximal length z if there is no (S, k) -killing sieve with length greater than z .

Remarks 2.3. (i.) If T is a $(S, 0)$ -killing sieve of length z , for simplicity we refer to it as a S -killing sieve of length z .

(ii.) If S is the set of the first n primes, then a S -killing sieve of maximal length has length $h(n) - 1$.

(iii.) If $T' \subset T$, where T is a (S, k) -killing sieve of length z , we say T' can be extended to a (S, k) -killing sieve of length z .

(iv.) By the Chinese Remainder Theorem, we can assume that there is an integer c such that all (or any subset) of the c_j in the definition of T satisfy $c_j \equiv c \pmod{t_{i_j}}$.

Examples 2.4. (i.) Let $S = \{2, 3, 5\} = \{t_1, t_2, t_3\}$. Then $T = \{(1, 1), (2, 2), (3, 4)\}$ is a S -killing sieve of length 5 as $x = 1, 3, 5 \in [1, 5]$ satisfy $x \equiv 1 \pmod{t_1}$, $x = 2$ satisfies $x \equiv 2 \pmod{t_2}$, and $x = 4$ satisfies $x \equiv 4 \pmod{t_3}$. The following table illustrates the smallest prime $t \in S$ used for each $x \in [1, 5]$.

x	1	2	3	4	5
t	2	3	2	5	2

(ii.) Let $S = \{2\}$. Then $T = \{(1, 1)\}$ is a $(S, 2)$ -killing sieve of length 5, as there are only two integers $x \in [1, 5]$ that do not satisfy $x \equiv 1 \pmod{2}$. The corresponding table is:

x	1	2	3	4	5
t	2	*	2	*	2

where the * indicates that the corresponding x is in the set I associated to T .

(iii.) Let $S_8 = \{3, 5, 7, 11, 13, 17, 19, 23\}$. Then

$$T = \{(1, 2), (2, 7), (3, 6), (4, 4), (5, 3), (6, 1)\}$$

defines a $(S_8, 2)$ -killing sieve of length 18. Its associated table is:

x	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
q	17	3	13	11	3	7	5	3	*	*	3	5	7	3	11	13	3	17

(iv.) Let $S_{19} = \{3, 5, \dots, 71\}$, the set of the first 19 odd prime numbers. Then

$$T = \{(1, 2), (2, 4), (3, 1), (4, 7), (5, 3), (6, 10), (7, 6), (8, 14), \\ (9, 12), (10, 21), (11, 30), (12, 31), (13, 33), (14, 28), (15, 13)\}$$

(the second entries come from the column for $n = 19$ in Table 3) is a $(S_{19}, 4)$ -killing sieve of length 86. Except for $x = 45, 46, 48, 58$, all $x \in [1, 86]$ satisfy $x \equiv c_j \pmod{t_{i_j}}$ for some j . Letting

$$T' = T \cup \{(16, 45), (17, 46), (18, 48), (19, 58)\}$$

we obtain a S_{19} -killing sieve of length 86. The additional elements of T' indicate that the primes $t_{16} = 59, t_{17} = 61, t_{18} = 67, t_{19} = 71$ each eliminate exactly one integer from $[1, z]$. These are the integers $\{45, 46, 48, 58\}$ that do not satisfy the congruence criteria of the other primes t_j . T' is not unique as there are $4! = 24$ different S_{19} -killing sieves T' that arise from T .

Proposition 2.5. *Let S be a set of r distinct primes. There is a S -killing sieve of length z if and only if there is a (S, k) -killing sieve of length z for some $k \in [0, r]$.*

Proof. (\Rightarrow) is clear since we can take $k = 0$. (\Leftarrow) Let T be a (S, k) -killing sieve of length z and let $I = \{c_1, \dots, c_k\}$ be the associated set of k distinct integers in $[1, z]$. Let j_1, \dots, j_k be the k integers in $[1, r]$ that do not appear as a first element of the pairs in T (see (2.1)). Then

$$T' = T \cup \{(j_1, c_1), \dots, (j_k, c_k)\}$$

is a $(S, 0)$ -killing sieve of length z . \square

It is useful to reduce the problem of searching for a (S, k) -killing sieve to the problem of searching for a $(S, k+1)$ -killing sieve. The following elementary lemma gives a specific case when we can do this reduction.

Lemma 2.6. *Let $S = \{t_1, \dots, t_n\}$ be a set of n distinct primes. Let T be a $(S, n-r)$ -killing sieve of length z , and let $T = \{(i_j, c_j)\}_{1 \leq j \leq r}$. Suppose that there is $j_0 \in [1, r]$ and $y \in [1, z]$ with the property that $y \equiv c_{j_0} \pmod{t_{i_{j_0}}}$ and $y \not\equiv c_j \pmod{t_{i_j}}$, for $j \neq j_0$. Then $\hat{T} = T \setminus (i_{j_0}, c_{j_0})$ is a $(S, n-r+1)$ -killing sieve of length z with the property that no pair in \hat{T} has i_{j_0} as its first coordinate.*

Proof. If $I \subset [1, z]$ is the set of k elements associated with T , let $\hat{I} = I \cup \{y_0\}$ be the set associated to \hat{T} . The lemma follows immediately. \square

We now define the function $w(n)$ and relate it to the function $h(n)$.

Definition 2.7. For $n \geq 1$, we define $w(n)$ to be the maximal length of a S_n -killing sieve, where S_n is the set of the first n odd primes.

Proposition 2.8. For $n \geq 1$, $h(n+1) = 2w(n) + 2$.

Proof. Let $h = h(n+1)$. We first show that $h \leq 2w(n) + 2$. By definition of h , there is an integer b such that each term in the sequence

$$(2.2) \quad b+1, b+2, \dots, b+h-1$$

is divisible by one of the first $n+1$ primes p_i . If $(b, P_{n+1}) \neq 1$ or $(b+h, P_{n+1}) \neq 1$, the sequence in (2.2) would then be a subsequence of a longer sequence with the same property. As this would imply $h(n+1) > h$, we must have $(b, P_{n+1}) = (b+h, P_{n+1}) = 1$. In particular, b is odd and h must be even. Thus, (2.2) gives an arithmetic sequence of odd integers

$$(2.3) \quad b+2, b+4, \dots, b+h-2,$$

where each term is divisible by one of the odd primes p_2, \dots, p_{n+1} . Let $N = p_2 \cdots p_{n+1}$ and choose $\beta \in \mathbb{Z}$ such that $2\beta \equiv 1 \pmod{N}$. Then the sequence

$$(2.4) \quad \beta(b+2), \beta(b+4), \dots, \beta(b+h-2)$$

derived from (2.3) is a sequence of $w = (h-2)/2$ consecutive terms in \mathbb{Z}_N , each of which is a non-unit. Let $a = \beta(b+2)$. Then rewriting (2.4), each term of the sequence

$$a+1, a+2, \dots, a+w$$

is divisible by one of the odd primes p_2, \dots, p_{n+1} . Equivalently, for every integer $i \in [1, w]$, there exists $j \in \{2, \dots, n+1\}$ such that

$$i \equiv -a \pmod{q_j}.$$

Hence there is a S_n -killing sieve of length w . Since $w \leq w(n)$, we have $h = 2w+2 \leq 2w(n)+2$. Conversely, if there is a S_n -killing sieve of length $w(n)$, these steps can be reversed to show $h(n+1) \geq 2w(n)+2$. The proposition then follows. \square

3. BOUNDING A KILLING SIEVE

In this section, we establish a bound in Proposition 3.10 that gives an efficient means to search through all possible (S_n, k) -killing sieves of maximal length. We use the same notations as described at the end of the Introduction and recall that $S_n = \{q_1, \dots, q_n\}$ is the set of the first n odd primes.

Let $n \geq 1$ and assume $T = \{(i_1, c_1), \dots, (i_r, c_r)\}$ is a S_n -sieve for some $r \leq n$. For a positive integer z , define:

$$I_j = I_j(T, z) = \begin{cases} [1, z] & \text{if } j = 0, \\ \{x \in I_{j-1} \text{ such that } x \not\equiv c_j \pmod{q_{i_j}}\} & \text{if } 1 \leq j \leq r, \\ I_r & \text{if } j > r. \end{cases}$$

and define

$$n_j = \begin{cases} |I_{j-1}| - |I_j|, & \text{if } 1 \leq j \leq r, \\ 0, & \text{otherwise.} \end{cases}$$

The number n_j represents the number of integers in I_{j-1} that are in the congruence class $c_j \pmod{q_{i_j}}$. By definition, $z \geq \sum_{j=1}^r n_j$. We can then use the sum to determine when T is a $(S_n, n-r)$ -sieve.

Lemma 3.1. *Let T , z , and n_j be defined as above. Then T is a $(S_n, n-r)$ -killing sieve of length z if and only if $z \leq (n-r) + \sum_{j=1}^r n_j$.*

Proof. (\Rightarrow) is clear. (\Leftarrow) We have $|I_r| = z - \sum_{j=1}^r n_j \leq n-r$ by hypothesis. Then T and I_r together define a $(S_n, n-r)$ -killing sieve. \square

We now prove a useful upper bound for the n_j . The case $i = 1$ is due to J. Haugland [4].

Definition 3.2. Let $\{m_i\}_{i \geq 0}$ be the sequence of positive integers defined by $m_0 = 1$, $m_1 = 3$, $m_2 = 4$, $m_3 = 6$, $m_4 = 8$, and $m_i = 10$ for $i \geq 5$.

Proposition 3.3. *Assume that T is a (S_n, k) -killing sieve of length z with $i_1 = 1$, $i_2 = 2$ (as defined in (2.1)) and that*

- (i) $i \in \{1, 2, 3\}$ and $j > 1$, or
- (ii) $i \in \{4, 5\}$ and $j > 2$.

If $m_i q_{i_j} > z - 1$, then $n_j \leq i + 1$.

Proof. (i) We first let $i = 1$. Suppose $n_j > 2$ and let $y \in [1, z]$ be the smallest integer in $I_{j-1} - I_j$. Since $j > 1$, $y \in I_1$ and $y \not\equiv c_1 \pmod{3}$. Since $n_j > 2$, there are positive integers $t_2 > t_1$ such that $\{y, y + t_1 q_{i_j}, y + t_2 q_{i_j}\} \subset I_{j-1} \subset I_1$. However, since either $y + q_{i_j}$ or $y + 2q_{i_j}$ is congruent to $c_1 \pmod{3}$, one of these elements is not in I_1 . Hence $t_2 \geq 3$ and

$$3q_{i_j} \leq t_2 q_{i_j} = (y + t_2 q_{i_j}) - y \leq z - 1,$$

which contradicts the hypothesis. The cases when $i = 2, 3$ are proved similarly. We now prove (ii). Let $i = 5$ and $j > 2$. Let y be the smallest element in $I_{j-1} - I_j$. Assume $n_j > 6$. Then there are positive integers $t_6 > t_5 > \dots > t_1$ such that

$$(3.1) \quad S = \{y, y + t_1 q_{i_j}, \dots, y + t_6 q_{i_j}\} \subset I_{j-1} \subset I_2.$$

Either $y + q_{i_j}$ or $y + 2q_{i_j}$ is congruent to $c_1 \pmod{3}$. Suppose $y + 2q_{i_j} \equiv c_1 \pmod{3}$. Then $t_k \not\equiv 2 \pmod{3}$ for each k and we must have $t_6 \geq 9$. If $t_6 = 9$, then $\{t_1, \dots, t_6\} = \{1, 3, 4, 6, 7, 9\}$. However, with this set of t_k , since $q_{i_j} \not\equiv 5 \pmod{5}$, the set S in (3.1) contains an element in each of the congruence classes $\{0, 1, 2, 3, 4\} \pmod{5}$. This results in a contradiction as one of the terms $y + t_k q_{i_j}$ would not be an element of I_2 . Hence $t_6 \geq 10$ and from (3.1), we have

$$10q_{i_j} \leq t_6 q_{i_j} = (y + t_6 q_{i_j}) - y \leq z - 1,$$

which contradicts the hypothesis. An identical argument when $y + q_{i_j} \equiv c_1 \pmod{3}$ also gives a contradiction. Hence, the initial assumption is wrong and $n_j \leq 6$. A similar argument proves (ii) for $i = 4$. \square

Remark 3.4. We note that the lemma can be generalized to $i > 5$, but these cases have not been useful for the calculation of $h(n)$.

Definition 3.5. Let q, z be integers satisfying $(z-1) < 10q$. We define $m(q, z) = 1 + i$, where i is the smallest natural number such that $m_i > (z-1)/q$.

Definition 3.6. Define $S_n(z)$ to be the set of primes $q \in S_n$ with $10q \leq z-1$. Define $r_n(z) = |S_n(z)|$ and $R_n(z) = \prod_{q \in S_n(z)} q$.

Example 3.7. Let $n = 3$, $z = 53$. Then $S_3(53) = \{3, 5\}$. We have $S_3 \setminus S_3(53) = \{7\}$. Then $m(7, 53) = 1 + 4 = 5$ as $m_4 = 8 > (53-1)/7 > m_3 = 6$. We have $r_3(53) = 2$ and $R_3(53) = 15$.

Later, we will need to use the following elementary lemma:

Lemma 3.8. *Let n, z be given. (i) If $n \geq 3$ and $71 \leq z \leq 105$, then $z \leq R_n(z)$. (ii) If $n \geq 4$ and $111 \leq z \leq \prod_{i=1}^n q_i$, then $z \leq R_n(z)$.*

We now establish a fundamental bound that expedites the calculation of $h(n)$. We first make the following definition.

Definition 3.9. Let $n, z \geq 1$. For $k \geq r_n(z)$, define

$$M(n, z, k) = \sum_{i=k+1}^n m(q_i, z).$$

We note that $i \geq k+1 > r_n(z)$ and thus the summand term $m(q_i, z)$ is defined.

Proposition 3.10. *Let $n, z \geq 1$ and assume $k \geq r_n(z)$. Let $T = \{(i_j, c_j)\}_{1 \leq j \leq k}$ be a S_n -sieve with $i_j = j$ for $j = 1, \dots, r_n(z)$. Assume that the elements of T are the first k pairs of a $(S_n, i_k - k)$ -killing sieve of length z . Then*

$$(3.2) \quad |I_k(T)| \leq i_k - k + M(n, z, i_k)$$

Proof. By definition, the $(S_n, i_k - k)$ -killing sieve must consist of pairs (i_j, c_j) for $j = 1, \dots, n + k - i_k$. By Lemma 3.1, we have $z \leq i_k - k + \sum_{j=1}^{n+k-i_k} n_j$. Since $|I_k| = z - \sum_{j=1}^k n_j$ and $n_j \leq m(q_{i_j}, z)$, we have:

$$|I_k| - (i_k - k) \leq \sum_{j=k+1}^{n+k-i_k} n_j \leq \sum_{j=k+1}^{n+k-i_k} m(q_{i_j}, z) \leq \sum_{j=i_k+1}^n m(q_j, z) = M(n, z, i_k).$$

Thus (3.2) is proved. \square

4. THE ALGORITHM

In this section, we describe an efficient algorithm for calculating $w(n)$ by finding a S_n -killing sieve of maximal length. We use the same notations as described at the end of the Introduction. Recall that $S_n = \{q_1, \dots, q_n\}$ is the set of the first n odd primes and that $r_n(z), R_n(z)$ are defined in Definition 3.6.

Assume $n \geq 4$. Suppose that $T = \{(i_1, c_1), \dots, (i_n, c_n)\}$ is a S_n -killing sieve of length z . By Remark 2.3(iv), there is an integer c with the property that the set $T' = \{(1, c \bmod q_1), \dots, (r_n(z), c \bmod q_{r_n(z)})\}$ is a subset of T . We note that $I_{r_n(z)}(T) = I_{r_n(z)}(T')$ and denote it by $I_{r_n(z)}$.

The elements of $I_{r_n(z)}$ defined in (3.2) can then be identified with the units mod $R_n(z)$ in the sequence of integers $1 - c, \dots, z - c$. Additionally, since we are ultimately trying to find a maximal S_n -killing sieve, we can assume that c is also a unit mod $R_n(z)$. Assume $111 \leq z \leq \prod_{i=1}^n q_i$ (in practice, the upper bound is always satisfied). By Lemma 3.8, we can assume $z \leq R_n(z)$ and the terms of the sequence will be distinct mod $R_n(z)$.

In a naive brute-force algorithm to find T , one tries all possible $c \in \mathbb{Z}_{R_n(z)}^*$ (which determines the subset T') and congruence classes $c_j \bmod q_{i_j}$, for $r_n(z) \leq j \leq n$ (which determines $T \setminus T'$). However, this algorithm can be sharpened to permit a more efficient search. First, by Proposition 3.10, $I_{r_n(z)}$ must satisfy

$$(4.1) \quad |I_{r_n(z)}| \leq M(n, z, r_n(z)).$$

Otherwise, T' cannot be extended to a S_n -killing sieve of length z . Hence, one must choose $c \in \mathbb{Z}_{R_n(z)}^*$ so that (4.1) is satisfied. Second, by Lemma 2.6, we can assume

that T is a $(S_n, n - r)$ -killing sieve of length z with $r_n(z) \leq r \leq n$ and $T' \subset T$. Then

$$T \setminus T' = \{(i_j, c_j) \mid \text{where } r_n(z) + 1 \leq j \leq r\},$$

for some integers $i_{r_n(z)+1}, \dots, i_r$ satisfying $r_n(z) < i_{r_n(z)+1} < \dots < i_r \leq n$, and $c_j \bmod q_{i_j}$ for $r_n(z) + 1 \leq j \leq r$. For each $k \in [r_n(z), r]$, we have

$$(4.2) \quad |I_k(T)| \leq (i_k - k) + M(n, z, i_k),$$

by Proposition 3.10. Most choices of c , i_j , and $c_j \bmod q_{i_j}$ do not satisfy Equations 4.1 and 4.2, and can be discarded. Due to the reduced number of possible c , i_j , and congruence classes $c_j \bmod q_{i_j}$ to consider, a modified brute-force search can successfully determine a maximal $(S_n, n - r)$ -killing sieve for $n < 49$, for some r .

We now discuss how r and the i_j for $j > r_n(z)$ are chosen. As there are fewer choices of parameters $c_j \bmod q_{i_j}$ in a $(S_n, h + 1)$ -killing sieve as compared to a (S_n, h) -killing sieve, one would like to make this reduction whenever possible. We repeatedly make the reduction in the following case. Given a (S_n, h) -killing sieve T , and two integers j, k with $0 < k < j \leq n - h$, suppose that no two of the elements of $|I_k(T)|$ lie in the same congruence class $\bmod q_{i_j}$ (with i_j as in (2.1)). Then $(i_j, c) \in T$ for some c . By Lemma 2.6, $\hat{T} = T \setminus (i_j, c)$ is a $(S_n, h + 1)$ -killing sieve in which i_j doesn't appear as the first coordinate of any pair.

Combining these observations, we obtain an algorithm (detailed in Table 4) for determining the maximal length of a S_n -killing sieve. The algorithm begins by searching for a S_n -killing sieve of length z , where z is an initial value. If we assume that $w(n - 1)$, the maximal length of a S_{n-1} -killing sieve, is known, one can begin with $z \geq w(n - 1) + 1$ as $w(n) \geq w(n - 1) + 1$. If the initial choice of z is too high, no S_n -killing sieve of length z will be found. If a S_n -killing sieve of length z is found, then the algorithm proceeds by finding S_n -killing sieves of increasing length until there is a z for which no S_n -killing sieve of length z can be found. Then $w(n) = z - 1$ and $h(n) = 2w(n) + 2$.

The algorithm cycles through all possible $c \in \mathbf{Z}_R^*$, where $R = R_n(z)$ (unless $105 \leq z < 111$). We note that as z increases, there are fewer possible choices of c and c_i satisfying Equations 4.1, 4.2 (see also the conditions in Steps 5 and 6(c)iii). Hence, as long as R remains unchanged, the search runs progressively faster as z increases. If z increases and R changes, then the search slows down as the number of possible c that need to be examined in Step 4 increases.

Finally, we note that when $z > R_n(z)$ (which only occurs when $z < 70$ or $106 \leq z \leq 110$), we can modify the algorithm by using the set $\{3, 5, 7, 11\}$ in place of the set $S_n(z)$ and define $r = 4$, $R = 1155$ in lieu of $r_n(z)$, $R_n(z)$.

5. EXAMPLE: CALCULATION OF $h(20)$

In this section, we work out the details of the algorithm in Table 4 for calculating $h(20)$. Suppose that we are looking for a gap of length $h(20) = 174$, or equivalently, a S_{19} -killing sieve of length $z = 86$. Then Definition 3.6 gives $S = S_{19}(z) = \{3, 5, 7\}$, $R = R_{19}(z) = 105$, and $r = r_{19}(z) = 3$. Then $Z = \mathbf{Z}_{105}^*$. We will need to search over the elements $c \in Z$ and the congruence classes for the primes in $S_{19} - S_{19}(z) = \{11, 13, \dots, 71\}$.

Suppose we have chosen $c = 29 \in Z$ and let $c_i \equiv c \bmod q_i$, for $i = 1, 2, 3$. Then $T_0 = \{(1, 2 \bmod 3), (2, 4 \bmod 5), (3, 1 \bmod 7)\}$ and $I_3 = I_3(T_0, 86)$ is the 37-element

1. Begin with a positive integer $z \geq 71$.
2. If $106 \leq z < 111$, let $r = 4$, $R = 1155$. Otherwise, let $R = R_n(z)$, $r = r_n(z)$ using Definition 3.6.
3. Let $Z = \mathbb{Z}_R^*$.
4. Choose $c \in Z$. If every element of Z has already been chosen, then there is no S_n -killing sieve of length z .
5. Let $I_r = [1, z] \cap (\mathbb{Z}_R^* + c)$, where $W + c$ is the set defined by adding c to each element of a set W . If $|I_r| > M(n, w, r)$, then choose a different c in Step 4. Otherwise, let $i_1 = 1, \dots, i_r = r$, $T_0 = \{(1, c), \dots, (r, c)\}$, $h = 0$, and $k_0 = 0$.
6. If $h < n - r - k_h$, then
 - a. Let j be the smallest integer with $i_{r+h} + 1 \leq j \leq n$ and the property that there exists $x, y \in I_{r+h}(T_h)$ with $x \equiv y \pmod{q_j}$.
 - b. If no such j exists, then
 - i. Let $k_h = n - r - h$. If $|I_{r+h}| \leq k_h$, then continue with Step 7. Otherwise, if $h = 0$, continue with Step 4; if $h > 0$, continue with Step 6(c)i.
 - c. If j exists, let $h = h + 1$, $i_{r+h} = j$ and $k_h = k_{h-1} + j - i_{r+h-1} - 1$. Then:
 - i. Choose $c_{r+h} \pmod{q_{i_{r+h}}}$. (If all possible choices for $c_{r+h} \pmod{q_{i_{r+h}}}$ have already been made (for a fixed T_{h-1}), then if $h \geq 2$, repeat this step with $h = h - 1$. If $h = 1$, let $h = 0$ and continue with Step 4.)
 - ii. Let $T_h = T_{h-1} \cup \{(i_{r+h}, c_{r+h})\}$ and $I_{r+h} = I_{r+h}(T_h, z)$.
 - iii. If $|I_{r+h}| \leq k_h + M(n, z, i_{r+h})$, continue with Step 6. Otherwise, goto Step 6(c)i.
7. T_h determines a (S_n, k_h) -killing sieve of length z with $r + h$ elements. Then:
 - a. Increment z . Let $R_0 = R$ and recalculate r , R as in Step 2.
 - b. If $R = R_0$, then continue with Step 4 and the same c . Subsequently, one need only consider $c \in Z$ not previously considered by the algorithm.
 - c. If $R \neq R_0$, let π be the projection map $\pi : \mathbb{Z}_R \rightarrow \mathbb{Z}_{R_0}$. Let $Z' \subset Z$ be the set consisting of c and elements in Z not previously considered by the algorithm. Then replace Z by $\pi^{-1}(Z')$ and continue with Step 4.

TABLE 2. Algorithm for calculating a maximal S_n -killing sieve for $n \geq 18$. Starting with an initial value of $z \geq 71$, the algorithm finds S_n -killing sieves of increasing length z . $w(n)$ is the final z for which a (S_n, k) -killing sieve of length z can be successfully found.

set

$$I_3 = \{3, 6, 7, 10, 12, 13, 16, 18, 21, 25, 27, 28, 30, 31, 33, 37, 40, 42, 45, \\ 46, 48, 51, 52, 55, 58, 60, 61, 63, 66, 67, 70, 72, 73, 75, 76, 81, 82\}$$

Using the notation of Step 5, we have $i_1 = 1$, $i_2 = 2$, $i_3 = 3$. Now $m(q, 86) = 5$, for $q = 11, 13$; $m(q, 86) = 4$, for $q = 17, 19$; $m(q, 86) = 3$, for $q = 23$; and $m(q, 86) = 2$, for $q = 29, \dots, 71$. Hence, we have $M(19, 86, 3) = 43 \geq 37 = |I_3|$. As the bound given by (3.2) for $k = 3$ is satisfied, it may be possible that T_0 can be extended to a S_{19} -killing sieve of length 86.

We now start with Step 6 in Table 4. We have $h = k = 0$ and $r = 3$. Since the elements $3, 25 \in T_0$ are congruent mod 11, we can take $h = 1$ and $i_4 = 4$. If we choose $c_4 \equiv 7 \pmod{11}$, we have $T_1 = T \cup \{(4, 7 \pmod{11})\}$ and $I_4 = I_4(T_1) =$

$I_3 - \{7, 18, 40, 51, 73\}$. Then the bound given by (3.2) is satisfied for $k = 4$ as $M(19, 86, 4) = 38 \geq 32 = |I_4|$.

By the same logic, we can choose $h = 2$, $i_5 = 5$, and $c_5 \equiv 3 \pmod{13}$. Then $I_5 = I_4 - \{3, 16, 42, 55, 81\}$ and $M(19, 86, 5) = 33 \geq 27 = |I_5|$. Continuing in this manner, we find that for $h = 1, 2, \dots, 12$, there is a choice of $c_{3+h} \pmod{q_{3+h}}$ (given by the entries in the column $n = 19$ in Table 3) such that the inequality $M(19, 86, j) \geq |I_j|$ is satisfied. Then

$$T_{12} = T_0 \cup \left(\bigcup_{h=1}^{12} \{(i, c_i \pmod{q_i})\} \right).$$

Proceeding through the algorithm, in Step 6, when $h = 12$ and $k_{12} = 0$, we find in Step 6(a) that no such j exists. Hence in Step 6(b) we set $k_{12} = 4$. The algorithm then concludes that T_{12} is a $(S_{19}, 4)$ -killing sieve of length 86.

We note that with the sieve T_{12} , there are five primes ($q = 23, 59, 61, 67, 71$), where n_i (with i determined by $q = q_i$) is less than the optimal bound $m(q_i, 86)$. In these cases, we have $n_i = m(q_i, 86) - 1$. One might hope that a different choice of the c_i would permit $n_i = m(q_i, 86)$ and result in a longer S_{19} -killing sieve.

Suppose we try to find a S_{19} -killing sieve of length 87. Using the same data as above, we would again arrive at Step 6b with $h = 12$ and then choose $k_{12} = 4$. But now $|I_{15}| = 5 > 4 = k_{12}$. Hence, there is no S_{19} -killing sieve of length 87 using this congruence data.

Finally, suppose in our original search for a S_{19} -killing sieve with length 86, we had started with $c = 97$. Then $|I_3| = 40$. Picking $i_4 = 4$, $c_4 \equiv 6 \pmod{11}$, and $i_5 = 5$, $c_5 \equiv 4 \pmod{13}$, we have $n_4 = n_5 = 2$ and $|I_5| = 36$. But since $M(19, 86, 5) = 33 < |I_5|$, we know that there is no S_{19} -killing sieve associated with $c = 97$ and $T_2 = \{(1, 97), (2, 97), (3, 97), (4, 6), (5, 4)\}$. Hence, in the algorithm, one must consider other congruence data for the primes q_4, q_5 and other $c \in Z$ to find a S_{19} -killing sieve of length 86.

6. DETAILS OF COMPUTATION

The algorithm was coded in C, and initially run on a Linux 2.6 Ghz server. The program uses minimal memory, and processor speed is the main constraint for the calculation of $h(n)$ for increasing values of n . For $n = 42$, the calculation took approximately two months (we note that once $h = h(n)$ is known, it is much faster to verify that $h(n) = h$ by starting the search with $z = h$). To enable the calculation of $h(n)$ for $n \geq 43$, a distributed computing approach was used [13] to enable a number of computers to simultaneously search different areas of the search space for $a \in Z$ (see Step (3) of the algorithm). With a cluster of thirty computers (GNU/Linux 2.4 Ghz) machines, the calculation of $h(49)$ took approximately two months.

Let w_{n-1} be the value calculated by the computer program as the maximal length of a S_{n-1} -killing sieve. From the data in Tables 3 and 4, it is simple to verify that there is a killing sieve of length w_{n-1} . Hence $w(n-1) \geq w_{n-1}$, and the values in Table 1 provide lower bounds for $h(n)$. Assuming a correct implementation in the computer program of the algorithm in this paper, these lower bounds are the actual values of $w(n-1)$, $h(n)$, respectively. We note that the computer program's calculations agree with previous calculations of $h(n)$, for $n \leq 24$.

EXPLANATION OF TABLES 3, 4: Fix $19 \leq n \leq 48$ and let $S_n = \{q_1, \dots, q_n\}$, where q_i is the i th odd prime. Fix the table column corresponding to n . The shaded entries indicate the primes in $S_n(w(n))$ for that n . Let $R = \{r_1, \dots, r_t\} \subset S_n$ be the set of those primes for which the corresponding entry is an asterisk. For $q \notin R$, let c_q be the corresponding entry. The set $T = \{(i, c_{q_i}) \mid \text{for } i \text{ such that } q_i \notin R\}$ forms a (S_n, t) -killing sieve of length $w(n)$. Let $I = \{y_1, \dots, y_t\} \subset [1, z]$ be the subset of t integers associated to T . Choose $a \in \mathbb{Z}$ such that $a \equiv -c_q \pmod q$, for all primes $q \in S_n \setminus R$ and $a \equiv -y_i \pmod{r_i}$ for $i = 1, \dots, t$. The sequence $a + 1, \dots, a + w(n)$ has length $w(n)$ and every term is divisible by a prime in S_n . Finally, $2a + 1 + \prod_{i=1}^n q_n$ is the first term of a sequence of $h(n + 1) - 1$ integers that are each divisible by one of the first $n + 1$ primes.

n	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33
$h(n + 1)$	174	190	200	216	234	258	264	282	300	312	330	354	378	388	414
$w(n)$	86	94	99	107	116	128	131	140	149	155	164	176	188	193	206
3	2	1	2	1	2	2	2	2	2	2	1	1	2	1	2
5	4	2	4	2	4	2	4	4	3	4	3	3	1	2	3
7	1	2	3	2	3	6	3	3	4	3	2	3	3	4	1
11	7	4	4	4	1	7	4	4	9	4	3	9	4	1	7
13	3	11	7	11	7	10	7	7	1	7	6	6	2	2	4
17	10	3	8	3	6	13	8	8	2	8	7	14	5	16	11
19	6	18	2	3	17	9	2	2	15	2	1	12	6	10	18
23	14	14	13	10	12	1	13	13	7	13	12	12	10	21	21
29	12	10	1	8	2	4	1	1	24	1	2	2	14	9	10
31	21	4	27	6	25	15	27	27	22	28	26	10	7	5	19
37	30	8	16	16	29	31	16	28	32	1	13	21	12	20	17
41	31	33	22	39	21	17	18	16	12	18	17	10	19	26	31
43	33	41	12	35	11	17	20	32	10	16	15	34	32	24	25
47	28	6	28	36	5	16	28	6	6	12	11	15	18	5	8
53	13	*	43	21	42	3	6	43	37	43	5	11	11	15	52
59	*	21	*	45	15	19	43	8	2	8	7	37	9	8	24
61	*	29	6	14	50	39	60	51	51	57	59	13	27	6	9
67	*	*	*	29	*	54	51	63	*	*	7	44	42	16	42
71	*	*	*	*	*	25	55	61	55	61	*	19	26	*	29
73		5	18	*	17	21	57	60	54	60	56	29	26	65	34
79			*	5	26	45	12	12	57	63	*	26	5	35	8
83				18	*	43	*	55	49	55	54	54	55	51	61
89					27	*	*	*	*	*	27	36	85	75	46
97						*	*	*	45	51	62	47	57	59	27
101							22	22	16	22	21	30	34	69	76
103								18	21	27	29	56	30	*	12
107									*	*	*	39	58	66	49
109										*	*	5	78	71	66
113											42	27	40	63	16
127												*	*	14	60
131													13	30	*
137														3	*
139															6

TABLE 3. Congruence data for S_n -killing sieve of maximal length w for $19 \leq n \leq 33$.

n	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48
$h(n+1)$	432	450	476	492	510	538	550	574	600	616	642	660	686	718	742
$w(n)$	215	224	237	245	254	268	274	286	299	307	320	328	342	358	370
3	1	1	2	2	1	1	1	1	1	1	1	1	2	1	1
5	3	1	4	4	3	1	1	1	2	1	2	4	4	1	3
7	5	2	1	6	5	5	3	5	1	3	4	5	5	4	2
11	6	2	6	7	6	10	5	5	6	10	1	7	5	1	7
13	4	8	12	5	4	5	10	5	10	1	8	1	3	2	11
17	9	3	15	3	3	8	1	13	8	16	3	4	6	14	9
19	8	7	1	9	5	14	3	14	13	9	14	6	7	14	14
23	5	4	17	10	9	4	21	3	12	21	11	15	2	5	13
29	3	5	2	17	16	15	20	5	11	12	6	6	20	24	12
31	11	27	11	12	11	12	12	12	3	24	5	11	21	7	4
37	7	32	13	30	14	2	15	8	16	3	9	7	9	34	17
41	21	39	11	32	25	2	2	2	4	11	14	24	31	10	21
43	35	24	16	29	34	20	9	5	41	9	41	40	24	20	10
47	20	6	29	36	43	38	8	14	33	8	18	30	36	10	22
53	34	45	27	16	34	23	30	6	21	30	13	37	5	29	22
59	14	18	38	45	32	48	33	40	9	48	16	23	28	3	15
61	15	52	14	42	57	1	12	1	5	15	49	3	15	30	26
67	59	62	21	*	44	9	63	14	60	39	1	20	1	47	6
71	58	33	10	50	21	24	48	69	56	57	26	45	14	17	10
73	28	14	67	47	35	35	37	51	54	1	15	60	22	37	47
79	7	38	33	21	7	*	65	35	48	42	29	7	70	8	18
83	24	75	82	44	1	17	14	24	44	29	67	2	5	59	42
89	36	48	2	58	13	25	39	17	38	78	12	78	73	79	42
97	2	95	14	60	80	80	55	65	30	13	46	1	30	9	7
101	66	7	7	25	99	69	57	42	26	2	44	71	13	72	88
103	92	12	18	5	41	52	32	50	24	62	50	8	20	35	92
107	102	78	70	61	7	30	40	102	20	18	94	49	106	88	8
109	41	74	48	87	65	53	53	20	22	46	30	28	38	105	20
113	57	42	37	52	16	45	19	29	10	19	63	49	37	*	5
127	29	15	3	81	*	13	50	113	1	35	19	80	63	107	119
131	45	84	*	112	15	3	99	13	28	63	52	102	10	129	80
137	*	15	55	1	27	72	72	87	129	75	114	48	14	27	132
139	71	29	*	93	2	29	29	80	125	119	59	113	44	83	7
149	*	*	46	82	36	78	123	78	135	*	141	132	97	84	22
151		59	45	15	59	104	68	77	143	23	38	146	132	113	4
157			30	78	*	92	47	32	119	20	131	41	18	125	122
163				*	29	77	77	*	95	5	140	50	90	77	1
167					60	*	*	15	111	72	69	36	100	42	57
173						60	42	39	18	60	*	57	160	117	27
179							54	9	*	*	51	*	118	153	126
181								*	*	68	104	56	105	98	56
191									63	69	24	*	112	*	*
193										89	113	17	*	44	137
197											48	108	43	75	39
199												32	66	68	101
211													51	134	110
223														50	134
227															45

TABLE 4. Congruence data for S_n -killing sieve of maximal length w for $34 \leq n \leq 48$.

REFERENCES

- [1] H. Cramér, *On the order of magnitude of the difference between consecutive prime numbers*, Acta. Arith. **2**, 396–403, (1936).
- [2] P. Erdős, *On the integers relatively prime to n and on a number theoretic function considered by Jacobsthal*, Math. Scand., **10**, 163–170, (1962).
- [3] D. Gordon, G. Rodemich, *Dense Admissible Sets*, In: Algorithmic Number Theory, Lecture Notes in Computer Science 1423, Springer-Verlag, Berlin, 1998.
- [4] J. Haugland, private correspondence, July 2005.
- [5] H. Iwaniec, *On the error term in the linear sieve*, Acta. Arith. **19**, 1–30, (1971).
- [6] H. Iwaniec, *On the problem of Jacobsthal*, Demonstratio Math. **11**, 225–231, (1978).
- [7] E. Jacobsthal. *Über Sequenzen ganzer Zahlen, von denen keine zu n teilerfremd ist. I-III.*, Norske Vid. Selsk. Forhdl. **33**, 117–124, 125–131, 132–139, (1960).
- [8] N.J.A. Sloane, (2007), The On-Line Encyclopedia of Integer Sequences, published electronically at <http://www.research.att.com/~njas/sequences/>, Sequence A048670.
- [9] H.J. Kanold, *Über eine zahlentheoretische Funktion von Jacobsthal*, Math. Annalen **170**, 314–326 (1967).
- [10] H.J. Kanold, *Neuere Untersuchungen über die Jacobsthal-Funktion $g(n)$* Monatsh. Math., **84**, 109–124 (1977).
- [11] H. Maier, C. Pomerance, *Unusually Large Gaps Between Consecutive Primes*, Trans. Amer. Math. Soc. **322**(1), 201–237, (1990).
- [12] J. Pintz, *Very large gaps between consecutive primes*, J. Number Theory, **63**(2), 286–301, (1997).
- [13] S.M. Pulimood, and T.R. Hagedorn, *Applying the Grid Computing Paradigm within a Liberal Arts Academic Environment*. In Proceedings of the 2007 International Conference on Grid Computing Applications (GCA 2007) held in conjunction with The 2007 World Congress in Computer Science, Computer Engineering, and Applied Computing, Las Vegas, USA, June 2007.
- [14] R. Rankin, *The difference between consecutive prime numbers. V*, Proc. Edinb. Math. Soc. (2) **13**, 331–332, (1962/63).
- [15] H. Stevens, *On Jacobsthal's $g(n)$ -function*, Math. Annalen, **226**, 95–97, (1977).

DEPARTMENT OF MATHEMATICS AND STATISTICS, THE COLLEGE OF NEW JERSEY, P.O. BOX 7718, EWING, NJ 08628-0718

E-mail address: hagedorn@tcnj.edu