Generation of Pseudoprimes

Danielle Stewart
Swenson College of Science and Engineering
University of Minnesota Duluth
dkbennet@d.umn.edu

1. Introduction

Number theory is a branch of mathematics that looks at the many properties of integers. The properties that are looked at in this paper are specifically related to pseudoprime numbers. Positive integers can be partitioned into three distinct sets: the unity, composites, and primes. It is much easier to prove that an integer is composite compared to proving primality.

Fermat's Little Theorem

If p is prime and a is any integer, then $a^p - a$ is divisible by p.

This theorem is commonly used to determine if an integer is composite. If a number does not pass this test, it is shown that the number must be composite. On the other hand, if a number passes this test, it does not prove this integer is prime (Anderson & Bell, 1997) . An example would be to let $p = 5$ and let $a = 2$. Then $2^5 - 2 = 32 - 2 = 30$ which is divisible by 5. Since $p = 5$ is prime, we can choose any a as a positive integer and $a^5 - a$ is divisible by 5. Now let $p = 4$ and $a = 2$. Then $2^4 - 2 = 14$ which is not divisible by 4. Using this theorem, we can quickly see if a number fails, then it must be composite, but if it does not fail the test we cannot say that it is prime. This is where pseudoprimes come into play. If we know that a number n is composite but n divides $a^n - a$ for some positive integer a, we call n a *pseudoprime*. (Anderson & Bell, 1997).

For example, let $p = 121$ and $a = 3$, then $3^{121} - 3$ is in fact divisible by 121. In this case, 121 is a base-3 pseudoprime. By choosing our base a to be 3, Fermat's test will pass, but with any other base, it will fail. Pseudoprimes are then divided into meaningful partitions. The partition that is considered in this paper is Carmichael pseudoprimes. These are composite numbers that will pass Fermat's Little Theorem for infinitely many bases a. For instance, let $p = 561$, then for any positive integer a, $a^{561} - a$ is divisible by 561. This happens to be the smallest Carmichael number.

In the late 1800's, Alwin Korselt determined to prove that there are no such thing as Carmichael numbers (Brennan, 2012). What he proved in 1899 was this:

Korselt's Criterion

$a^n \equiv a(mod\ n)$ for all a if and only if n is not divisible by any square and $n - 1$ is divisible by $p - 1$ for each prime divisor p of n.

Proof

Assume that we have a positive integer n such that $a^n \equiv a(mod\ n)$. In other words, we have a number n such that n divides $a^n - a$for all integers a. Assume that p is a prime divisor of n. Since n divides $a^n - a$ then p also divides $a^n - a$. Now suppose that n is divisible by a square, then we can find a factor of n in the form b^2. This implies that b^2 divides n and n divides $b^2 - b$ and thus $b2$ divides $b^2 - b$. But this tells us that b^2 divides b which is impossible for integers. Thus n must not be divisible by a square (i.e. n is square free).

Now, let p divide n and suppose we have a generator a of the finite group U(p) with order $p - 1$. If n divides $a^n - a$, then p divides $a^n - a$. This implies that $a^n \equiv a(mod\ n)$. Since p does not divide a, so p divides $a^{n-1} - 1$ and hence $a^n \equiv 1(mod\ p)$. If $a^k \equiv 1(mod\ p)$ then the order of a in U(p) must divide k. So we have that $n - 1$ is divisible by the order of a. In other words, $n - 1$ is divisible by $p - 1$.

Conversely, suppose n is a composite square free integer and $n - 1$ is divisible by $p - 1$ for all p that divides n. If p does not divide n, then $a^{p-1} \equiv 1(mod\ p)$ and since $p - 1$ divides $n - 1$, we have that $a^{n-1} \equiv 1(mod\ p)$. Multiply by a and we get $a^n \equiv a(mod\ p)$. Suppose p divides a, then $a^n \equiv a(mod\ p)$. We see that if p does not divide n or if p does divide n, $a^n \equiv a(mod\ p)$ for each prime divisor p of n. Since n is square free, $a^n \equiv a(mod\ n)$.

The understanding of this theorem will give an insight into why Carmichael numbers can be generated.

In 1956, Paul Erdös devised a simple method for generating Carmichael numbers (Erdös, 1956) We will look at this method in light of Korselt's criterion proven above. A modification of the method is as follows (Brennan, 2012).

Erdös' Method

Let m be a highly composite number. Let P be the set of primes such that $P = \{p \mid p\ does\ not\ divide\ m\ but\ p - 1\ divides\ m\}$. Then if S is any subset of P for which $\Pi_{p \in S}\, p$ has remainder 1 when divided by m and $|S| > 2$, then $\Pi_{p \in S} p$ is a Carmichael number (LeVeque, 1977).

Proof

Let P be the set of primes $P = \{p \mid p\ does\ not\ divide\ m\ but\ p - 1\ divides\ m\}$. Suppose we have some subset S of P with $|S| > 2$ such that $\Pi_{p \in S}\, p = C$ and $C \equiv 1(mod\ m)$. Then C is the product of primes in S and is square free. Since each $p - 1$ divides m and m divides $C - 1$ we can apply Korselt's Criterion. That is, $p - 1$ divides $C - 1$ so C must be a Carmichael number.

As an example, let $m = 36 = 2_2 * 3_2$. To find the set P, we first find all divisors of m:

{1, 2, 3, 4, 6, 9, 12, 18, 36}

and then add one to each of them:

{2, 3, 4, 5, 7, 10, 13, 19, 37}

This takes care of the criteria that divides m. Now we need to remove $p - 1$ nonprimes and any primes that divide m. What is left over is our set P.

$P = \{5, 7, 13, 19, 37\}$

To find the Carmichael numbers from this set we find all subsets that give a remainder of 1 when we divide $\Pi_{p \in S} p$ by 36 = m. Notice that there are no repeated primes in the set P and clearly, $\Pi_{p \in S} p$ is square free.

By finding all subsets of P, we see that there are 4 that will give a remainder of 1:

∅, {37}, {7, 13, 19}, {7, 13, 19, 37}

Only the last two subsets give us Carmichael numbers. These numbers are 7 * 13 * 19 = 1729 and 7 * 13 * 19 * 37 = 63,973. This tells us that for any positive integer a, $a^{1729} - a$ is divisible by 1729 and for any positive integer a, $a^{63,973} - a$ is divisible by 63,973.

Looking back at Korselt's Criterion, for each prime p in S, $p - 1$ divides $C - 1$. For instance, looking at $S_1 = \{7, 13, 19\}$, we see that 6, 12, and 18 are all divisors of 1728.

2. Group and Number Theory

This project requires some fundamental understanding of a few principles of Group Theory and Number Theory.

Greatest Common Divisor (GCD)

The greatest common divisor of two integers m and n is the largest integer d such that both m and n is divisible by d (Gallian, 2012). This is commonly written as gcd(m, n).

An example of this property is as follows: Look at m = 30 and n = 20. The divisors of 30 are {1, 2, 3, 5, 6, 10, 15, 30}. The divisors of 20 are {1, 2, 4, 5, 10, 20}. The largest common divisor is clearly 10. Thus, gcd(30, 20) = 10.

If we have two integers m and n such that gcd(m, n) = 1, we say that m and n are relatively prime (Anderson & Bell, 1997).

An example is taking the integers 8 and 3. There are no common divisors other than 1, so gcd(8, 3) = 1. Hence, 8 and 3 are relatively prime.

Reduced Residue

A reduced residue is a positive integer less than n but relatively prime to n (LeVeque, 1977). In Group Theory, reduced residues are commonly referred to as the *Unit Group under multiplication,* written as U(m) for some positive integer m. This group consists of all integers in the reduced residue class of m (Gallian, 2012).

For instance, let $m = 12$, then the reduced residues are {1, 5, 7, 11}.

For every positive integer m, there is a reduced residue associated with it. The number of reduced residues of an integer m can easily be found using a function called *Euler's Totient Function.*

Euler's Totient Function
$\phi(m)$ is the number of positive integers less than m and relatively prime to m (Gallian, $\varphi(m)$ 2012). In other words, the size of our group U(m), and the size of the reduced residue class of m.

For $m = 1$, we define $\phi(1) = 1$.

$$\text{If } m = p_1^{a_1} * p_2^{a_2} * p_3^{a_3} * ... * p_n^{a_n}, \text{ then } \varphi(m) = m*(1-\tfrac{1}{p_1}) *(1-\tfrac{1}{p_2}) *...*(1-\tfrac{1}{p_n})$$

For example, take $m = 100 = 2^2 * 5^2$. So $p_1 = 2$ $p_2 = 5$.

$\phi(100) = 100 * (1 - 1/2)*(1- 1/5) = 100 * (1/2) * (1/5) = 10$. This is the number of elements in the reduced residue class of 100.

Congruence

The definition of congruence states that a is congruent to b modulo m if a b is divisible by m [9number theory text]. In short, we write $a \equiv b \ (mod\ m)$. If we look at $a = 40$, $b = 0$, and $m = 10$, we have $40 \equiv 0 \pmod{10}$. This also tells us that the remainder of dividing 40 by 10 is zero. The idea of congruence is not to be confused with equality. We will be using this idea in the foundation of this project.

Order Modulo m

The order modulo m of the reduced residue r is the smallest positive integer n such that $r^n \equiv 1(mod\ m)$ LeVeque, 1977). This is often denoted as $|r| = n$. For example, look again at $m = 36$. The reduced residues are {1, 5, 7, 11, 13, 17, 19, 23, 25, 29, 31, 35}. To find the orders, we take elements of the reduced residue and multiply by itself.

Since $1 \equiv 1(mod\ 36)$, the order of 1 is 1. Now look at 5: $5^2 \equiv 25(mod\ 36)$, $5^3 \equiv 17(mod\ m)$, $5^4 \equiv 13(mod\ 36)$, $5^5 \equiv 29(mod\ 36)$, $5^6 \equiv 1(mod\ 36)$. So, the order of 5 modulo 36 is 6.

To help tie this together, we introduce some group theory. A *group* is a nonempty set with an associative operation such that an identity exists, each element has an inverse, and the set is closed under the group operation (Gallian, 2012).

Multiplicative Group of Integers Modulo m U(m)

For n > 1, the multiplicative group of integers modulo m is as follows:
$U(m) = \{k \mid 1 \leq k < m \text{ with } gcd(k, m) = 1\}$.

A cyclic group is a group G with an element a such that $G = \{a^n \mid n \in \mathbb{Z}\}$. In this case, a is called a *generator* of G. That is, each element in G is a multiple of a.

Cover
The set A covers a residue r if $\Pi_{a \in A}\, a \equiv r \pmod m$. We can say that r is covered by A.

Full Cover

We have a *full cover* for our composite integer m if every reduced residue of m is covered by some subset of P.

Again, let's look at $m = 36$. To get a full cover for this m, we must cover $\phi(36) = 12$ values. Our set P produces $2^5 = 32$ subsets, therefore 32 ways to cover. The process of covering these residues is akin to having 12 boxes and 32 balls. It's as if taking the product of each subset and reducing modulo 36 corresponds to randomly selecting a box to put the ball into.

Table 1.1 shows clearly how the residues are covered in the case that $m = 36$ and which subset produced specific covers.

Residues - U(36)	Number of Covers	Subsets Producing Cover
1	4	∅, {37}, {7,13,19}, {7,13,19,37}
5	4	{5},{5,37},{5,7,13,19}, {5,7,13,19,37}
7	2	{7},{7,37}
11	2	{5,13,19},{5,7,19,37}
13	2	{13},{13,37}
17	2	{5,7,19},{5,7,19,37}
19	4	{19},{19,37},{7,13}, {7,13,37}
23	4	{5,19},{5,19,37},{5,7,13}, {5,7,13,37},
25	2	{7,19},{7,19,37}
29	2	{5,13},{5,13,37}
31	2	{13,19},{13,19,37}
35	2	{5,7},{5,7,37}

Table 1.1

From this table, it is clear that residues can have multiple covers and $m = 36$ will produce a full cover. It can also be seen that when a subset covers a specific residue, by adding the element 37 to that subset, it will still reduce to the same residue. The reason for this is that and $37 \equiv 1 \pmod{36}$ due to properties of modulo arithmetic, multiplying by 37 is equivalent to multiplying by 1. Thus, when $m + 1$ is prime, $m + 1$ will be part of our set P. By adding this element to our subsets, it only increases the amount of times something is covered. It will not change our covering or chances of covering the entire group $U(m)$. We will keep this in mind throughout this paper.

3. Balls in Boxes

In Probability Theory, there is a model of normal distribution called *Balls in Boxes* (Chung, 2001).The concept of this method is this: say you have 10 boxes and 12 balls. Randomly distribute the 12 balls into each of the boxes. What is the probability that every box contains a ball? This method was considered due to the similarities between residue classes and their

coverings using Erdös' method to generate Carmichael pseudoprimes. The boxes are associated with the reduced residue elements and the balls are associated with $\Pi_{p\in S}p$.

Balls in Boxes

$$P(x) = \sum_{k=0}^{x-1}\left(\frac{x!}{k!(x-k)!}\right)\left(1-\frac{k}{x}\right)^{p}(-1)^{k}$$

Where p = $2^{|P|}$ = number of balls (subsets of *P*), x = number of boxes, p = number of balls, and P(x) is the probability that every box contains a ball after a random placement of balls into the boxes.

Using our previous example of $m = 36$ in this context, we have $\phi(36) = 12$ boxes. Since our set *P* contains 5 elements, the power set of *P* has the size $2^5 = 32$ which gives us 32 balls. Plugging into the formula, we see the probability of having a ball in every box.

$$P(12) = \sum_{k=0}^{11}\left(\frac{12!}{k!(12-k)!}\right)\left(1-\frac{k}{12}\right)^{32}(-1)^{k} \approx 0.4309$$

Hence, there is about a 41% chance that all boxes will be filled.

Now, from Table 1.1, we know that $m = 36$ gives a full cover. We also know that 37 ($m + 1$) is prime. If we remove the element 37 from our set *P*, this will not change the fact that we have a full cover, but it will change the probability formula.

For example, having removed 37 from our set *P*, we then have $P = \{5, 7, 13, 19\}$ which will give $2^4 = 16$ subsets. This is similar to having 16 balls and 12 boxes. When we recalculate *P*(x),

$$P(12) = \sum_{k=0}^{11}\left(\frac{12!}{k!(12-k)!}\right)\left(1-\frac{k}{12}\right)^{16}(-1)^{k} \approx 0.0071$$

Clearly, from this *m* value we would not expect a full cover due to such a small probability.

Normal Distribution

In probability theory, the *normal distribution* is a continuous probability distribution defined by

$$f(x) = \frac{1}{\sigma\sqrt{2\pi}}e^{-\frac{(x-\mu)^2}{2\sigma^2}}$$

The parameter μ is the mean of the distribution and the parameter σ is the standard deviation. So the variance of this distribution is σ^2.

Standard Normal Distribution

If a normal distribution has $\mu = 0$ and $\sigma = 1$ then we say it is a *standard normal distribution.*

4. Data Analysis and Discussion

In 2012, Trevor Brennan completed a master's project studying the construction of Carmichael numbers for $m < 20{,}000$. We chose to explore a part of the project that he did not cover. First, we

looked at all values of *m* for which there could be a full cover. In other words, when there are enough primes to cover all the residues.

Phi Ratio

There are enough primes to cover the residues if $\frac{2^{|P|}}{\varphi(m)} \geq 1$.

For example, if $m = 20$:
Divisors of 20 = {1, 2, 4, 5, 10, 20}
Add one: {2, 3, 5, 6, 11, 21}
Remove nonprimes and primes that divide 20: $P = \{3, 11\}$

U(20) = {1, 3, 7, 9, 11, 13, 17, 19}
Clearly, there is no way to take $2^2 = 4$ balls and fill 7 boxes. If we look at the ratio, we have $\frac{4}{7} < 1$. There can be no full cover in this case.

Using Mathematica, we collected the values of *m* for which there is a full cover. There are 506 values of $2 < m < 20,000$ for which there could be a full cover (Table 1). Of these values, 154 provide a full cover which verifies Brennan's work (Brennan, 2012).

Do the coverings act randomly? Are the coverings independent of the *m* chosen, and can we describe these coverings using the probability model Balls in Boxes?

To answer these questions, we ran the 506 values of *m* that give us a chance of having a full cover through the formula *P*(x). If the covering follows the normal distribution of the Balls in Boxes model the sum of all probabilities should be very close to the actual number of full covers.

Each value for which *m* is sufficient for a full cover $\left(\text{i.e. } \frac{2^{|P|}}{\varphi(m)} \geq 1\right)$ was run through the Balls in Boxes formula and the probability P(x) found. After each probability was collected (506 values), the summation of these probabilities was calculated.

Recall that the total number of *m* values which produce a full cover is 156. What we found was that $\Sigma P(x) \approx 141.8$, which is very close to the actual number of full covers.

Taking the set of all probabilities, the standard deviation and variance was calculated. We expected the variance to be close to 1. This is what the distribution model, Balls in Boxes, should give if the set is actually normally distributed. What we found was that the variance for this set of probabilities was approximately 0.231848 and the standard deviation was approximately 0.4815061.

Upon these findings, we focused on what could be causing the extreme variance within this set of probabilities. As explained previously, when $m + 1$ is prime, the effect had on the coverings is that the same residues are covered more often.

For any multiplicative group U(*m*), . So when we multiply $m + 1 \equiv 1 (mod\ m)$ any value by $m + 1$ modulo *m*, we will get that same value back. In essence, it is like multiplying by 1.

So for our purposes, we chose to separate out the values of m where $m + 1$is prime and then recalculate the probability summation and see if this is the complicating factor in our strange variance.

Testing began on all 506 values of m and for any m where $m + 1$ is prime, the set P (primes generated using Erdös method) was modified in that the prime $m + 1$was removed from the set. This decreased the set size, |P|, by 1 and decreased the power set size, $2^{|P|}$ by a magnitude of 2. This would hopefully eliminate the confounding factors in finding the appropriate variance, if in fact this set of m is normally distributed and can be modeled by Balls in Boxes.

The total number of m values where $m + 1$ is prime is 214 out of the original 506 values. After removing $m + 1$ from the set of primes, P, the probabilities were again calculated. Upon taking the summation of this modified set of probabilities, it was found that the sum was approximately 105.16 (recall that the number of m's that provide a full cover is 156). The variance was about 0.2256 and the standard deviation was approximately 0.475. Clearly, this was not the reason for the unexpected variance.

Upon these findings, the set of probabilities were more closely scrutinized. A possible reason why the variance was so far off the expected variance is that there are two distinct peaks. If many probabilities are close to one and many are close to zero with only a few in between, we would not expect a normal distribution. A normal distribution has only one peak (see Figure 2).

Using *Mathematica*, the probabilities were graphed in a histogram plot in order to clearly see the behavior of these probabilities.

The data set was split into three categories:

- $0 < P(x) < 0.01$
- $0.01 \leq P(x) \leq 0.99$
- $0.99 < P(x) < 1$

The findings indicated the following:

- 324 values fell into the first range ($P(x) < 0.01$)
- 151 values fell into the third range ($P(x) > 0.99$)
- 31 values fell into the midrange
  ($0.01 \leq P(x) \leq 0.99$)

These values were then plotted in a histogram form to clearly see the behavior of this data set.

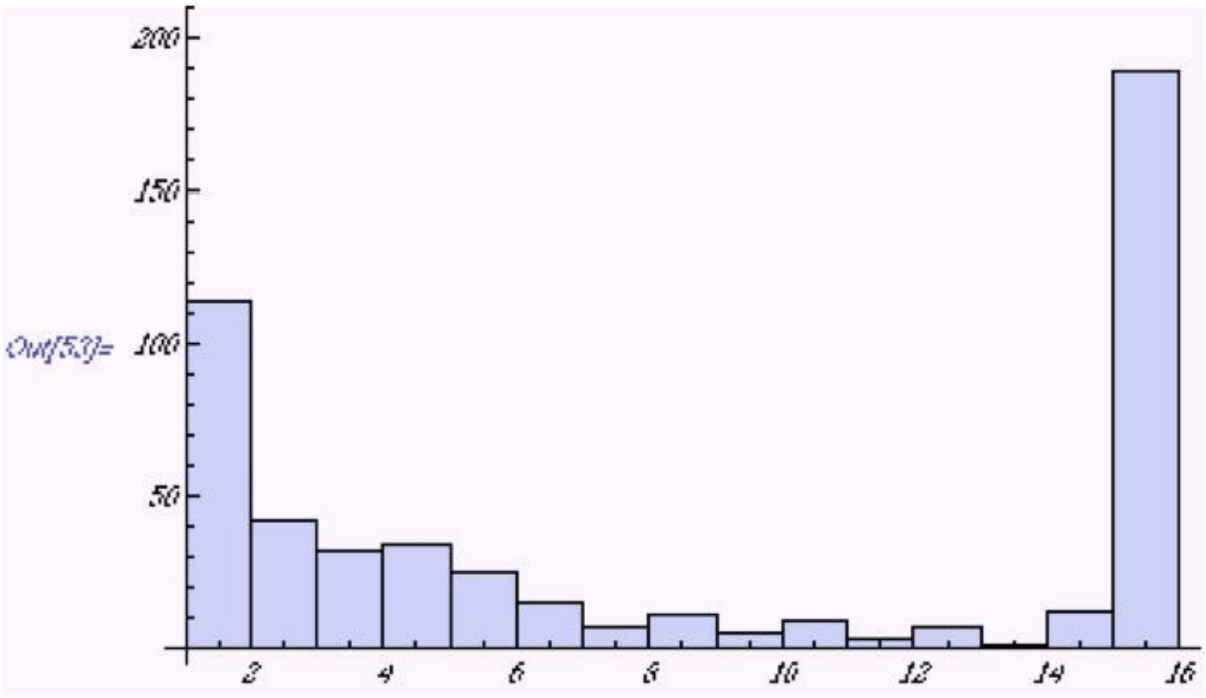

Figure 1

It is clear to see from Figure 1 these probabilities do not follow the normal distribution behavior. For comparison, a normal distribution would look like Figure 2.

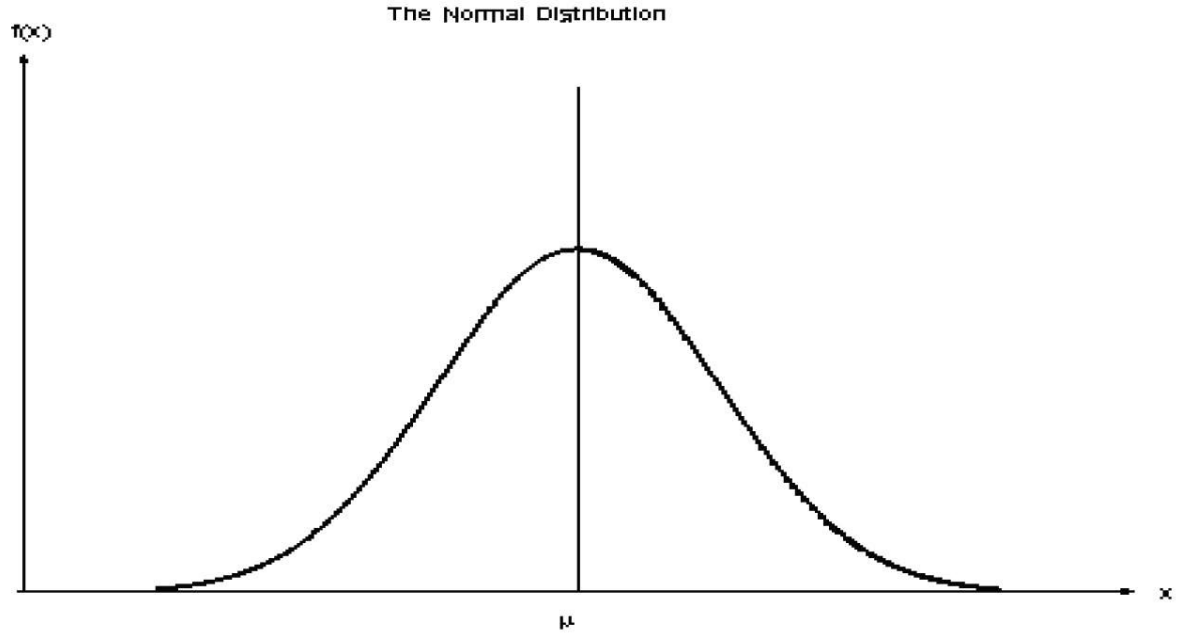

Figure 2

The data indicates that the distribution does not follow the proposed model, Balls in Boxes. Using this procedure to determine the behavior of the residue coverings is not helpful and is incorrect. Thus, the conclusion to this project is that the coverings cannot be assumed to occur randomly for each value m.

5. Conclusion

In order to clearly see the behavior of the residue coverings, a closer look at each m value is necessary. For some m, the set P contains up to 27 primes and varies in size. A consideration $\phi(m)$ must be made for the size of the ratio $2^{|P|}/\phi(m)$, the specific m value, and the distribution of that particular residue class covering.

In this research, the focus was on the residue coverings for all values of m for which there can be a full cover. This research has shown that the behavior of the coverings cannot be predicted when looking at all values of m together. Each value must be scrutinized in and of itself.

References

Anderson, James A.; & Bell, James M. (1997). *Number theory with applications*. Upper Saddle River, NJ: Prentice Hall.

Brennan, T. (2011). An investigation of Erdos method: A scheme for generating Carmichael numbers. *University of Minnesota Duluth, Computational and Applied Mathematics Project.* URL: http://www.d.umn.edu/math/Technical%20Reports/Technical%20Reports%202007-/TR%202011/TR_2011_9.pdf

Chung, Kai L. (2011). *A course in probability theory*. San Diego: Academic Press.

Gallian, Joseph A. (2013). *Contemporary abstract algebra*. Brooks: Cengage Learning.

Erdos, P. (1956). *On pseudoprimes and Carmichael numbers*. URL: http://ftp.math-inst.hu/~p_erdos/1956-10.pdf

LeVeque, William J. (1977). *Fundamentals of number theory*. Reading, Mass: Addison-Wesley.

Appendix

Annotated Code

In bold lettering is annotation. This code was written in Mathematica 7.

Part I: Collect values of m (with thanks to Trevor Brennan for his assistance in this part of the code).

```
listGrid = {}; P = {}; residue = {};
```
Initialization of sets holding set of primes P and the set of residue values.
```
For[m = 2, m <= 20000, m += 1, t = 0;
```
This for loop will increment through all integer values for 2 <=m<=20,000
```
i = 1;

While[i <= m,
If[CoprimeQ[i, m]
```
This while loop finds the values of U(m), the multiplicative group modulo m and places these
values in the set called 'residue.'
```
AppendTo[residue, i]]; i += 2];

divisor = Divisors[m];
```
Find all divisors of m and put in set called 'divisor.'

```
PQ = PrimeQ[divisor + 1];
```
Defines function called 'PQ' that will determine primality of divisor of m plus 1.

```
For[i = 1, i <= Length[divisor], i++,

If[PQ[[i]],
```
Using PQ function to determine primality of (div+1),
if it's prime, put it in a list, P = {p∈P|p divides m but (p1)
does not divide m}

```
AppendTo[P, divisor[[i]] + 1], null]];

intersect = Intersection[P, divisor];
```
Find intersection of P and the set 'divisor.' Save in set called 'intersect.'

```
For[i = 1, i <= Length[intersect], i++, P = DeleteCases[P, intersect[[i]]]];
```
Makes sure no element in P is divisor of m; P is subset of U(m)

```
For[i = 1, i <= Length[intersect], i++, P = DeleteCases[P, intersect[[i]]]];
```
Makes sure no element in P is divisor of m; P is subset of U(m)

```
p = Length[P];
orders = {};
```
List of the orders of all the elements in P ⊂ U(m)

```
Q = {};
```
Initialization of set 'Q' which will hold elements of order 2 or 1 from the group U(m).

```
For[i = 1, i <= p, i++, AppendTo[orders, MultiplicativeOrder[P[[i]], m]];
If[MultiplicativeOrder[P[[i]], m] == 2 ||
MultiplicativeOrder[P[[i]], m] == 1,
AppendTo[Q, P[[i]]]]];

phi = Length[residue];
```
Euler's Totient function 'Phi.'
```
t = 2^p/phi;
```
Define t to be the ratio of the size of the power set of P and the length of the residues.
```
H = Subsets[P];
prdctH = {};
```
The product of all elements in the power set of P (now held in set 'H.'
```
product = 1;

For[n = 1, n <= Length[H], n++, AppendTo[prdctH, Apply[Times, H[[n]]]]]

prdctModM = Mod[prdctH, m];
```
Modulo m each product of the subsets of P.
```
Clear[i];

remainderList = {};
```
Holds all remainders after modulo m on each product of the subsets of P.

```
For[i = 1, i <= Length[prdctModM], i++,
If[TrueQ[prdctModM[[i]] == 1], AppendTo[remainderList, prdctH[[i]]]]]
```

The following code was written by Trevor Brennan to collect the number of residues each remainder covers.
```
binTotal =
BinCounts[{1}, {Union[residue, {m}]}];

f[x_] := Mod[residue*P[[x]], m];

resideMod = residue;
j = 1;

While[j <= p, residueMod = f[j];
sortResidue =
Drop[Flatten[Sort[Partition[Riffle[residueMod, binTotal], 2]]], {1, 1,
```

```
2}]; binTotal += sortResidue; j++];

cov = Partition[Riffle[residue, binTotal], 2];

COV = Tally[Sort[binTotal]];

covering = DeleteDuplicates[prdctModM];
If[Length[covering] == Length[residue], isFull = true, isFull = false];
```
This loop tests to see if we have a full cover.

```
If[Length[covering] == Length[residue], x = 1, x = 0];
```
If the cover is not full, print values of m, |P|, and 2^(|P|)/Phi
```
If[(t >= 1) && (x == 1), Print[{m, p, 2^p, t}]]]
```

Part III: Probability collections

This loop calculates the probability using the Balls in Boxes formula (Uses the approximation formula when the number of primes is greater than 13 due to memory constraints.) Note that the set 'totalNoFull' contains all values where there is not a full cover.

```
For[j = 1, j <= Length[totalNoFull], j += 2,

tmp = totalNoFull[[j]];
p = totalNoFull[[j + 1]];
n1 = 2^p;
x = EulerPhi[tmp];
If[(n1/x) > 1,
If[p > 13, AppendTo[totalNoFullProb, N[((1 E^(
n1/
x))^x)]],
AppendTo[totalNoFullProb,
N[Sum[Binomial[x, k]*((1 k/
x)^n1)*((1)^
k), {k, 0, x 1}]]]]]
]
```

This next loop will count how many values are close to 0 and close to 1, then print out the standard deviation and variance.

```
m := 0;
k := 0;
n := 0;
```
Initialized counter variables
```
For[i = 1, i <= Length[prob2], i++,
n = prob2[[i]] + n;
If[prob2[[i]] < 0.01, m += 1,
```

```
If[prob2[[i]] > 0.99, k += 1]]]
Print["Zero = ", m, " One = ", k]
Print["Std Dev = ", StandardDeviation[prob2], " Variance = ", Variance[prob2]]
```

Table 1

m	p	2^p	(2^p)/phi	Full Cover
2	1	2	2.0	Yes
4	2	4	2.0	Yes
8	2	4	1.0	Yes
12	3	8	2.0	Yes
24	3	8	1.0	Yes
36	5	32	2.66667	Yes
60	5	32	2.0	No
72	6	64	2.66667	Yes
108	6	64	1.77778	No
120	6	64	2.0	No
144	7	128	2.66667	Yes
180	8	256	5.33333	Yes
216	7	128	1.77778	Yes
240	8	256	4.0	No
252	7	128	1.77778	No
288	8	256	2.66667	No
300	7	128	1.6	No
324	7	128	1.18519	No
336	7	128	1.33333	No
360	10	1 024	10.6667	Yes
396	9	512	4.26667	No
420	9	512	5.33333	Yes
432	9	512	3.55556	No

480	9	512	4.0	Yes
504	8	256	1.77778	No
540	11	2 048	14.2222	Yes
560	8	256	1.33333	No
576	10	1 024	5.33333	No
600	9	512	3.2	No
612	8	256	1.333333	No
630	8	256	1.77778	No
648	8	256	1.18519	No
660	8	256	1.6	No
672	9	512	2.66667	No
720	12	4 096	21.3333	Yes
756	10	1 024	4.74074	No
780	8	256	1.33333	No
792	11	2 048	8.53333	Yes
828	9	512	1.93939	No
840	11	2 048	10.6667	Yes
864	10	1 024	3.55556	No
900	10	1 024	4.26667	Yes
936	10	1 024	3.55556	No
960	10	1 024	4.0	Yes
990	8	256	1.06667	No
1008	12	4 096	17.0667	Yes
1056	9	512	1.6	No
1080	13	8 192	28.4444	Yes
1152	11	2 048	5.33333	No

1188	10	1 024	2.84444	No
1200	13	8 192	25.6	Yes
1224	11	2 048	5.33333	Yes
1248	9	512	1.33333	No
1260	14	16 384	56.8889	Yes
1296	11	2 048	4.74074	No
1320	11	2 048	6.4	Yes
1344	11	2 048	5.33333	Yes
1380	11	2 048	5.18182	No
1440	13	8 192	21.3333	Yes
1500	9	512	1.28	No
1512	11	2 048	18.9630	Yes
1560	11	2 048	21.3333	Yes
1584	12	4 096	8.53333	Yes
1620	14	16 384	37.9259	Yes
1656	11	2 048	3.87878	No
1680	15	32 768	85.3333	Yes
1728	12	4 096	7.11111	Yes
1764	9	512	1.01587	No
1800	14	16 384	34.1333	Yes
1836	10	1 024	1.77778	No
1848	9	512	1.06667	No
1872	12	4 096	7.11111	Yes
1890	10	1 024	2.37037	No
1920	11	2 048	4.0	Yes
1980	14	16 384	34.1333	Yes

2016	15	32 768	56.8889	Yes
2040	10	1 024	2.0	No
2088	11	2 048	3.04762	No
2100	13	8 192	17.0667	Yes
2112	11	2 048	3.2	No
2160	17	131 072	227.556	Yes
2268	12	4 096	6.32099	No
2280	12	4 096	7.11111	Yes
2304	13	8 192	10.6667	Yes
2310	9	512	1.06667	No
2340	13	8 192	14.2222	Yes
2376	13	8 192	11.3778	Yes
2400	14	16 384	25.6	Yes
2448	11	2 048	2.66667	No
2484	10	1 024	1.29293	No
2496	10	1 024	1.33333	No
2520	18	262 144	455.111	Yes
2592	13	8 192	9.48148	No
2640	14	16 384	25.6	Yes
2688	12	4 096	5.33333	No
2700	13	8 192	11.3778	Yes
2730	10	1 024	1.77778	No
2760	12	4 096	5.81818	Yes
2772	12	4 096	5.68889	Yes
2800	12	4 096	4.26667	No
2808	11	2 048	2.37037	No

2856	11	2 048	2.66667	No
2880	15	32 768	42.6667	Yes
2916	10	1 024	1.05350	No
2940	12	4 096	6.09524	Yes
2970	10	1 024	1.42222	No
3000	12	4 096	5.12	No
3024	16	65 536	75.8519	Yes
3060	14	16 384	21.3333	Yes
3120	14	16 384	21.3333	Yes
3132	10	1 024	1.01587	No
3150	10	1 024	1.42222	No
3168	15	32 768	34.1333	Yes
3240	16	65 536	75.8519	Yes
3300	11	2 048	2.56	No
3312	13	8 192	7.75758	No
3360	18	262 144	341.333	Yes
3420	10	1 024	1.18519	No
3432	11	2 048	2.03175	No
3456	14	16 384	14.2222	Yes
3480	10	1 024	1.14286	No
3528	11	2 048	2.03175	No
3564	12	4 096	3.79259	No
3600	18	262 144	273.067	Yes
3672	14	16 384	14.2222	Yes
3696	13	8 192	8.53333	Yes
3744	14	16 384	14.2222	Yes

3780	19	524 288	606.815	Yes
3840	13	8 192	8.0	Yes
3888	13	8 192	6.32099	No
3900	12	4 096	4.26667	No
3960	18	262 144	273.067	Yes
4032	18	262 144	227.556	Yes
4080	12	4 096	4.0	No
4140	15	32 768	31.0303	Yes
4176	13	8 192	6.09524	Yes
4200	17	131 072	136.533	Yes
4224	12	4 096	3.2	No
4284	13	8 192	7.11111	Yes
4320	18	262 144	227.556	Yes
4356	13	8 192	6.20606	No
4368	12	4 096	3.55556	No
4410	11	2 048	2.03175	No
4440	11	2 048	1.77778	No
4480	11	2 048	1.33333	No
4500	13	8 192	6.82667	Yes
4536	13	8 192	6.32099	Yes
4560	15	32 768	28.4444	Yes
4608	13	8 192	5.33333	Yes
4620	15	32 768	34.1333	Yes
4680	18	262 144	227.556	Yes
4752	15	32 768	22.7556	Yes
4800	17	131 072	102.4	Yes

4860	16	65 536	50.5679	Yes
4896	12	4 096	2.66667	No
4968	13	8 192	5.17172	No
4992	11	2 048	1.33333	No
5040	23	8 388 608	7 281.78	Yes
5100	11	2 048	1.6	No
5112	11	2 048	1.21905	No
5148	12	4 096	2.84444	No
5160	11	2 048	1.52381	No
5184	15	32 768	18.96296	Yes
5220	12	4 096	3.04762	No
5280	17	131 072	102.4	Yes
5292	13	8 192	5.41799	No
5304	11	2 048	1.33333	No
5376	14	16 384	10.6667	Yes
5400	17	131 072	91.0222	Yes
5460	16	65 536	56.8889	Yes
5508	11	2 048	1.18519	No
5520	15	32 768	23.2727	Yes
5544	15	32 768	22.7556	Yes
5568	11	2 048	1.14286	No
5580	13	8 192	5.68889	No
5600	12	4 096	2.13333	No
5616	14	16 384	9.48148	Yes
5670	12	4 096	3.16049	No
5700	13	8 192	5.68889	No

5712	13	8 192	5.33333	No
5760	17	131 072	85.3333	Yes
5796	13	8 192	5.17172	Yes
5832	11	2 048	1.05350	No
5880	15	32 768	24.3810	Yes
5940	18	262 144	182.044	Yes
6000	16	65 536	40.96	Yes
6048	19	524 288	303.407	Yes
6072	11	2 048	1.16364	No
6120	19	524 288	341.333	Yes
6160	11	2 048	1.06667	No
6240	17	131 072	85.3333	Yes
6264	13	8 192	4.06349	No
6300	19	524 288	364.089	Yes
6336	19	525 288	273.067	Yes
6384	11	2 048	1.18519	No
6480	22	4 194 304	2 427.259	Yes
6552	15	32 768	18.9630	Yes
6600	15	32 768	20.48	Yes
6624	14	16 384	7.75758	Yes
6660	12	4 096	2.37037	No
6720	20	1 048 576	682.667	Yes
6732	14	16 384	8.53333	No
6804	13	8 192	4.21399	No
6840	16	65 536	28.4444	Yes
6900	14	16 384	9.30909	No

6912	16	65 536	28.4444	Yes
6930	14	16 384	11.3778	Yes
6960	13	8 192	4.57143	No
7020	17	131 072	75.8519	Yes
7056	16	65 536	32.5079	Yes
7128	16	65 536	30.3407	Yes
7140	15	32 768	21.3333	Yes
7176	12	4 096	1.93939	No
7200	19	524 288	273.067	Yes
7260	11	2 048	1.16364	No
7280	12	4 096	1.77778	No
7308	11	2 048	1.01587	No
7344	15	32 768	14.2222	Yes
7380	13	8 192	4.26667	Yes
7392	17	131 072	68.2667	Yes
7440	11	2 048	1.06667	No
7452	12	4 096	1.72391	No
7488	17	131 072	56.8889	Yes
7560	24	16 777 216	9 709.04	Yes
7644	11	2 048	1.01587	No
7680	14	16 384	8.0	No
7728	13	8 192	3.87879	No
7740	13	8 192	4.06349	No
7776	15	32 768	12.6420	Yes
7800	16	65 536	34.1333	Yes
7920	21	2 097 152	1 092.27	Yes

7956	12	4 096	1.77778	No
7980	13	8 192	4.74074	No
8064	20	1 048 576	455.111	Yes
8100	18	262 144	121.363	Yes
8160	14	16 384	8.0	No
8190	15	32 768	18.9630	Yes
8208	12	4 096	1.58025	No
8280	18	262 144	124.121	Yes
8316	17	131 072	60.6815	Yes
8352	16	65 536	24.3810	Yes
8400	24	16 777 216	8 738.13	Yes
8424	12	4 096	1.58025	No
8448	14	16 384	6.4	Yes
8460	13	8 192	3.71015	No
8568	18	262 144	113.778	Yes
8580	14	16 384	8.53333	Yes
8640	21	2 097 152	910.222	Yes
8712	16	65 536	24.8242	Yes
8736	16	65 536	28.4444	Yes
8820	19	524 288	260.064	Yes
8880	15	32 768	14.2222	Yes
8910	13	8 192	3.79260	No
8928	12	4 096	1.42222	No
8960	12	4 096	1.33333	No
9000	19	524 288	218.453	Yes
9072	19	524 288	202.272	Yes

9108	15	32 768	12.4121	Yes
9120	17	131 072	56.889	Yes
9180	20	1 048 576	455.111	Yes
9216	13	892	2.66667	No
9240	21	2 097 152	1 092.27	Yes
9360	22	4 194 304	1 820.44	Yes
9396	12	4 096	1.35450	No
9408	13	8 192	1.89630	No
9450	12	4 096	1.89630	No
9504	18	262 144	91.0222	Yes
9520	13	8 192	2.66667	No
9600	19	524 288	204.8	Yes
9660	20	1 048 576	496.485	Yes
9720	19	524 288	202.2716	Yes
9792	14	16 384	5.333333	No
9828	15	32 768	12.64198	Yes
9856	12	4 096	1.066667	No
9900	19	524 288	218.4533	Yes
9936	16	65 536	20.68687	Yes
9984	14	16 384	5.333333	Yes
10 080	27	134 217 728	58 254.22	Yes
10 152	12	4 096	1.236715	No
10 200	15	32 768	12.8	Yes
10 224	12	4 096	1.219048	No
10 260	14	16 384	6.32098	Yes
10 296	17	131 072	45.5111	Yes

10 320	14	16 384	6.09523	No
10 332	12	4 096	1.42222	No
10 368	18	262 144	75.8519	Yes
10 440	16	65 536	24.3809	Yes
10 500	16	65 536	27.3067	Yes
10 530	12	4 096	1.58025	No
10 560	19	524 288	204.8	Yes
10 584	15	32 768	10.8359	Yes
10 620	12	4 096	1.47126	No
10 656	12	4 096	1.18519	No
10 692	14	16 384	5.05679	No
10 710	15	32 768	14.2222	Yes
10 752	15	32 768	10.66667	No
10 764	12	4 096	1.292929	No
10 800	23	8 388 608	2 912.711	Yes
10 890	12	4 096	1.551515	No
10 920	20	1 048 576	455.111	Yes
10 944	12	4 096	1.18519	No
11 016	15	32 768	9.48148	Yes
11 040	16	65 536	23.2727	Yes
11 088	20	1 048 576	364.089	Yes
11 160	16	65 536	23.2727	Yes
11 200	14	16 384	4.26667	No
11 220	12	4 096	1.6	No
11 232	16	65 536	18.9629	Yes
11 280	13	8 192	2.78619	No

11340	23	8 388 608	3 236.35	Yes
11 400	18	262 144	91.0222	Yes
11 424	15	32 768	10.66667	Yes
11 484	14	16 384	4.87619	Yes
11 520	19	524 288	170.667	Yes
11 550	13	8 192	3.41333	No
11 592	17	131 072	41.3737	Yes
11 616	12	4 096	1.16364	No
11 664	15	32 768	8.42799	Yes
11 700	19	524 288	182.044	Yes
11 760	19	524 288	195.048	Yes
11 880	23	8 388 608	2 912.71	Yes
11 952	12	4 096	1.04065	No
12 000	18	262 144	81.92	Yes
12 012	14	16 384	5.68889	No
12 096	23	8 388 608	2 427.26	Yes
12 144	13	8 192	2.327273	No
12 168	13	8 192	3.047619	No
12 180	13	8192	3.047619	No
12 240	22	4 194 304	1 365.33	Yes
12 276	14	16 384	4.55111	No
12 300	12	4 096	1.28	No
12 320	12	4 096	1.066667	No
12 384	12	4 096	1.015873	No
12 420	20	1 048 576	330.990	Yes
12 432	14	16 384	4.92307	No

12 480	18	262 144	85.3333	Yes
12 528	16	65 536	16.2539	Yes
12 540	14	16 384	5.68889	No
12 600	27	134 217 728	46 603.38	Yes
12 672	21	2 097 152	546.1333	Yes
12 720	14	16 384	4.92307	No
12 768	13	8 192	2.37037	No
12 780	14	16 384	4.87619	No
12 852	19	524 288	151.7037	Yes
12 870	12	4 096	1.42222	No
12 960	24	16 777 216	4 854.519	Yes
13 020	12	4 096	1.42222	No
13 068	14	16 384	4.13737	No
13 104	20	1 048 576	303.4074	Yes
13 200	20	1 048 576	327.68	Yes
13 230	14	16 384	5.41789	No
13 248	17	131 072	31.0303	Yes
13 260	13	8 192	2.66667	No
13 320	16	65 536	18.9629	Yes
13 440	24	16 777 216	5 461.33	Yes
13 464	18	262 144	68.2667	Yes
13 500	16	65 536	18.2044	Yes
13 608	14	16 384	4.21399	No
13 650	13	8192	2.84444	No
13 680	20	1 048 576	303.4074	Yes
13 728	16	65 536	17.0667	Yes

13 770	12	4 096	1.18519	No
13 800	16	65 536	18.2857	Yes
13 824	16	65 536	14.2222	Yes
13 860	23	8 388 608	2 912.711	Yes
13 920	16	65 536	18.2857	Yes
14 000	14	16 384	3.41333	No
14 040	22	4 194 304	1 213.63	Yes
14 076	14	16 384	3.87879	No
14 112	19	524 288	130.0317	Yes
14 160	13	8192	2.20688	No
14 196	12	4 096	1.09402	No
14 220	12	4 096	1.09402	No
14 256	19	524 288	121.363	Yes
14 280	22	4 194 304	1 365.333	Yes
14 352	13	8 192	1.93939	No
14 364	13	8 192	2.10700	No
14 400	24	16 777 216	4 369.067	Yes
14 490	13	8 192	2.58386	No
14 520	14	16 384	4.65455	No
14 560	14	16 384	3.55556	No
14 580	18	262 144	67.4239	Yes
14 592	13	8 192	1.77778	No
14 616	14	16 384	4.06349	No
14 640	13	8 192	2.13333	No
14 688	16	65 536	14.2222	Yes
14 700	17	131 072	39.0095	Yes

14 760	15	32 768	8.53333	Yes
14 784	20	1 048 576	273.0667	Yes
14 820	14	16 384	4.74074	No
14 850	13	8 192	2.27556	No
14 880	12	4 096	1.06667	No
14 904	15	32 768	6.89562	No
14 976	19	524 288	113.7778	Yes
15 000	12	4 096	1.024	No
15 048	13	8 192	1.89630	No
15 120	32	4 294 967 296	1 242 757.0	Yes
15 180	17	131 072	37.2364	Yes
15 288	13	8 192	2.03175	No
15 300	18	262 144	68.2667	Yes
15 336	13	8 192	1.62540	No
15 360	15	32 768	8.0	No
15 444	14	16 384	3.79259	No
15 456	16	65 536	15.5152	Yes
15 480	17	131 072	32.5079	Yes
15 540	15	32 768	9.48148	Yes
15 552	17	131 072	25.2840	Yes
15 600	22	4 194 304	1 092.267	Yes
15 624	13	8 192	1.89630	No
15 680	13	8 192	1.52381	No
15 708	12	4 096	1.06667	No
15 750	13	8 192	2.275556	No
15 840	25	33 554 432	8 738.133	Yes

15 876	16	65 536	14.4479	No
15 912	18	262 144	56.8889	Yes
15 960	18	262 144	75.8519	Yes
15 984	14	16 384	3.16049	No
16 080	13	8 192	1.93940	No
16 128	22	4 194 304	910.2222	Yes
16 200	22	4 194 304	970.9037	Yes
16 236	13	8 192	1.70667	No
16 320	16	65 536	16.0	Yes
16 368	13	8 192	1.70667	No
16 380	25	33 554 432	9 709.037	Yes
16 416	14	16 384	3.16049	No
16 500	14	16 384	4.096	No
16 524	13	8 192	1.58025	No
16 560	23	8 388 608	1 985.939	Yes
16 632	22	4 194 304	970.9037	Yes
16 704	19	524 288	97.5238	Yes
16 740	17	131 072	30.3407	Yes
16 800	27	134 217 728	34 952.53	Yes
16 830	14	16 384	4.26667	No
16 848	16	65 536	12.6419	Yes
16 896	14	16 384	4.21399	No
16 920	18	262 144	59.3623	Yes
16 992	13	8 192	1.471264	No
17 010	14	16 384	4.21399	No
17 028	13	8 192	1.62540	No

17 040	14	16 384	3.65714	No
17 100	15	32 768	7.58518	Yes
17 136	22	4 194 304	910.2222	Yes
17 160	20	1 048 576	273.0667	Yes
17 220	14	16 384	4.26667	No
17 280	24	16 777 216	3 640.889	Yes
17 388	17	131 072	27.5825	Yes
17 400	16	65 536	14.6285	Yes
17 424	17	131 072	24.8242	Yes
17 460	13	8 192	1.77778	No
17 472	18	262 144	56.8889	Yes
17 520	13	8 192	1.77778	No
17 550	13	8 192	1.89630	No
17 568	13	8 192	1.42222	No
17 640	25	33 554 432	8 322.032	Yes
17 712	13	8 192	1.42222	No
17 748	13	8 192	1.52381	No
17 760	17	131 072	28.4444	Yes
17 784	14	16 384	3.16049	No
17 820	22	4 194 304	970.9037	Yes
17 850	12	4 096	1.06667	No
17 856	15	32 768	5.68889	No
17 920	13	8 192	1.33333	No
17 928	13	8 192	1.38753	No
17 940	17	131 072	31.0303	Yes
18 000	23	8 388 608	1 747.627	Yes

18 060	14	16 384	4.06349	No
18 144	23	8 388 608	1 618.173	Yes
18 180	13	8 192	1.70667	No
18 200	13	8 192	1.42222	No
18 216	20	1 048 576	198.5939	Yes
18 240	19	524 288	113.7778	Yes
18 360	26	67 108 864	14 563.56	Yes
18 396	14	16 384	3.16049	No
18 432	14	16 384	2.66667	No
18 480	28	268 435 456	69 905.07	Yes
18 564	14	16 384	3.55556	No
18 720	25	33 554 432	7 281.778	Yes
18 792	16	65 536	10.8359	No
18 816	14	16 384	3.04761	No
18 900	24	16 777 216	3 883.615	Yes
19 008	23	8 388 608	1 456.356	Yes
19 040	13	8 192	1.333333	No
19 080	15	32 768	6.56410	No
19 110	13	8 192	2.03175	No
19 140	14	16 384	3.65714	No
19 152	16	65 536	12.6419	Yes
19 200	21	2 097 152	409.6	Yes
19 260	13	8 192	1.61006	No
19 320	23	8 388 608	1 985.939	Yes
19 380	13	8 192	1.77778	No
19 404	15	32 768	6.50158	No

19 440	27	134 217 728	25 890.77	Yes
19 488	14	16 384	3.04761	No
19 500	16	65 536	13.6533	No
19 536	13	8 912	1.42222	No
19 584	16	65 536	10.6667	Yes
19 600	14	16 384	2.43809	No
19 656	19	524 288	101.1358	Yes
19 712	13	8 192	1.06667	No
19 740	14	16 384	3.71014	No
19 800	26	67 108 864	13 981.01	Yes
19 872	17	131 072	20.6869	Yes
19 890	13	8 192	1.77778	No
19 968	14	16 384	2.66667	No
19 980	16	65 536	12.6419	Yes
19 992	15	32 768	6.09523	No

Project Faculty Adviser:
Dr. John R. Greene, Department of Mathematics and Statistics, Swenson College of Science and Engineering, University of Minnesota Duluth. Email: jgreene@d.umn.edu

View Statistics