The Rabin- Miller Probabilistic Primality Test:
Some Results on the Number of Non-Witnesses to Compositeness

Brian C. Higgins
Division of Science
Penn State Erie-The Behrend College
Erie, PA 16563

Faculty Advisor: Mr. Charles L. Burchard

Abstract

This paper introduces the reader to the Rabin-Miller probabilistic primality test, the concept of non-witnesses to compositeness, and the problem of determining the number of non-witnesses to compositeness. Given in this paper are two conjectures: one on determining the number of non-witnesses to compositeness of numbers with two distinct prime factors, and another on producing composite numbers with a maximal number of non-witnesses. We also present computer generated data that supports these conjectures.

1. Introduction

The problem of determining if a given number is prime is of great interest to both computer scientists and mathematicians. According to the great mathematician Gauss [1], the problem of distinguishing prime numbers from composite numbers and of resolving the latter into their prime factors is known to be one of the most important and useful in arithmetic. For example, in today's technological world one needs to be able to identify "large" prime numbers to implement a public key encryption system. An excellent description of public key algorithms can be found in, Schneier [2]. As stated by Schneier [2], the security of a public key encryption system is based on the conjecture that multiplying two large primes is a one-way function. That is, it is easy to multiply the numbers to get a product but hard to factor the product and recover the large primes. This provides the reader with some motivation of the importance of determining the primality of a number. There are several tests that can quickly determine if a given large number is prime with a certain confidence. One such test is the Rabin-Miller probabilistic primality test.

2. Features of The Rabin-Miller Probabilistic Primality Algorithm

The Rabin-Miller probabilistic primality test was developed by Rabin [3], based on Miller's [4] ideas. This algorithm provides a fast method of determining the primality of a number with a controllably small probability of error. The algorithm is described below.

2.1. The Rabin-Miller Probabilistic Primality Algorithm

Given (b,n) where n is the number to test for primality, and b is randomly chosen in [1, n -1]. Let $n - 1 = 2^q m$, where m is an odd integer. If either

(a) $b^m \equiv 1 \pmod{n}$ or
(b) there is an integer i in [0, q -1] such that $b^{m2^\wedge i} \equiv -1 \pmod{n}$

then return ‘inconclusive’ else return ‘n is composite.’

Rabin [3], shows that the algorithm has the characteristic that for a composite number, n, at most 1/4 of the bases, b, will result in ‘inconclusive.’ The interpretation of the result ‘inconclusive’ is that so far the number n is acting as a prime (i.e. n may be prime) This characteristic is described in more detail in section 3 of this paper. However, we will now describe how this allows one to test the primality of a number probabilistically.

2.2. Interpreting the Rabin-Miller Probabilistic Primality Algorithm

The algorithm enables one to probabilistically test the primality of a number n as follows:

1. If n fails the test (i.e. results in 'n is composite') for any b in [1,n-1] then n is definitely composite (although, interestingly, no factor is provided by the algorithm).

2. A composite number has at most 1 chance in 4^k of passing all k of a series of k tests, where b is chosen randomly from [1,n -1] for each test. Therefore, if a suspected prime, n, passes k of k tests, we conclude with a certainty at least $1 - (1/4)^k$ that n is prime.

Rabin [3], gives the following interpretation of step 2 above. This statement does not mean that an integer n asserted as prime by use of 50 random numbers is prime with probability at least $1 - (1/4)^{50}$. Such an interpretation is nonsensical since n is either prime or not. The correct meaning is that if the test is applied to $m = 4^{50}$ integers n_1, n_2,..., n_m, then the expected number of wrong answers is one.

2.3. Implementation of the Algorithm on a Known Prime

We will now demonstrate this algorithm on a number that we definitely know is prime, say n = 29. Since $28 = 2^2 * 7$, we let $q = 2$ and $m = 7$. To apply this algorithm we need to randomly select a number to use in the test, say b =10. Then $10^7 \equiv 17 \pmod{29}$ which is not congruent to 1 or -1 so we continue the test. We obtain $(10^7)^2 \equiv -1 \pmod{29}$ so the test returns 'inconclusive' (i.e. 29 may be prime).

Let us perform the test with another randomly selected base, say b = 19. Then $19^7 \equiv 12 \pmod{29}$ which is not congruent to 1 or -1 so we continue the test. We obtain $(19^7)^2 \equiv -1 \pmod{29}$ so the test again returns 'inconclusive' (i.e. 29 may be prime). If we perform the algorithm on all bases b in [1,28] the test returns 'inconclusive' in each case. In fact for any prime number, p, we know all the bases in [1, p-1] result in 'inconclusive'.

2.4. Implementation of the Algorithm on a Composite Number

To demonstrate the result of the test for various bases on a composite number we will use $n = 13*17 = 221$. Since $220 = 2^2 * 55$, we let $q = 2$ and $m = 55$. To apply this algorithm we will need a randomly selected base, say b = 5. Then $5^{55} \equiv 112 \pmod{221}$ which is not congruent to 1 or -1 so we continue the test. We obtain $(5^{55})^2 \equiv 168 \pmod{221}$ which is not congruent to -1. Since we used all i in [0,1] the test returns that 221 is definitely composite.

However what happens if we did not randomly choose b = 5 but say we selected b = 21. Then $(21)^{55} \equiv 200 \pmod{221}$ which is not congruent to 1 or -1 so we continue the test. We obtain $(21^{55})^2 \equiv -1 \pmod{221}$ so the test returns 'inconclusive.' That is for a composite number 221 the test returns 'inconclusive' (i.e. 221 may be prime) for the base 21.

We call such a base a ***non-witness*** to the compositeness of 221. That is, if the base b in [1,n-1] results in 'inconclusive' for a composite number n, then b is a non-witness to the compositeness of n. In fact, 221 has six non-witnesses -- namely 1, 21, 47, 174, 200, and 220. We denote the number of non-witnesses for a number, n, by $nw(n)$. So in our example $nw(221) = 6$.

3. The Number of Non- Witnesses to the Compositeness of a Number

Rabin [3], states that the number of witnesses to compositeness has a lower bound. This statement is given as our first theorem.

Theorem 1 If $n > 4$ is composite, then the number of bases, b, in $[1, n-1]$ such that b is a witness to the compositeness of n is at least $3(n-1)/4$.

The following corollary describing the upper bound on non-witnesses to compositeness follows directly from theorem 1.

Corollary 1 If $n > 4$ is composite then at most $(n-1)/4$ of the bases, b, in $[1, n-1]$ are non-witnesses to the compositeness of n.

For the composite number 221 = 13 * 17 we expect at least 3 (220) / 4 = 165 of the bases are witnesses to the compositeness of 221. In fact we found that 221 has 214 witnesses to its compositeness. Similarly, for the composite number 221 = 13 * 17 we expect at most 220 / 4 = 55 of the bases are non-witnesses. In fact we found that 221 has only 6 non-witnesses.

4. Empirical Evidence

The reader can verify that the composite number 221 has very few non-witnesses. In fact, while implementing the Rabin-Miller probabilistic primality test on very large composite numbers we rarely, if ever, found non-witnesses. We therefore set out to answer two questions which are stated below.

1. As Corollary 1 states, we know the number of non-witnesses is bounded. However we want to determine the exact number of non-witnesses for a composite number.

2. We want to know if we can produce composite numbers whose number of non-witnesses approaches the 1/4 upper bound proven by Rabin.

4.1. Initial Empirical Data

As stated above, we rarely discovered composite numbers with the number of non-witnesses approaching the upper bound. **Table 1** (located at the end of this paper) displays composite numbers, their factorization, the number of non-witnesses, denoted $nw(n)$, and the upper bound of non-witnesses. The number of non-witnesses for any composite number given in the table does not approach the upper bound of $(n-1)/4$.

When analyzing our data we discovered the most interesting composite numbers appear to be those with two distinct prime factors. **Table 2** (found at the end of this paper) shows a list of composite numbers having two distinct prime factors, p and q. Also shown is d, the greatest common divisor of $p - 1$ and $q - 1$ (i.e. $d = \gcd(p-1, q-1)$), and the number of non-witnesses of n, denoted $nw(n)$. When analyzing this data we discovered recurring numbers for $nw(n)$. For example, the composite numbers 65, 221, 493, 1073, 1517, 2173, 3233, 9797, 11009, and 12317 all have 6 non-witnesses.

As stated earlier we are interested in determining a method for calculating *nw*(*n*). After studying such data as displayed in Table 2, we believe the number of non-witnesses is a function of d = gcd(p -1, q -1). That is, given d = gcd(p -1, q -1) the table below can be used to determine the exact number of non-witnesses of $n = pq$ where p and q are distinct primes.
Using this table we conclude that for a composite number 4187 = 53*79 with d = gcd(52, 78) = 26 the number of non-witnesses is 338. The reader can verify this claim by looking at Table 2.

d	*nw*(*n*)	*d*	*nw*(*n*)	*d*	*nw*(*n*)	*d*	*nw*(*n*)
2	2	26	338	50		74	
4	6	28	294	52	1014	76	
6	18	30	450	54	1458	78	3042
8	22	32		56	1078	80	
10	50	34	578	58	1682	82	
12	54	36	486	60	1350	84	
14	98	38		62		86	
16	86	40	550	64		88	2662
18	162	42	882	66		90	
20	150	44		68		92	
22	242	46	1058	70	2450	94	
24	198	48		72	1782	96	3078

Note: This table was produced after analyzing a great amount of data similar to that shown in Table 2. The table contains gaps because calculations were performed on 32-bit integers.

4.1. Our Conjecture of the Number of Non-Witnesses of n = pq

This table allowed us to discover a formula relating d to *nw*(*n*). We state this formula as our first conjecture.

Conjecture 1
Let $n = pq$ with p and q distinct primes and let d = gcd(p-1,q-1). Then the number of non-witnesses to the compositeness of n, denoted *nw*(*n*) is

$$r^2 * (2 + (4^t - 4) / 3) \text{ where } d = 2^t * r \text{ with } r \text{ odd.}$$

Example Let n = 8321 = 53 * 157. Then d = gcd(52, 156) = 52. Also 52 = 2^2 * 13. So from our conjecture *nw*(8321) = 13^2 (2 +(4^2- 4) / 3) = 1014. In fact Table 2 verifies that the number 8321 has 1014 non-witnesses to its compositeness. So our conjecture holds for 8321.

4.2. Our Conjecture of Composite Numbers with *nw*(*n*) Approaching the Upper Bound

The second question we want to answer is if we can produce composite numbers whose number of non-witnesses approaches the upper bound of (n -1) / 4. We have found certain numbers whose number of non-witnesses equals one-fourth $\phi(n)$, the Euler Totient function of n. This is stated as our second conjecture.

Conjecture 2 Let $n = pq$ where p and q are prime such that $p = 2r + 1$ and $q = 4r + 1$ with r an odd positive integer. Then $nw(n) = \phi(n) / 4$. (Note that if $n = pq$ where p and q are distinct primes, then $\phi(n) = (p-1)(q-1)$)

Example Let n = 1891 = 31 * 61. Note 31 = 2*15 +1 and 61 = 4*15 +1. From Table 2 we see that nw(1891) = 450, and in fact 4 * 450 = 30 * 60 = 1800 = ϕ (1891).

It is important to realize that $\phi(n)$ / 4 approaches n / 4 as n approaches infinity. Thus for large composite numbers of the form described in conjecture 2 the number of non-witnesses approaches the upper bound.

4.3. Empirical Data Supporting Conjectures 1 and 2

Next we set out to test our conjectures on larger composite numbers, n. Since testing every number in the interval [1, n-1] to find the number of non-witnesses is infeasible, we randomly sampled this interval to determine the proportion of non-witnesses.

We first need to find prime numbers of the form $2r$+1 and $4r$+1 where r is an odd positive integer. Then we compute $n = (2r+1)(4r+1)$ and randomly test the numbers in the interval [1, n-1] for non-witnesses. **Table 3** shows a list of numbers r (where $2r$+1 and $4r$+1 are prime), the sample size, the number of non-witnesses, and the proportion of non-witnesses to the sample size. Our conjectures suggest this proportion should be close to 1/4. The reader can verify that Table 3 supports this claim.

5. Further Work

We have given empirical evidence to support our conjecture for the number of non-witnesses to the compositeness of $n = pq$, but we have not yet proven this. Further, we have not extended our conjecture to composite numbers of other forms.

6. Summary

This paper introduced the reader to the Rabin-Miller probabilistic primality test, the concept of non-witnesses to compositeness, and the problem of determining the number of non-witnesses to compositeness. Given in this paper are two conjectures: one on determining the number of non-witnesses to compositeness and another on producing composite numbers with the maximal number of non-witnesses. We also presented computer generated data that supports these conjectures. Our investigation of this problem supports our earlier observations that, except for composite numbers of a very specific form, the number of non-witnesses to compositeness is extremely small.

7. References

1. Gauss, C. F., "Disquistiones Arithmeticae" (A.A Clarke, Transl.) Yale Univ. Press, New Haven, Conn. London, 1966. p. 396.

2. Schneier, Bruce., Applied Cryptography: Protocols, Algorithms, and Source Code in C . New York: John Wiley & Sons, Inc., 1994. pp. 213.

3. Rabin, M.O., "Probabilistic Algorithm for Primality Testing" Journal of Number Theory. Vol. 12, 1980. pp. 128-138.

4. Miller, G.L., "Riemann's Hypothesis and Tests for Primality," Journal of Computer Systems Science, Vol. 13, No. 3, Dec 1976, pp 300-317.

TABLE 1.

N	*phi*(*N*)	nw(N)
105 = 3*5*7	48	2
111 = 3*37	72	2
115 = 5*23	88	2
117 = 3^2*13	72	2
119 = 7*17	96	2
121 = 11^2	110	10
123 = 3*41	80	2
125 = 5^3	100	4
129 = 3*43	2	2
133 = 7*19	108	18
135 = 3^3*5	72	2
141 = 3*47	92	2
143 = 11*13	120	2
145 = 5*29	112	6
147 = 3*7^2	84	2
153 = 3^2*17	96	2
155 = 5*31	120	2
159 = 3*53	104	2
161 = 7*23	132	2
165 = 3*5*11	80	2
169 = 13^2	156	12
171 = 3^2*19	108	2
175 = 5^2*7	120	6
177 = 3*59	116	2
183 = 3*61	120	2
185 = 5*37	144	6
187 = 11*17	160	2
189 = 3^3*7	108	2
195 = 3*5*13	96	2

N	*phi(N)*	*nw(N)*	
1903 = 11*173	1720	2	
1905 = 3*5*127	1008	14	
1909 = 23*83	1804	2	
1911 = 3*7^2*13		1008	2
1915 = 5*383	1528	2	
1917 = 3^3*71	1260	2	
1919 = 19*101	1800	2	
1921 = 17*113	1792	86	
1923 = 3*641	1280	2	
1925 = 5^2*7*11		1200	2
1927 = 41*47	1840	2	
1929 = 3*643	1284	2	
1935 = 3^2*5*43		1008	2
1937 = 13*149	1776	6	
1939 = 7*277	1656	18	
1941 = 3*647	1292	2	
1943 = 29*67	1848	2	
1945 = 5*389	1552	6	
1947 = 3*11*59	1160	2	
1953 = 3^2*7*31		1080	2
1955 = 5*17*23	1408	2	
1957 = 19*103	1836	18	
1959 = 3*653	1304	2	
1961 = 37*53	1872	6	
1963 = 13*151	1800	18	
1965 = 3*5*131	1040	2	
1967 = 7*281	1680	2	
1969 = 11*179	1780	2	
1971 = 3^3*73	1296	2	
1975 = 5^2*79	1560	6	
1977 = 3*659	1316	2	
1981 = 7*283	1692	18	
1983 = 3*661	1320	2	
1985 = 5*397	1584	6	
1991 = 11*181	1800	50	
1995 = 3*5*7*19		864	2

TABLE 2.

N		D	NW(N)
15	= 3*5	2	2
35	= 5*7	2	2
65	= 5*13	4	6
77	= 7*11	2	2
91	= 7*13	6	18
143	= 11*13	2	2
341	= 11*31	10	50
221	= 13*17	4	6
247	= 13*19	6	18
481	= 13*37	12	54
323	= 17*19	2	2
493	= 17*29	4	6
697	= 17*41	8	22
1649	= 17*97	16	86
437	= 19*23	2	2
589	= 19*31	6	18
703	= 19*37	18	162
667	= 23*29	2	2
1541	= 23*67	22	242
899	= 29*31	2	2
1073	= 29*37	4	6
1247	= 29*43	14	98
3277	= 29*113	28	294
1147	= 31*37	6	18
1271	= 31*41	10	50
1891	= 31*61	30	450
1517	= 37*41	4	6
1591	= 37*43	6	18
2257	= 37*61	12	54
2701	= 37*73	36	486
1763	= 41*43	2	2
2173	= 41*53	4	6
2501	= 41*61	20	150
9881	= 41*241	40	550
2021	= 43*47	2	2
2623	= 43*61	6	18
3053	= 43*71	14	98
5461	= 43*127	42	882
2491	= 47*53	2	2
6533	= 47*139	46	1058
3127	= 53*59	2	2
3233	= 53*61	4	6
4187	= 53*79	26	338
8321	= 53*157	52	1014
3599	= 59*61	2	2
4087	= 61*67	6	18
4331	= 61*71	10	50

N		D	NW(N)
6161	= 61*101	20	150
9211	= 61*151	30	450
11041	= 61*181	60	1350
4757	= 67*71	2	2
4891	= 67*73	6	18
5963	= 67*89	22	242
13333	= 67*199	66	2178
5183	= 71*73	2	2
7171	= 71*101	10	50
8023	= 71*113	14	98
14981	= 71*211	70	2450
5767	= 73*79	6	18
6497	= 73*89	8	22
7081	= 73*97	24	198
7957	= 73*109	36	486
31609	= 73*433	72	1782
6557	= 79*83	2	2
7663	= 79*97	6	18
10349	= 79*131	26	338
12403	= 79*157	78	3042
7387	= 83*89	2	2
8633	= 89*97	8	22
17711	= 89*199	22	242
31417	= 89*353	88	2662
9797	= 97*101	4	6
9991	= 97*103	6	18
10573	= 97*109	12	54
10961	= 97*113	16	86
18721	= 97*193	96	3078
11009	= 101*109	4	6
13231	= 101*131	10	50
15251	= 101*151	50	1250
11021	= 103*107	2	2
11227	= 103*109	6	18
14111	= 103*137	34	578
31621	= 103*307	102	5202
11663	= 107*109	2	2
12317	= 109*113	4	6
13843	= 109*127	18	162
17767	= 109*163	54	1458
14351	= 113*127	14	98
21809	= 113*193	16	86
22261	= 113*197	28	294
31753	= 113*281	56	1078
16637	= 127*131	2	2
17653	= 127*139	6	18
20701	= 127*163	18	162
26797	= 127*211	42	882

Table 3. Sample size: 1000

r = 1000185	n = 8002966274911	Non-witnesses: 267
r = 1000365	n = 8005847067991	Non-witnesses: 237
r = 1000875	n = 8014012130251	Non-witnesses: 265
r = 1001163	n = 8018624827531	Non-witnesses: 253
r = 1001169	n = 8018720939503	Non-witnesses: 247
r = 1001193	n = 8019105393151	Non-witnesses: 248
r = 1001403	n = 8022469755691	Non-witnesses: 271
r = 1001433	n = 8022950436511	Non-witnesses: 259
r = 1001595	n = 8025546361771	Non-witnesses: 235
r = 1001919	n = 8030739472003	Non-witnesses: 250
r = 1002003	n = 8032086108091	Non-witnesses: 220
r = 1002045	n = 8032759468471	Non-witnesses: 260
r = 1002285	n = 8036607783511	Non-witnesses: 243
r = 1002465	n = 8039494624591	Non-witnesses: 234
r = 1002723	n = 8043633334171	Non-witnesses: 243
r = 1002759	n = 8044210913203	Non-witnesses: 239
r = 1002789	n = 8044692244903	Non-witnesses: 260
r = 1002843	n = 8045558678251	Non-witnesses: 250
r = 1003143	n = 8050373046451	Non-witnesses: 226
r = 1003389	n = 8054321902903	Non-witnesses: 259
r = 1003479	n = 8055766848403	Non-witnesses: 251
r = 1003533	n = 8056633877911	Non-witnesses: 253
r = 1003743	n = 8060006102851	Non-witnesses: 239
r = 1003809	n = 8061066090703	Non-witnesses: 245

r = 1003935	n = 8063089897411	Non-witnesses:	272
r = 1004025	n = 8064535629151	Non-witnesses:	248
r = 1004859	n = 8077938908203	Non-witnesses:	251

r = 1004865	n = 8078035374991	Non-witnesses:	223
r = 1005069	n = 8081315588503	Non-witnesses:	227
r = 1005549	n = 8089036364503	Non-witnesses:	248
r = 1005585	n = 8089615571311	Non-witnesses:	236
r = 1005645	n = 8090580962071	Non-witnesses:	242
r = 1005795	n = 8092994690971	Non-witnesses:	263
r = 1005993	n = 8096181364351	Non-witnesses:	232
r = 1006005	n = 8096374516231	Non-witnesses:	263
r = 1006413	n = 8102943051031	Non-witnesses:	247
r = 1006485	n = 8104102480711	Non-witnesses:	229
r = 1006623	n = 8106324952771	Non-witnesses:	235
r = 1006755	n = 8108451080731	Non-witnesses:	269
r = 1006809	n = 8109320940703	Non-witnesses:	245
r = 1006875	n = 8110384166251	Non-witnesses:	228
r = 1007073	n = 8113574261071	Non-witnesses:	266
r = 1007133	n = 8114541080311	Non-witnesses:	261
r = 1007229	n = 8116088110903	Non-witnesses:	216
r = 1007379	n = 8118505641403	Non-witnesses:	276
r = 1007535	n = 8121020255011	Non-witnesses:	259
r = 1007589	n = 8121890788903	Non-witnesses:	258
r = 1007643	n = 8122761369451	Non-witnesses:	246
r = 1007673	n = 8123245045471	Non-witnesses:	256
r = 1007745	n = 8124405926671	Non-witnesses:	242

r = 1938472012374902718493827486 15

n = 30061_38994_20864_39985_49240_64133_18286_92398_52965_42927_45718_37491

Non-witnesses: 230

r = 42342342455564745747657475645354531395
n =
14_34299_17169_94565_94175_96370_67138_75678_09312_55074_72733_09678_48556_39035_24523_56571
Non-witnesses: 279

TABLE 2.

N		D	NW(N)
15	= 3*5	2	2
35	= 5*7	2	2
65	= 5*13	4	6
77	= 7*11	2	2
91	= 7*13	6	18
143	= 11*13	2	2
341	= 11*31	10	50
221	= 13*17	4	6
247	= 13*19	6	18
481	= 13*37	12	54
323	= 17*19	2	2
493	= 17*29	4	6
697	= 17*41	8	22
1649	= 17*97	16	86
437	= 19*23	2	2
589	= 19*31	6	18
703	= 19*37	18	162
667	= 23*29	2	2
1541	= 23*67	22	242
899	= 29*31	2	2
1073	= 29*37	4	6
1247	= 29*43	14	98
3277	= 29*113	28	294
1147	= 31*37	6	18
1271	= 31*41	10	50
1891	= 31*61	30	450
1517	= 37*41	4	6
1591	= 37*43	6	18
2257	= 37*61	12	54
2701	= 37*73	36	486
1763	= 41*43	2	2
2173	= 41*53	4	6
2501	= 41*61	20	150
9881	= 41*241	40	550
2021	= 43*47	2	2
2623	= 43*61	6	18
3053	= 43*71	14	98
5461	= 43*127	42	882
2491	= 47*53	2	2
6533	= 47*139	46	1058

3127 = 53*59	2	2
3233 = 53*61	4	6
4187 = 53*79	26	338
8321 = 53*157	52	1014
3599 = 59*61	2	2
4087 = 61*67	6	18
4331 = 61*71	10	50

N	D	NW(N)
6161 = 61*101	20	150
9211 = 61*151	30	450
11041 = 61*181	60	1350
4757 = 67*71	2	2
4891 = 67*73	6	18
5963 = 67*89	22	242
13333 = 67*199	66	2178
5183 = 71*73	2	2
7171 = 71*101	10	50
8023 = 71*113	14	98
14981 = 71*211	70	2450
5767 = 73*79	6	18
6497 = 73*89	8	22
7081 = 73*97	24	198
7957 = 73*109	36	486
31609 = 73*433	72	1782
6557 = 79*83	2	2
7663 = 79*97	6	18
10349 = 79*131	26	338
12403 = 79*157	78	3042
7387 = 83*89	2	2
8633 = 89*97	8	22
17711 = 89*199	22	242
31417 = 89*353	88	2662
9797 = 97*101	4	6
9991 = 97*103	6	18
10573 = 97*109	12	54
10961 = 97*113	16	86
18721 = 97*193	96	3078
11009 = 101*109	4	6
13231 = 101*131	10	50
15251 = 101*151	50	1250
11021 = 103*107	2	2
11227 = 103*109	6	18
14111 = 103*137	34	578
31621 = 103*307	102	5202
11663 = 107*109	2	2
12317 = 109*113	4	6
13843 = 109*127	18	162

17767 = 109*163	54	1458
14351 = 113*127	14	98
21809 = 113*193	16	86
22261 = 113*197	28	294
31753 = 113*281	56	1078
16637 = 127*131	2	2
17653 = 127*139	6	18
20701 = 127*163	18	162
26797 = 127*211	42	882

Table 3. Sample size: 1000

r = 1000185	n = 8002966274911	Non-witnesses: 267
r = 1000365	n = 8005847067991	Non-witnesses: 237
r = 1000875	n = 8014012130251	Non-witnesses: 265
r = 1001163	n = 8018624827531	Non-witnesses: 253
r = 1001169	n = 8018720939503	Non-witnesses: 247
r = 1001193	n = 8019105393151	Non-witnesses: 248
r = 1001403	n = 8022469755691	Non-witnesses: 271
r = 1001433	n = 8022950436511	Non-witnesses: 259
r = 1001595	n = 8025546361771	Non-witnesses: 235
r = 1001919	n = 8030739472003	Non-witnesses: 250
r = 1002003	n = 8032086108091	Non-witnesses: 220
r = 1002045	n = 8032759468471	Non-witnesses: 260
r = 1002285	n = 8036607783511	Non-witnesses: 243
r = 1002465	n = 8039494624591	Non-witnesses: 234
r = 1002723	n = 8043633334171	Non-witnesses: 243
r = 1002759	n = 8044210913203	Non-witnesses: 239
r = 1002789	n = 8044692244903	Non-witnesses: 260
r = 1002843	n = 8045558678251	Non-witnesses: 250
r = 1003143	n = 8050373046451	Non-witnesses: 226

r = 1003389	n = 8054321902903	Non-witnesses:	259
r = 1003479	n = 8055766848403	Non-witnesses:	251
r = 1003533	n = 8056633877911	Non-witnesses:	253
r = 1003743	n = 8060006102851	Non-witnesses:	239
r = 1003809	n = 8061066090703	Non-witnesses:	245
r = 1003935	n = 8063089897411	Non-witnesses:	272
r = 1004025	n = 8064535629151	Non-witnesses:	248
r = 1004859	n = 8077938908203	Non-witnesses:	251
r = 1004865	n = 8078035374991	Non-witnesses:	223
r = 1005069	n = 8081315588503	Non-witnesses:	227
r = 1005549	n = 8089036364503	Non-witnesses:	248
r = 1005585	n = 8089615571311	Non-witnesses:	236
r = 1005645	n = 8090580962071	Non-witnesses:	242
r = 1005795	n = 8092994690971	Non-witnesses:	263
r = 1005993	n = 8096181364351	Non-witnesses:	232
r = 1006005	n = 8096374516231	Non-witnesses:	263
r = 1006413	n = 8102943051031	Non-witnesses:	247
r = 1006485	n = 8104102480711	Non-witnesses:	229
r = 1006623	n = 8106324952771	Non-witnesses:	235
r = 1006755	n = 8108451080731	Non-witnesses:	269
r = 1006809	n = 8109320940703	Non-witnesses:	245
r = 1006875	n = 8110384166251	Non-witnesses:	228
r = 1007073	n = 8113574261071	Non-witnesses:	266
r = 1007133	n = 8114541080311	Non-witnesses:	261

r = 1007229	n = 8116088110903	Non-witnesses:	216
r = 1007379	n = 8118505641403	Non-witnesses:	276
r = 1007535	n = 8121020255011	Non-witnesses:	259
r = 1007589	n = 8121890788903	Non-witnesses:	258
r = 1007643	n = 8122761369451	Non-witnesses:	246
r = 1007673	n = 8123245045471	Non-witnesses:	256
r = 1007745	n = 8124405926671	Non-witnesses:	242

r = 193847201237490271849382748615
n = 30061_38994_20864_39985_49240_64133_18286_92398_52965_42927_45718_37491
Non-witnesses: 230

r = 42342342455564745747657475645354531395
n =
14_34299_17169_94565_94175_96370_67138_75678_09312_55074_72733_09678_48556
_39035_24523_56571
Non-witnesses: 279