Finding Large Primes

Gavriel Yarmish Brooklyn College  Joshua Yarmish Pace University
Jason Yarmish NYU Tandon School of Engineering

Keywords: Prime Number Theorem, Digital Root, Fermat primality test, Euler Test, Miller-Rabin test, GNU GMP Library

Abstract: In this paper we present and expand upon procedures for obtaining large \( d \) digit prime number to an arbitrary probability. We use a layered approach. The first step is to limit the pool of random number to exclude numbers that are obviously composite. We first remove any number ending in 1, 3, 7 or 9. We then exclude numbers whose digital root is not 3, 6, or 9. This sharply reduces the probability of the random number being composite. We then use the Prime Number Theorem to find the probability that the selected number \( n \) is prime and use primality tests to increase the probability to an arbitrarily high degree that \( n \) is prime. We apply primality tests including Euler’s test based on Fermat Little theorem and the Miller-Rabin test. We computed these conditional probabilities and implemented it using the GNU GMP library.

1. Introduction

In 1978 Rivest, Shamir and Adleman (RSA) [1] created the RSA cryptosystem. This system plays a significant role in securing our information on the internet. The security of this system is based on the difficulty in factoring large numbers, which are created by multiplying two very large prime numbers. As we will see, although factoring large integers is a very difficult problem, finding large primes is relatively easy. The Prime Number Theorem tells us that if we choose a number \( x \) at random the chance that \( x \) is prime is about \( \sim \frac{1}{\log x} \) i.e. If we pick \( \log x \) numbers at random we expect about 1 to be prime. But how do we know when this \( x \) is prime?

We use a probabilistic approach. We choose a large random number of a particular digit size but exclude numerous classes of numbers that we know are composite. We use the prime number theorem to calculate the probability that a random \( d \)-digit size number is prime. We then show how this probability increases when we exclude classes of composites. The first step is to limit the pool of random number to exclude numbers that are obviously composite; we remove any number ending in 1, 3, 7 or 9. We then exclude numbers whose digital root is not 3, 6, or 9. These steps sharply reduce the probability of the random number being composite. We then apply primality tests to increase the probability to an arbitrarily high degree that \( n \) is
prime. If the test indicates the random number is likely prime we calculate the increased probability. In section 2 we review the Prime Number Theorem and calculate the base probability. We also adjust this probability calculation assuming we exclude numbers ending in 2, 4, 5, 6 or 8. We again adjust the probabilities by excluding numbers with specific digital roots. In section 3 we review the Fermat Primality Test, Euler Test and Miller-Rabin Test. We also calculate exactly how the probability is affected by application of these tests. Finally, in Section 4 we present our application of these tests using C++ and the GNU GMP library.

2. Calculating and increasing probabilities

2.1 Probability a d-digit prime: the Prime Number theorem

The Prime Number Theorem [2](PNT) gives an asymptotic approximation for

\[ \pi(x) = \text{number of prime numbers } \leq x \text{ i.e.} \]

\[ \lim_{x \to \infty} \pi(x) \frac{\ln x}{x} = 1 \text{ or } \lim_{x \to \infty} \frac{\pi(x)}{x} = \frac{x}{\ln x} \]

Thus the odds that a randomly selected number not exceeding x is a prime can be approximated by

\[ \frac{\pi(x)}{x} = \frac{x}{\ln x} \]

So the number of 75 digit primes is

\[ \pi(10^{75}) - \pi(10^{74}) = \text{number of primes } \leq 10^{75} - \text{number of primes } \leq 10^{74} = \text{number of primes in interval } (10^{99}, 10^{100}) \]

Let \( N(x) = \text{number of x digit primes} \).

\( N(75) \) can be approximated by

\[ \frac{10^{75}}{\ln 10^{75}} - \frac{10^{74}}{\ln 10^{74}} = \frac{10^{74}}{\ln 10^{74}} \left( \frac{665}{5550} \right) = 0.052037087 \times 10^{74} \]

In general \( N(k) \sim \frac{10^{k-1}}{\ln 10} \left( \frac{9k-10}{k(k-1)} \right) \)

There are more precise estimates of \( \pi(x) \), one of which is [3]

\[ \frac{x}{\ln x - 1} < \pi(x) < \frac{x}{\ln x - 1.1} \text{ for } x \geq 60184 \]

With this formula we get
.05233970251 \times 10^{74} < \pi(75) < .05237015782 \times 10^{74}

To find the probability that a generated k digit number is actually a prime we divide N(k) by the total number of k digit numbers: $9 \times 10^{k-1}$ thus

$$P(A) = \frac{N(k)}{9 \times 10^{k-1}} = \frac{10^{k-1} (9k - 10)}{9 \times 10^{k-1}} = \frac{9k - 10}{9k(k - 1) \ln 10}$$

Where A is the event that the k digit number selected is a prime.

And for k=75 we get

P(A)=.005781899

2.2 Excluding obvious composites: Increasing the prime probability

If we use k digits which end in 1, 3, 7 or 9, we can increase the probability that the k digit number is prime. (any multi-digit number ending with 2, 4, 5, 6 or 8 cannot be prime). The number of k digit numbers having a 1, 3, 7 or 9 in the last digits is $9 \times 10^{k-2} \times 4 = 36 \times 10^{k-2}$ so the probability now becomes

$$P(A) = \frac{N(k)}{36 \times 10^{k-2}} = \frac{10}{4} \left( \frac{9k - 10}{9k(k - 1) \ln 10} \right)$$

So we increase the probability by a factor $\frac{10}{4} = 2.5$. We now have P(A)=.014454748

2.3 Digital Roots: Further increasing the prime probability

We can further increase the probability of A by avoiding all k digit numbers where digital root are 3, 6 or 9.

Recall [4] that the digital root of a nonnegative integer n (dr(n)) is a single digit obtained by continually summing the digits until a single digit is obtained. dr(n) can be defined using the floor function $\lfloor x \rfloor$ as $dr(n) = n - 9 \left\lfloor \frac{n-1}{9} \right\rfloor$ or in terms of congruences

$$dr(n) = \begin{cases} 
  0 & \text{if } n = 0 \\
  9 & \text{if } n \neq 0, n \equiv 0 \mod n \text{ (n is a multiple of 9)} \\
  n \mod 9 & \text{if } n \neq 0 \mod 9
\end{cases}$$

Thus if
\[
\begin{align*}
\text{dr}(n) &= 3 \Rightarrow n = 9k + 3 \quad \text{for } k = 0,1,2, \ldots \\
\text{dr}(n) &= 6 \Rightarrow n = 9k + 6 \quad \text{for } k = 0,1,2, \ldots \\
\text{dr}(n) &= 9 \Rightarrow n = 9k \quad \text{for } k = 1,2, \ldots 
\end{align*}
\]

So that if \( \text{dr}(n) = 3, 6 \) or 9, \( n \) is divisible by 3 and is composite. If we eliminate all \( n \) whose digital root is 3, 6 or 9 we decrease the \( k \) digit pool that we can choose \( n \) from by 1/3 thus increasing the \( P(A) \) by a factor of 3, thus

\[ P(A) = .043364243 \]

i.e. If we restrict our \( k \) digit number choice to only those that end in 1,3,7 or 9 and whose digital root is not 3,6, or 9 we can expect about 1 prime in about 23 attempts or \( \frac{1}{23} \). But how do we know whether the selected number \( n \) is actually prime? We discuss some primality tests [5] [6] [7] which can determine that a given \( n \) is definitely not a prime but can tell us that \( n \) is a prime with a very high probability i.e. these tests allow for false positives (\( n \) is prime when it is actually not) and no false negatives (\( n \) is not prime when it actually is).

### 3. Primality tests

#### 3.1 Fermat primality test

Fermat’s Little Theorem (FLT): If \( p \) is prime and \( a \) is an integer not divisible by \( p \) then \( a^{p-1} \equiv 1 \mod p \) (and for all \( a \), \( a^{p} \equiv a \mod P \)). By the contrapositive if \( a^{n-1} \not\equiv 1 \mod n \) for some \( a \) (\( a \not\equiv 0 \mod n \)) then \( n \) is composite. Using the contrapositive of FLT we can prove that a number is composite without actually factoring it.

However if \( n \) passes the test i.e. \( a^{n-1} \equiv 1 \mod n \) it is not a proof that \( n \) is prime because the converse of FLT is not necessarily true.

Example 1: \( n = 561 \) \( a = 2 \) and yet \( 2^{560} \equiv 1 \mod 561, \text{But } 561 = 3 \times 11 \times 7 \text{ is composite} \)

Example 2: \( n = 341 \) \( a = 2 \) and yet \( 2^{340} \equiv 1 \mod 561, \text{But } 341 = 11 \times 31 \text{ is composite} \)

Any composite number \( m \) that passes the test is called a “Fermat Pseudoprime to the base \( a \)” [8]. Thus 561 and 341 are both Fermat Pseudoprimes to the base 2. In fact there are many numbers \( n \) that are composite such that \( a^{n-1} \equiv 1 \mod n \) for every \( a \) such that \( \gcd(a,n)=1 \) (i.e. \( a \) and \( n \) are relatively prime). Such numbers are called Carmichael numbers.

FERMAT PRIMALITY TEST: To test if \( n \) is prime or composite
1) Choose a number a so that a is not divisible by n
2) Compute \( a^{n-1} \mod n \)
3) If \( a^{n-1} \equiv 1 \mod n \) claim “n is a probable prime”
   Repeat steps 1, 2 and 3 with a different a. The probability of n being a prime number increases with each iteration
4) If \( a^{n-1} \not\equiv 1 \mod n \) output “n is definitely composite.”

As we noted above Fermat’s test fails for all a when n is a Carmichael number. So what are the chances that a Carmichael number will be randomly chosen to be tested – Not likely

1) There are only 7 Carmichael numbers within the first \( 10^4 \) numbers.
2) There are only 585,355 Carmichael numbers within the first \( 10^{17} \) numbers.

For a randomly chosen odd integer with 100 or more digits the probability that n is a Carmichael is so small that for practical purposes we can consider it to be zero.

Thus, the Fermat test is a good reliable test provided the test number is not a Carmichael number in which case no matter how many times step 3 is repeated the test will conclude that n is a probably prime.

We look for more primality tests that are an improvement over the Fermat Test.

### 3.2 Euler Test

**Some Math Background**

**Fact 1:** If a and b are integers, and a, b > 0 there exist integers s and t such that \( \gcd(a,b) = sa + tb \)
Please see any intro number theory text

**Fact 2:** If a,b,c are integers and a,b,c>0 such that \( \gcd(a,b)=1 \) and a|bc then a|c
i.e. if p is prime and p|bc then p|b or p|c

**Fact 3:** If p is prime and \( x^2 \equiv 1 \mod p \) then \( x \equiv 1 \mod p \) or \( x \equiv -1 \mod p \)
i.e. if \( x^2 \equiv 1 \mod p \) and \( x \not\equiv \pm 1 \mod p \) then p is not prime.

Proof of fact 2: by fact 1 \( \gcd(a,b) =1=sa+tb \) for some s,t. c=csa+ctb \( \Rightarrow a|csa \) and a|cb (same a|bc) \( \Rightarrow a|c \).

Proof of fact 3: \( x^2 \equiv 1 \mod p \) \( \Rightarrow x^2 - 1 \equiv b \mod p \). \( (x+1)(x-1) \equiv 0 \mod p \) Let b=x+1, \( c=x-1 \ bc \equiv 0 \mod p \) \( \Rightarrow p|bc \) and by Fact 2 p|b or p|c. p|(x-1) or p|(x+1) then \( x \equiv 1 \mod p \) or \( x \equiv -1 \mod p \)
Fact 4 from above FTL: If \( p \) is prime and a positive integer \( p \nmid a \) then \( a^{p-1} \equiv 1 \mod p \).

We note that \( a^{\frac{n-1}{2}} \) is the square root of \( a^{n-1} \left( a^{\frac{n-1}{2}} = a^{n-1} \right) \) and if \( a^{n-1} \equiv 1 \mod p \), by fact 3

\[ a^{\frac{n-1}{2}} \equiv \pm 1 \mod n \], and if not then \( n \) is composite.

We have the Euler Primality test:

1) Choose a number \( a \) so that \( a \) is not divisible by \( n \)
2) Compute \( a^{\frac{n-1}{2}} \)
3) If \( a^{\frac{n-1}{2}} \equiv \pm 1 \mod n \) claim “\( n \) is a probable prime.”
   Repeat steps 1, 2 and 3 for several different values of \( a \) - the probability of \( n \) being a prime number increases with each iteration
4) If \( a^{\frac{n-1}{2}} \nmid \pm 1 \mod n \) output “\( n \) is definitely composite.”

We previously saw that Fermat test failed (found \( n \) to be pseudoprime when it was in fact a composite number) for \( n=561 \) and \( n=341 \).

Using Euler’s test:

\[ \left(2^{\frac{560}{2}}\right) = 2^{280} = 1 \mod 561 \]

\[ \left(2^{\frac{340}{2}}\right) = 2^{170} = 1 \mod 341 \] so \( 341 \) is an Euler pseudoprime to base 2

But \( 5^{280} \equiv 67 \mod 561 \nmid \pm 1 \mod 561 \) so \( 561 \) is composite

\( 5^{170} = 56 \mod 341 \nmid \pm 1 \mod 341 \) so \( 341 \) is composite

Note that 561 is not an Euler pseudoprime base 5 but it is a Fermat pseudoprime base 2. Also note, 341 is a Euler pseudoprime base 2 but not base 5.
Note

1) If the Fermat test concludes that \( n \) is composite (i.e. \( a^{n-1} \not\equiv 1 \mod n \)) Euler test also finds that \( n \) is composite (i.e. \( a^{\frac{n-1}{2}} \not\equiv \pm 1 \mod n \)) for if \( a^{\frac{n-1}{2}} \equiv \pm 1 \mod n \) then \( \left(a^{\frac{n-1}{2}}\right)^2 \equiv (\pm 1)^2 \mod n \).

2) If Euler test finds \( n \) to be composite \( (a^{\frac{n-1}{2}} \not\equiv \pm 1 \mod n) \) Fermat test may still fail (mistakenly find \( n \) to be pseudoprime). As an example, as above, 561 is composite by the Euler test using \( a=5 \) but using the Fermat test \( (5^{280})^2 = 67^2 \mod 561 = 1 \mod 561 \). So for \( n=561 \) using \( a=5 \) the Euler test correctly finds \( n \) composite where the Fermat test fails (it finds 561 a probable prime).

Fact 4: If \( n \) is composite it has at least 4 square roots \( 1 \mod n \).

Proof: Consider the simple case when \( n = pq \), \( (p \neq q) \)
\[ x^2 \equiv 1 \mod p \iff x \equiv \pm 1 \mod p \]
\[ x^2 \equiv 1 \mod q \iff x \equiv \pm 1 \mod q \]

We have 4 systems of equations

\[ x \equiv 1 \mod p, \quad x \equiv -1 \mod p, \quad x \equiv 1 \mod p, \quad x \equiv -1 \mod p \]
\[ x \equiv 1 \mod q, \quad x \equiv 1 \mod q, \quad x \equiv -1 \mod q, \quad x \equiv -1 \mod q \]

Each of these can be solved \( \mod pq \) using the Chinese remainder Theorem each yielding the square root of 1. It is clear that if \( n=pq \) we would get more than 4 square roots of 1.

Example: \( n=15=5*3 \)
\[ x \equiv \pm 1 \mod 5 \]
\[ x \equiv \pm 1 \mod 3 \]

So we solve
\[ x \equiv 1 \mod 5 \]
\[ x \equiv 1 \mod 5 \]
\[ x \equiv -1 \mod 5 \]
\[ x \equiv -1 \mod 5 \]
\[ x \equiv 1 \mod 3 \]
\[ x \equiv -1 \mod 3 \]
\[ x \equiv 1 \mod 3 \]
\[ x \equiv -1 \mod 3 \]

\[ x = 1 \]
\[ x = 11 \]
\[ x = -11 \]
\[ x = -1 \]

So square root of 1 in \( \mod 15 \) are 1, -1, 11, -11 hence for \( n \) composite
\[ a^{\frac{n-1}{2}} \equiv k \mod n \text{ where } k \not\equiv \pm 1, \text{ can nonetheless be a square root of 1. i.e. } a^{\frac{(n-1)^2}{2}} \equiv k^2 \mod n \equiv 1 \mod n \]

In this example: \( a^{\frac{n-1}{2}} \equiv 11 \mod 15 \) and \( a^{n-1} \equiv 11^2 \mod 15 \equiv 1 \mod 15 \).
In such a case Fermat test finds \( n \) probable primes since \( a^n - 1 \equiv 1 \mod n \), but Euler test finds \( n \) composite since \( a^{n/2} \not\equiv \pm 1 \mod n \).

Unfortunately there are odd composites such that the Euler test \( a^{n-1} \equiv \pm 1 \mod n \) for every \( a \) with \( \gcd(a,n) = 1 \). These components are called absolute Euler Pseudoprimes (1729 and 2465 are 2 examples). There are far fewer absolute Euler Pseudoprimes than there are Carmichael numbers.

### 3.3 Miller-Rabin test (MRtest)

The Miller-Rabin test [9] uses fact 3 more extensively than in the Euler test (Fact 3 teaches that if the square root of 1 is not \( \pm 1 \mod n \) then \( n \) is composite).

To test \( n \) if prime or composite:

1) Choose \( a \) such that \( 2 < a \leq n - 1 \)
2) Write \( n - 1 = 2^k m \) (\( m \) is odd, \( K \geq 1 \))
3) In \( \mod n \) evaluate \( b_0 = a^m, b_1 = (a^m)^2, b_2 = (a^m)^2, b_3 = (a^m)^2, \ldots b_k = (a^m)^{2^k} = a^{n-1} \)
   
   Note \( b_i = b_{i-1}^2, i = 1,2,\ldots,k \) i.e. \( b_{i-1} \) is square root of \( b_i \)
   
4) Consider the first \( b_j \equiv 1 \mod n \) (if \( b_j \not\equiv 1 \mod n \) for all \( j \) then \( n \) is composite.)
5) If \( b_{j-1} \not\equiv \pm 1 \mod n \) then \( n \) is composite (\( a \) is called a witness); otherwise \( n \) is "probably prime" and is called a strong pseudoprime.

Fact 5: If \( n \) is an odd prime one of the following two conditions must hold

a) \( b_0 \equiv 1 \mod n \) or
b) \( b_i \equiv -1 \mod n \) for some \( i = 0,1,2,\ldots,k \)

Proof: if a) is true then all \( b_i \equiv 1 \mod n \) since \( b_i = b_{i-1}^2, i = 1,2,3,\ldots,k \)

i.e. \( b_k = a^{n-1} \equiv 1 \mod n \) (Fermat Little Theorem)

If b) is true \( b_i \equiv -1 \mod n \) implies \( b_j \equiv 1 \mod n \) \( j = i + 1,2,3,\ldots,k \) again we get

\( b_k = a^{n-1} \equiv 1 \mod n \)

If neither conditions a or b are satisfied the \( n \) is not prime (by contrapositive of Fact 5).

We have the following test: A number \( a \), where \( 2 \leq a \leq n - 2 \) (if \( a=n-1 \) then condition b is satisfied \( (n-1)^m \equiv -1 \) since \( m \) is odd) is a witness – the test indicates that \( n \) is composite- if:

\[ b_0 = a^m \not\equiv \pm 1 \mod n \] and
\[ b_i \not\equiv -1 \mod n \] for all \( i = 0,1,2,\ldots,k \)
If \( n \) is composite, then any \( a, 1 \leq a \leq n - 1 \), not a witness is called a \textbf{Liar} (i.e. test indicates \( n \) is prime using that \( a \)). Note that \( a=1 \) and \( a=n-1 \) are trivial liars. The \( n \) associated with liar \( a \) is called a strong pseudoprime base \( a \).

The probability is less than \( \frac{1}{4} \) that test gives wrong answers where \( n \) is composite, \([10]\) and if \( n \) is composite the probability that the test will indicate \( n \) is prime for each of \( m \) different \( a \) (denoted by \( T^mP \)) is less than \( \left( \frac{1}{4} \right)^m \) i.e. \( P(\text{test gives a false positive}) = P(T^mP|c) \leq \frac{1}{4} \) and \( P(\text{test failed to detect a single witness in m attempts}) = P(T^mP|c) \leq \left( \frac{1}{4} \right)^m \)

We want to find the reliability of the results i.e. if test indicates prime what is the chance that \( n \) is indeed prime. We use Bayes theorem:

\[
P(p|T^mP) = \frac{P(p)P(T^mP|p)}{P(p)P(T^mP|p) + P(c)P(T^mP|p)}
\]

Where \( P(p) \) is the probability that the selected \( k \) digit number is prime.

\( P(c) = 1 - P(p) \)

\[
P(T^mP|p) = 1
\]

\[
P(T^mP|c) \leq \left( \frac{1}{4} \right)^m
\]

So, probability \( P(p|T^mP) \) that the selected \( n \), which goes through the test \( m \) times (each with a different \( a \)) and whose test indicates \( n \) is prime each time, is indeed prime is

\[
P(p|T^mP) = \frac{P(p)(1)}{P(p)(1) + P(c)P(T^mP|c)} \geq \frac{P(p)(1)}{P(p) + P(c) \left( \frac{1}{4} \right)^m}
\]

\[
> \frac{1}{P(c) \left( \frac{1}{4} \right)^m} > 1 - \frac{P(c) \left( \frac{1}{4} \right)^m}{P(p)} =
\]

Recall \( P(\text{k digit selected number is prime}) = P(p) = \frac{9k-10}{k(k-1)ln10} \)

So \( P(\text{k digit selected number is composite}) = P(c) = 1 - P(p) \)

As an example For \( k=75 \): \( P(p) = 0.043364243; P(c) = 0.956635757 \quad \frac{P(c)}{P(p)} = 22.66047407 \), and \( 4 \) iterations \( m=4 \).
We have \( P(p|T^mP) \geq 1 - \frac{22.66047407}{4^m} = 1 - .088517477 = .911482523 \)

We get a better than 91\% reliability for just 4 repetitions. Has we used the selection process without restricting the pool of k digit numbers we would have

\[
P(p) = \frac{N(75)}{9*10^{74}} = .005781899 \quad P(c) = .994218101 \quad \frac{P(c)}{P(p)} = \frac{.994218101}{.005781899} = 171.9535573
\]

\[
P(p|T^mP) > 1 - \frac{P(c)}{P(p)4^m} = 1 - \frac{171.9535573}{4^m} = 1 - .671692583 = .328306417
\]

Thus using the test for 4 iterations without pre-restricting the pool of random k digit numbers to exclude obvious composite numbers gives us a 32\% confidence that the number selected is prime. When we pre-restrict the pool we obtain a 91\% confidence that the number is indeed prime.

In either case we can increase other confidence level by performing more iterations of the test.

In summary, if we analyze the

\[
P(p|T^mP) > 1 - \frac{P(c)}{P(p)4^m} = 1 - A \quad \text{where } A = \frac{P(c)}{P(p)4^m}.
\]

Because our confidence is 1-A, the smaller A the more confident we are that indeed n is prime. There are 2 ways to decrease A: 1) increase P(p) 2) increase m. Both methods can be utilized simultaneously.

4. Experimental Results

We implemented this method in C++ using the GNU GMP library for arbitrarily large numbers. We generated 100 random 75-digit numbers, note that we could have used arbitrarily large numbers but this would have made it unwieldy to present in figure 1.

As specified in the method above, the random number generator only generated numbers whose last digit ended with a 1, 3, 7 or 9 since all other are certainly composite numbers. The random number generator also excluded all numbers whose digital root was 3, 6 or 9 as these too, are obviously composite.

We then implemented the Rabin-Miller test to determine for each generated random number n if it is composite or probably prime. For each 75-digit random number we looped \( m = 10 \) times. Each time we randomly chose a value \( a \) of the primality test. If a particular \( a \) was a ‘witness’ then the 75-digit number is composite and the loop ended. If it was not a witness then the probability of the number being prime rose.

In this experiment, the calculation of the probability is the same as calculated in the last section except that \( m \) is 10 instead of 4.
We have $P(p | T^n P) \geq 1 - \frac{22.66047407}{410} = 1 - .000026 = .999978$. This means that a number that lasted through the full loop of 10 is more than 99.99% likely to be prime.

In Figure 1 below we list all the 100 generated numbers in column 1 together with the output from our program in column 2.

There were 5 primes out of the 100 numbers. We manually checked each of the 100 numbers utilizing an online Prime number checker [11]. As would be expected from the probability, they were all correct.

5. References

[1] R. L. A. S. a. L. A. Rivest, "A method for obtaining digital signatures and public-key cryptosystems," *Communications of the ACM*, vol. 21, no. 2, pp. 120-126, 1978.

[2] I. H. S. Z. a. H. L. M. Niven, An introduction to the theory of numbers, John Wiley & Sons, 1980.

[3] P. Dusart, "Estimates of some functions over primes without RH," *arXiv preprint arXiv:1002.0442*, 2010.

[4] 2017. [Online]. Available: https://en.wikipedia.org/wiki/Digital_root. [Accessed 14 8 2017].

[5] G. L. Miller, "Riemann's Hypothesis and Tests for Primality," *Journal of Computer and System Sciences*, vol. 13, no. 3, pp. 300-317. doi:10.1145/800116.803773, 1976.

[6] R. Schoof, "Four primality testing algorithms," in *Algorithmic Number Theory: Lattices, Number Fields, Curves and Cryptography (PDF)*, Cambridge University Press ISBN 0-521-80854-5, 2004.

[7] V. e. a. Kochar, "Contrast various tests for primality," in *Accessibility to Digital World (ICADW) 2016 International Conference on. IEEE*, 2016.

[8] C. Pomerance, J. L. Selfridge and S. S. Wagstaff, "The pseudoprimes to $25 \cdot 10^9$," *Mathematics of Computation*, vol. 35, no. 151, pp. 1003-1026, 1980.

[9] M. O. Rabin, "Probabilistic algorithm for testing primality," *Journal of Number Theory*, vol. 12, no. 1, pp. 128-138, 1980.

[10] L. Monier, "Evaluation and comparison of two efficient probabilistic primality testing algorithms," *Theoretical Computer Science*, vol. 12, no. 1, pp. 97-108, 1980.

[11] "Prime Numbers Generator and Checker," [Online]. Available: http://www.numberempire.com/primenumbers.php. [Accessed 2017].
Random numbers ending in 1, 3, 7 or 9 not having a prime root of 3, 6 or 9

P/C

3165145730262073866331017499340036779797286806917452739134275993863501047889
COMPOSITE

29765064277966142352322644977410307005313534682136555013446701896830945338
COMPOSITE

616933869592967029766709641562418345634452441553247912915732178012012016973
COMPOSITE

90985419481411427960257734803333343568243704540055037717004912759454299093
COMPOSITE

22872834804058843832266162953786978566808345970316174869560479537957230329
COMPOSITE

649891629917275630589349261358251848153161602502383001606035790937327956047979
COMPOSITE

7983899401325653265219748981058846568672605551061526148465749930541732415749
COMPOSITE

734662394520977216042497925591675020898069885642162306184570257367970015511
COMPOSITE

792694675381351078160481984960451150424297041420789331637494005020909796811
COMPOSITE

632921800854443523500411885211851112782675524097438828268406137299652681
COMPOSITE

5307703925071843814246227827488097865039328737459802697528729991225701
COMPOSITE

2288141800551894023770611669351526247229714149529834485997456091735774727439
COMPOSITE

4294377797145193648808986047114463005379612249686873002425166264722440710061
COMPOSITE

85360935230830285442723420412454192480593957002214364091978127221538549877609
COMPOSITE

35899788185633894542093246646249258604711218857421145396838278238152446777
COMPOSITE

126389462465110759662708780283110561867994110577842039554728995309699176339
COMPOSITE

97103737002237171213411546294727396174057464395771668225514135488071112969627
COMPOSITE

424708857617746277757303329797575509320111385857115529729302009283039265409
COMPOSITE

162177375645940334378000907481719944137909233317330576002923422187171952093
COMPOSITE

444278265659568442316126384053017942116384246463868244045209365025354268009
COMPOSITE

6639708963138376503864666949925219838397152102551115367798485679737137
COMPOSITE

45686377934141781638088062079392551506809499767256797288728921979093824189413
COMPOSITE

122091240881817724623600051159864204314781149741386142963325660049582559
COMPOSITE

624189746335896102695722623620310278566565350634992725047531450774129352961
COMPOSITE

7712817058408890195271771162951679819240088749786114578289798185713076803
COMPOSITE

8976565954700505589104879145237940681230583428438489584934035074387747207249
COMPOSITE

81396044982767749665528591932528893884081989431312871511986523273664170191
COMPOSITE

58145777418980746279759934216433104040964364353874296260015472291501914129
COMPOSITE

708033709986264201987560748400967824718850083588985391917141612036502904809
COMPOSITE

5198850812887543278778041025398656508773239381343894001759650917864307453
COMPOSITE

343672436467540021020025366449544858400458442164123760357928289158425110923
COMPOSITE

195318212747829324819772335819569487800196229591686827995677405378063653
COMPOSITE

36709502863477870127515999124760242093219512808984993872542534812981146959
COMPOSITE

234773451375480040220334287669288301883344287909669541215658882406949153601
COMPOSITE

820776440483898738020755240477469059172556019483226067183191530572248725487
COMPOSITE

1731783604201757419227068060911433755591686706889835735397499274527456941
COMPOSITE
Figure 1: 100 75-digit random numbers labeled whether they are prime or composite

56987603704820585710173924183063843680721382061262556345628090001572699947 COMPOSITE
977107084071477189293704278613232264403584591133499920044751704893231936463 COMPOSITE
6793155851233454964460836972813396232326550724527262185260118469592705007 COMPOSITE
9331253249091269204318446140934607137704624272156225472853582324058425027 COMPOSITE
965229968255818197619948058469725477602160813673368970975272160032015649031 COMPOSITE
858542030825079594829661820038976573273390740452998345407830062790692449747 COMPOSITE
321279061857594270472380594849921324045717746083616240909682967183698020513 COMPOSITE
23664113770319763440424991339078429735923780690751353141185310980673510991 COMPOSITE
533165600339804012311571604245660003767767556755599502252896524658865752217 COMPOSITE
73256936138674977168897622791519514181641753250066595610757522742657865983 COMPOSITE
795427619760864700069797568013984567474777365311527984128398681881223645973 COMPOSITE
5639523353800353799120109193075528000135437674188830000585986747409031013703 PRIME
6478185395776797945653177374281026045992308978865820617589117024170512331 COMPOSITE
390401201810491630562663741867686158210481604862027789019034578889017406527 COMPOSITE
7334240329145700805669357365703343182792992633370756797068964931871382996361 COMPOSITE
21969823996102394110824254512655034618396395829783400460815104116018281651 COMPOSITE
87446536128690082616895690953063174845040354416579211732236350022372120191 COMPOSITE
5742632855779390292734469045058241003577278225607947522871270374798271731527 COMPOSITE
337378475285907785332816956280622555263570773284065327930232439542520335553 COMPOSITE
923858854417266802249920620513613034217951635456501784026184652148649095851 COMPOSITE
1203143230559381806304428143041989366450150897929076775514496338385456900881 COMPOSITE