Accepted for Publication: Utilitas Mathematica

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, RSA Public Key Encryption

Abstract: In this paper we present and expand upon procedures for obtaining a large *k*-digit prime number to an arbitrarily high probability. We use a layered approach. The first step is to limit the pool of random numbers to exclude numbers that are obviously composite. We remove numbers not ending in 1, 3, 7, or 9, then exclude numbers with a digital root of 3, 6, or 9. This sharply increases the probability of the random number being prime. We then use the prime number theorem to find the probability that a selected number *n* is prime and use the Miller-Rabin test to increase the probability that *n* is prime to an arbitrarily high degree. Conditional probabilities are computed and confirmed experimentally using the GNU GMP library.

1. Introduction

In 1978 Rivest, Shamir and Adleman (RSA) [1] created the RSA cryptosystem which plays a significant role in securing information on the Internet. The security provided by this system is based on the difficulty inherent in factoring large numbers that are the result of multiplying two very large prime numbers. As we will demonstrate, although factoring large integers is a very difficult problem, finding large primes is relatively less difficult. From the prime number theorem we know that for a number *n* chosen at random not exceeding *x* the probability that *n* is prime is about $\frac{1}{\ln x}$. Thus for $\ln x$ numbers chosen at random we expect about one to be prime. But how do we know when a given number *n* is prime?

We use a probabilistic approach. We choose a large random number of a particular digit size *k* but exclude classes of numbers that we know to be composite. The prime number theorem can estimate the prior probability that this random *k*-digit number is prime. We then show how the posterior probability increases when particular classes of composites are excluded. We first limit the pool to exclude numbers not ending with 1, 3, 7, or 9, then we exclude numbers with a digital root of 3, 6, or 9. These steps sharply increase the probability of the random number being prime. We then apply the Miller-Rabin test to increase the probability that *n* is prime to an arbitrarily high degree. If the test indicates that the resulting number is a probable prime, we calculate the increased probability.
In Section 2 we review the prime number theorem and calculate the base probability, then adjust this calculation assuming exclusion of obviously composite numbers. In Section 3 we review the Miller-Rabin test. In Section 4 we describe our new results for estimating the asymptotic probability of primality. In Section 5 we implement our method using C++ and the GNU GMP library.

2. Calculating and Increasing the Probability of Primality

2.1 Probability of Finding a *k*-digit Prime Using the Prime Number Theorem

The prime number theorem [2] gives an asymptotic approximation for $\pi(x) =$ the number of primes $\leq x$, i.e.,

$$\lim_{x\to\infty} \pi(x)\frac{\ln x}{x} = 1 \quad \text{or} \quad \lim_{x\to\infty} \pi(x) = \frac{x}{\ln x}. \tag{1}$$

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

$$\frac{\pi(x)}{x} \sim \frac{(x/\ln x)}{x} = \frac{1}{\ln x} \tag{2}$$

as $x \to \infty$. It follows from here that the number of k-digit primes is the number of primes in the interval $(10^k, 10^{k-1})$ and it is given by $\pi(10^k) - \pi(10^{k-1})$.

For example, the number of 75-digit primes is the number of primes in interval $(10^{74}, 10^{75})$ and it is given by

$$\pi(10^{75}) - \pi(10^{74}) \approx \frac{10^{75}}{\ln 10^{75}} - \frac{10^{74}}{\ln 10^{74}} = 5.2037087 \times 10^{72}.$$

2.2 Our Estimate for the Number of *k*-digit Primes and the probability of a *k*-digit Prime

We now use the prime number theorem in order to approximate the number of k-digit primes and the probability of picking a k-digit prime.

Theorem 1: Let $\mathrm{N}(k)$ be the number of k-digit primes, then

$$\mathrm{N}(k) \sim \frac{10^{k-1}}{\ln 10}\left(\frac{9k-10}{k(k-1)}\right).$$

Let p be the event that a selected k-digit number is prime, then the corresponding probability $\mathrm{P}(p)$ is given by

$$\mathrm{P}(p) \sim \frac{9k-10}{9k(k-1)\ln 10}$$

Proof:

$$\begin{aligned}
\mathrm{N}(k) &= \pi(10^{\mathrm{k}}) - \pi(10^{\mathrm{k}-1}) \\
&\sim \frac{10^k}{\ln 10^k} - \frac{10^{k-1}}{\ln 10^{k-1}} \\
&= \frac{10^k}{k\ln 10} - \frac{10^{k-1}}{(k-1)\ln 10} \\
&= \frac{10^{k-1}}{\ln 10}\left(\frac{10}{k} - \frac{1}{k-1}\right) \\
&= \frac{10^{k-1}}{\ln 10}\left(\frac{10(k-1)-k}{k(k-1)}\right) \\
&= \frac{10^{k-1}}{\ln 10}\left(\frac{9k-10}{k(k-1)}\right)
\end{aligned}$$

Now dividing $\mathrm{N}(k)$ by $9 \times 10^{k-1}$ and simplifying yields the probability. ■

For example, for k=75 we get $\mathrm{N}(k) \approx 5.2037087 \times 10^{72}$ and $\mathrm{P}(p) \approx 0.005782$ using our theorem.

There are more precise estimates of $\pi(x)$ [3]. One such estimate is

$$\frac{x}{\ln x - 1} < \pi(x) < \frac{x}{\ln x - 1.1}.$$

The following estimate is even more precise:

$$\mathrm{Li}(x) = \int_2^x \frac{1}{\ln t}\,dt.$$

Its expansion is

$$\mathrm{Li}(x) = \frac{x}{\ln x}\sum_{k=0}^{\infty} \frac{k!}{(\ln x)^k} = \frac{x}{\ln x} + \frac{x}{(\ln x)^2} + \frac{2x}{(\ln x)^3} + \cdots.$$

Note that the prime number theorem uses the first term of this expansion.

Any estimate of $\pi(x)$ would work for our analysis. We will use the results in Theorem 1 derived from the prime number theorem in subsequent calculations.

2.3 Increasing the Probability of Primality by Excluding Obvious Composites

If we restrict the k-digit numbers to those ending in 1, 3, 7, or 9, we increase the probability of primality. The number of k-digit numbers ending in 1, 3, 7, or 9 is $9 \times 10^{k-2} \times 4 = 36 \times 10^{k-2}$. For a k-digit number there are nine choices for the first digit, ten choices for each intermediate digit and four choices for the last digit, namely: 1, 3, 7, or 9.

If we restrict the k-digit numbers to those ending in 1, 3, 7, or 9, we decrease the k-digit pool from which we can choose n by 6/10 so that 4/10 of the original pool remains. This increases P(p) by a factor of $\frac{10}{4}$. In general, if the original probability is $\frac{a}{b}$ then after reducing the pool the new probability is

$$\frac{a}{(4/10)b} = \frac{10}{4}\left(\frac{a}{b}\right) = \frac{5}{2}\left(\frac{a}{b}\right). \tag{3}$$

The updated probability of primality is now

$$\left(\frac{5}{2}\right)\frac{9k - 10}{9k(k-1)\ln 10}. \tag{4}$$

In our example, the probability is increased by a factor of $\frac{5}{2} = 2.5$ and now the probability of a k-digit number being a prime is 0.014455.

2.4 Further Increasing the Probability of Primality Using Digital Roots

We can further increase the probability that a k-digit number is prime by avoiding k-digit numbers with a digital root of 3, 6, or 9.

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. The digital root of n, dr(n), can be defined using the floor function $\lfloor x \rfloor$ as $\mathrm{dr}(n) = n - 9\left\lfloor \frac{n-1}{9} \right\rfloor$, or in terms of congruences

$$\mathrm{dr}(n) = \begin{cases} 0 & \text{if } n = 0 \\ 9 & \text{if } n \neq 0, n \equiv 0 \bmod 9 \ (n \text{ is a multiple of } 9) \\ n \bmod 9 & \text{if } n \not\equiv 0 \bmod 9 \end{cases}$$

Thus

$$\begin{aligned} \mathrm{dr}(n) = 3 &\Longrightarrow n = 9k + 3 \quad \text{for } k = 0,1,2,\dots \\ \mathrm{dr}(n) = 6 &\Longrightarrow n = 9k + 6 \quad \text{for } k = 0,1,2,\dots \\ \mathrm{dr}(n) = 9 &\Longrightarrow n = 9k \qquad\quad \text{for } k = \quad 1,2,\dots \end{aligned}$$

so that if dr(n)= 3, 6, or 9, n is divisible by 3 and is composite [3].

If we eliminate every n whose digital root is 3, 6 or 9 we decrease the k-digit pool from which we can choose n by 1/3 so that 2/3 of the original pool remains. This increases P(p) by a factor of $\frac{3}{2}$. In general, if the original probability is $\frac{a}{b}$ then after reducing the pool the new probability is

$$\frac{a}{(2/3)b} = \frac{3}{2}\left(\frac{a}{b}\right). \tag{5}$$

Theorem 2: Suppose the pool of k-digit numbers is restricted to those numbers which end in 1, 3, 7, or 9 and not divisible by 3, then the new restricted probability, denoted by $\mathrm{P_R}(p)$, is given by

$$\mathrm{P}_R(p) = 3.75\ \mathrm{P}(p).$$

Proof:

From Theorem 1, (3), and (5), we obtain

$$\mathrm{P}_R(p) = \frac{3}{2}\cdot\frac{5}{2}\left(\frac{9k-10}{9k(k-1)\ln 10}\right) = \frac{15}{4}\left(\frac{9k-10}{9k(k-1)\ln 10}\right) = 3.75\ \mathrm{P}(p)\ \blacksquare$$

For example, for k=75, $\mathrm{P}_R(p) \approx 0.021682 \approx \frac{1}{46}$.

Thus restricting our choice of k-digit numbers as described, we expect one prime in about 46 attempts.

Performing these two steps in succession is actually equivalent to excluding multiples of 2, 3, and 5.

3. A Review of the Miller-Rabin Primality Test

How does one know whether the selected number *n* is actually prime? We review the Miller-Rabin primality test which determines whether a given *n* is definitely not a prime and can additionally inform us that *n* is a prime with a very high probability. These tests allow false positives (*n* tests as prime when it is actually not) and no false negatives (*n* tests as not prime when it actually is).

It is important to note that the Miller-Rabin test is an expansion upon both the Fermat test, which is based upon Fermat's little theorem, and the Euler test which expanded upon the Fermat test. The reader is referred to the references [4], [5], [6], [7], [8], and [9] for a more extensive background on these important results.

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

Thus to test a number if a number *n* is composite we pick a whole number *a* that is not divisible by *p* and calculate a^{n-1}. If $a^{n-1} \not\equiv 1 \bmod n$ then *n* is composite. This is called the Fermat test.

It is also true that if *n* is prime and $a^{n-1} \equiv 1$ then $\sqrt{a^{n-1}} = a^{(n-1)/2} \equiv \pm 1$. Therefore we can also test if $a^{(n-1)/2} \not\equiv \pm 1$, in which case *n* is composite. This is called the Euler test.

The Miller-Rabin test extends this principle further. Since *n* is an odd prime *n*-1 is an even number. We make a list: $a^{n-1}, a^{(n-1)/2}, a^{(n-1)/4}, \ldots, a^{(n-1)/2^s}$, where the exponent is divided by 2 until $(n-1)/2^s$ is odd.

Using the same principle, we note that for any element in that list that is congruent to 1 mod *n*, the next element, its square root, must be congruent to either 1 or -1.

Now we can check to make sure we have two such numbers in succession somewhere in that list, by traversing the list in reverse order. As soon as we encounter a 1 we then check the number before it and if it is not a 1 or -1 then we conclude that the number is composite. If we do have a 1 or -1 then the number is referred to as a "probable prime."

In our implementation, we cycle through the Miller-Rabin test choosing a new value of *a* each time. If the test claims that we have a composite we stop since it is a definite composite. If the test claims that it is a probable prime, the probability of primality increases and we can perform another cycle to further increase the probability.

These are the steps that we use in detail to test whether *n* is prime or composite:

1. Choose *a* such that $2 \leq a \leq n-1$.
2. Write $n - 1 = 2^s d$ where $s \geq 1$ is chosen such that *d* will be odd.
3. In mod *n*, evaluate $b_0 = a^d, b_1 = \left(a^d\right)^2, b_2 = \left(a^d\right)^{2^2}$,
   $b_3 = \left(a^d\right)^{2^3}, \ldots, b_s = \left(a^d\right)^{2^s} = a^{n-1}$.
   Note: $b_i = b_{i-1}^2$ for $i = 1,2, \ldots, s$,
   i.e., b_{i-1} is the square root of b_i.
4. Consider the first value of b_i such that $b_i \equiv 1 \bmod n$. Note: if $b_i \not\equiv 1 \bmod n$ for all *i* then *n* is composite.
5. If $b_{i-1} \not\equiv \pm 1 \bmod n$ then *n* is composite, otherwise *n* is a "probable prime" and is called a strong pseudoprime.

4. Our Main Result

Let c denote the event that n is actually composite. Let p denote the event that n is actually a prime. P(c) = 1–P(p) is the probability that the selected k-digit number is composite. A false positive result is a test that indicates n to be prime when it is in fact composite.

If n is composite, the probability that the test yields a false positive is less than or equal to $\frac{1}{4}$ (see [10]). Symbolically,

$$\mathrm{P}(\mathrm{T}p|c) \leq \frac{1}{4}$$

where Tp is the event that n tests prime using a single value of a. Similarly, the probability that the test yields a false positive for each of m different independent values of a is less than or equal to $\left(\frac{1}{4}\right)^m$. Symbolically,

$$\mathrm{P}(\mathrm{T}^{\mathrm{m}}\mathrm{p}|\mathrm{c}) \leq \left(\frac{1}{4}\right)^{\mathrm{m}}$$

where $\mathrm{T}^m p$ is the event that n tests prime using each of m different values of a. Note that Tp =$\mathrm{T}^1 p$.

If we apply the Miller-Rabin test to a prime it will certainly indicate that it is prime, i.e., $\mathrm{P}(T^m p|p) = 1$. On the other hand, if the test is applied to a composite, the probability is

$$\mathrm{P}(\mathrm{T}^{\mathrm{m}}\mathrm{p}|\mathrm{c}) \leq \left(\frac{1}{4}\right)^{\mathrm{m}}.$$

We wish to find the reliability of the results. Given that the test indicates that n is prime, what is the probability that it is indeed prime? Our next theorem uses Bayes' theorem to estimate $\mathrm{P}(T^m p|p)$ and thereby answer this question.

Theorem 3:

For the case of selection from an unrestricted pool:

$$\mathrm{P}(p|\mathrm{T}^m p) \geq \frac{1}{1+\frac{1/\mathrm{P}(p)-1}{4^m}} \text{ where } \mathrm{P}(p) \sim \frac{9k-10}{9k(k-1)\ln 10}.$$

For the case of selection from a restricted pool:

$$\mathrm{P}_R(p|\mathrm{T}^m p) \geq \frac{1}{1+\frac{1/\mathrm{P}_\mathrm{R}(p)-1}{4^m}} \text{ where } \mathrm{P}_\mathrm{R}(p) = 3.75\ \mathrm{P}(p).$$

Proof: $\mathrm{P}(p|T^m p)$ denotes the conditional probability that the selected *n* is indeed prime after *m* cycles of the Miller-Rabin test. We begin with Bayes' theorem:

$$\begin{aligned}
\mathrm{P}(p|\mathrm{T}^m p) &= \frac{\mathrm{P}(p)\mathrm{P}(T^m p|p)}{\mathrm{P}(p)\mathrm{P}(T^m p|p)+\mathrm{P}(c)\mathrm{P}(T^m p|c)} \\
&= \frac{\mathrm{P}(p)(1)}{\mathrm{P}(p)(1)+\mathrm{P}(c)\mathrm{P}(T^m p|c)} \\
&\geq \frac{\mathrm{P}(p)}{\mathrm{P}(p)+\mathrm{P}(c)\left(\frac{1}{4}\right)^m} \\
&= \frac{1}{1+\frac{\mathrm{P}(c)/\mathrm{P}(p)}{4^m}}.
\end{aligned}$$

Recall that if we restrict our *k*-digit number to those with last digit 1, 3, 7, or 9 and avoid multiples of 3, then from Theorem 2

$$\mathrm{P}_R(p) = 3.75\ \mathrm{P}(p).$$

Note that:

$$\frac{\mathrm{P}(c)}{\mathrm{P}(p)} = \frac{1-\mathrm{P}(p)}{\mathrm{P}(p)} = \frac{1}{\mathrm{P}(p)} - 1.$$

Similarly we have:

$$\frac{P_R(c)}{\mathrm{P}_R(p)} = \frac{1}{\mathrm{P}_R(p)} - 1.$$

Upon substitution we obtain the formulas of our theorem. ■

As an example, if we use the selection process without restricting the pool of *k*-digit numbers, for *k*=75 using four iterations (*m*=4) our theorem gives:

$$\mathrm{P}(p) = 0.005782$$

and

$$\mathrm{P}(p|\mathrm{T}^m p) \geq \frac{1}{1+\frac{1/\mathrm{P}(p)-1}{4^m}}$$

$$= 1 + \cfrac{1}{\cfrac{171.953557}{256}}$$

$$= 0.598196\,. \tag{6}$$

Therefore, four iterations on an unrestricted pool results in a 59.8% probability or confidence of primality.

If we restrict our pool, we use the second part of Theorem 3 to get:

$$\mathrm{P}_R(p) = 3.75\ \mathrm{P}(p) = 0.021682$$

and

$$\begin{aligned} \mathrm{P}_R(p|\mathrm{T}^m p) &\geq \cfrac{1}{1 + \cfrac{1/\mathrm{P_R}(p) - 1}{4^m}} \\ &= 1 + \cfrac{1}{\cfrac{45.120953}{256}} \\ &= 0.850157. \end{aligned} \tag{7}$$

Now, we get better than 85.0% probability after just four iterations.

Next we measure the increase in probability, also referred to here as confidence.

The increase in confidence is given by

$$\mathrm{P}_R(p|\mathrm{T}^m p) - \mathrm{P}(p|\mathrm{T}^m p) \tag{8}$$

and the relative increase in confidence is given by

$$\frac{\mathrm{P}_R(p|\mathrm{T}^m p) - \mathrm{P}(p|\mathrm{T}^m p)}{\mathrm{P}(p|\mathrm{T}^m p)}\,. \tag{9}$$

For example, for *k*=75 and *m*=4:

$$\mathrm{P}_R(p|\mathrm{T}^m p) - \mathrm{P}(p|\mathrm{T}^m p) \quad = 0.850157 - 0.598196 = 0.251961$$

and

$$\frac{\mathrm{P}_R(p|\mathrm{T}^m p) - \mathrm{P}(p|\mathrm{T}^m p)}{\mathrm{P}(p|\mathrm{T}^m p)} \quad = \frac{0.251961}{0.598196} = 0.421202.$$

Thus restricting the pool increases our probability by about 25.2% (compare (6) and (7)), which is an increase by a factor of about .42.

To summarize, we have used two ways to increase the probability of primality in succession.

(a) $P(p) \rightarrow P_R(p)$: We restrict the pool of random numbers to exclude obvious composites.

(b) $P_R(p) \rightarrow P_R(p|T^m p)$: We perform *m* iterations of the Miller Rabin test, where larger *m* results in increased probability of primality.

5. Experimental Results

We implemented our method using C++ and the GNU GMP library for arbitrarily large numbers, generating one-hundred random 75-digit numbers.

As described, we instructed the random number generator to restrict the pool to only numbers with a last digit of 1, 3, 7, or 9 and to additionally exclude all numbers with a digital root of 3, 6, or 9 as the latter are obviously composite numbers.

According to the prime number theorem a 75-digit number approaches 0.58% probability of primality. If we first limit the random numbers to our restricted pool, the asymptotic probability now becomes 2.17% (See Theorem 2 for *k*=75). In our example there were three primes found among the one-hundred randomly-generated numbers, so the actual empirical probability is 3%. The close agreement between these two probabilities corroborates our results.

We then implemented the Miller-Rabin test to determine for each generated *n* whether it is composite or a probable prime. For each 75-digit number we looped *m*=10 times, each time randomly choosing a value *a* for the primality test. If a particular *a* was found to be a witness then the 75-digit number was proved composite and the loop ended. If *a* was not a witness then the new conditional probability of the number being prime increased and we looped again.

In this experiment, the methodology used for calculation of the probability was the same as that of the last section, except we used *m*=10 instead of *m*=4.

We now have $P_R(p|T^m p) \geq \frac{1}{1+\frac{45.1209531}{4^{10}}} = 0.999957$. This means that a number that lasted through ten iterations is more than 99.9% likely to be prime.

The appendix lists the one-hundred generated numbers in the first column and their associated program output in the second column.

We manually checked each of the one-hundred numbers utilizing an online prime number checker [11]. As would be expected from the 99.9% probability, all results were correctly identified by the Miller-Rabin test as prime.

6. Conclusion

Identification of arbitrarily large primes is critical to Internet security methodologies as provided in public key cryptosystems. We use a probabilistic approach to finding these arbitrarily large primes.

We derived an asymptotic estimate for the number of *k*-digit primes, namely:

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

The corresponding asymptotic probability that a selected *k*-digit number is prime is

$$P(p) \sim \frac{9k-10}{9k(k-1)\ln 10}.$$

For any k-digit number chosen at random, applying the Miller-Rabin primality test, the probability that after m passes the number is indeed prime is estimated by:

$$\mathrm{P}(p|\mathrm{T}^m p) \geq \frac{1}{1+\frac{1/\mathrm{P}(p)-1}{4^m}} \text{ where } \mathrm{P}(p) \sim \frac{9k-10}{9k(k-1)\ln 10}.$$

However, if one restricts the pool of random k-digit numbers to exclude multiples of 2, 3, and 5, the probability that the selected number is indeed prime increases. The formula for the increase is:

$$\mathrm{P}_R(p) = 3.75\ \mathrm{P}(p).$$

We then estimate the increased probability of primality using

$$\mathrm{P}_R(p|\mathrm{T}^m p) \geq \frac{1}{1+\frac{1/\mathrm{P}_\mathrm{R}(p)-1}{4^m}}.$$

Theoretical results are substantiated using one hundred random numbers for k=75, using C++ and the GNU GMP library for arbitrarily large (75-digit) numbers. Experimental results confirm our asymptotic probability estimates.

7. References

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

[2] I. Niven, H. S. Zuckerman and H. L. Montgomery, An introduction to the theory of numbers, John Wiley & Sons, 1980.

[3] "Digital Root," [Online]. Available: https://en.wikipedia.org/wiki/Digital_root. [Accessed 2017].

[4] 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.

[5] 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.

[6] V. Kochar, D. P. Goswami, M. Agarwal and S. Nandi, "Contrast various tests for primality," in *Accessibility to Digital World (ICADW) 2016 International Conference on. IEEE,* 2016.

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

[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] K. Rosen, Elementary Number Theory, 6 ed., Addison Wesley, 2011.

[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].

Appendix: The Output of Our Program

This is the output of our program labeling one-hundred randomly generated 75-digit numbers as either prime or composite.

Random numbers ending in 1, 3, 7 or 9 not having a digital root of 3, 6 or 9	P/C
463275858019879249574056168859818805682547221425653953171238312251525950279	COMPOSITE
320993429997565812077243872011200796965196435102163246819153542371553324287	COMPOSITE
563492914442674876775601937883819855289709847701017440205206719692701455703	PRIME
333532597907151620007442636650408511298049820009384726844244252479251889113	COMPOSITE
925687429488062887205037569696066691687236670524165467615753868161610888323	COMPOSITE
261802749418585625555398860418051466234564626790035809081087044969658926743	COMPOSITE
269044233961641329011201715457808694341315392285353433098810008419246739517	COMPOSITE
518307139152866062883752946752540000531197311598385289597311524149187986287	COMPOSITE
230964718209932946020660456458887084579626329956329569973520958876063645841	COMPOSITE
6894564096634361714260244885222151115569665264111701119946278313347526847063	COMPOSITE
711740558493539399832317415878355247159515932215502440586188921378965832769	COMPOSITE
475292172239624476257786524988734271007420976422662324336214150984131370789	COMPOSITE
321370100374685699642340341499398092430719030229040171067446136530027876913	COMPOSITE
781108222499550690156257118313591271945747926978079719473425780827335911617	COMPOSITE
873499445720212726493978219107825318856966864972965153898871053485704821741	COMPOSITE
410956534010657683059962924638288395692613055574427681866195458599332957321	COMPOSITE
284815880386043155601073664123848081027752181457076626146814469796845062331	COMPOSITE
586629754731907246766935156729856756549792084538277552483055374972786447289	COMPOSITE
693820606695319491723694163824406534851224540502756029467541367145841190081	COMPOSITE
902423086546782983749363936311580040428215565679140953330977766939912283843	COMPOSITE
428887749111509262638141004833819932369111904202330425125127392937623921417	COMPOSITE
365841889084037795447873556210977889740077168934316548399114973215611833097	COMPOSITE
149832572986115074176843869976088367374020930408894716249699259449301522557	COMPOSITE
345384566526226685838655946787545471481382787357941935190111322149432728161	COMPOSITE
308392254991463374172878782218158003343892846177887843276121549754602196739	COMPOSITE
911173368032257338231158359521431132230361122777228077540949706206550702863	COMPOSITE
208597846362432415870631653384302953297493112040777767729503288905908533467	COMPOSITE
160807208637658416184403473526993066840405465321501741647303404600129336649	COMPOSITE
467727801117339161676496542916664628372332642031739473901831633058653210069	COMPOSITE
152861401210923136336807270146651305348174853866724995295994224787850355299	COMPOSITE
225562101789239769942868497303842524188035594779244417671788523872676496383	COMPOSITE
663829936646889222047066704866916032810992895660941790711373095451766651857	COMPOSITE
422977329015121540736011865939347857174457321355503662144074058678698716669	COMPOSITE
276210098155614537111822418174234340015154314498101985528625344669584605739	COMPOSITE
767610215332885977309194557830279988632503006940748098234651340265614189049	COMPOSITE
130194238005471399764602278417024945361533480795002960616854527958251811269	COMPOSITE
449187728165617378048511557159436255626102396302347796626434688154988247101	PRIME
180010462444945264602537282998069902582815468658153854995753584022214128723	COMPOSITE
921470625753751150782023177665658943613013875746363048746455849493774169533	COMPOSITE
654972864616561205498166380875022097210107457596386417383198732337344819383	COMPOSITE
690375941624556769726680201681899410770790863445998001583752509003906887327	COMPOSITE
417889097848449778687483891001107193441767760179146036069090726698058675563	COMPOSITE
330028132251105938229998794546097514352139678974960343667891299925596015329	COMPOSITE
805548718225871134642415399028061293999503291741865846924265187503684333907	COMPOSITE
894132777705111311657554729394017742987368271386321590798910718617236250547	COMPOSITE
244602976343641392048178421627013505201640580493900286525416170068826401201	COMPOSITE
821557937970542512953444435983563276074797026284159676515267449589952827377	COMPOSITE
439028241146838958214587577649114305830711180635148041149475944434288074563	COMPOSITE

468252454665851073611875320420041837409699914375530585546471050287113275133	COMPOSITE
158573754118930935742797488052702530684256779778303864099989512904740578493	COMPOSITE
859339150335500204404321989141877959381381751314887084431800551567875600943	COMPOSITE
609255436318669596191524659184483638859686995333179371071176634194750430467	COMPOSITE
765972558890106859244562281628217007896718118536093967861640302518627511853	COMPOSITE
664597955067925504043731177398472952202395025565709270687790268433400781313	COMPOSITE
661750564073895558746048705893665694997449494449146394166891397836194573861	COMPOSITE
826905058896449025017206846450541091732771683125879338111227374286839201829	COMPOSITE
893093675857041745231357070820791872012499298449384003047867553300691662389	COMPOSITE
969874847328148573789645623491234784524131192080536662228566105551079633463	COMPOSITE
911241230197259413555532614926964171138869315068861654949111327682444934507	COMPOSITE
694429052374283078522414551414908393367729473226388804648402352974558448923	COMPOSITE
940147711152483393734033534680307906751520426234695196498372490902406786917	COMPOSITE
549755258862707611233840481460561505332520878912537711958593006368308783023	COMPOSITE
351774464022204028377241908152926909466938287261486331570663204633706435711	COMPOSITE
656602457915592792067357496725333689871461067560268935985243756945324543447	COMPOSITE
787392777999028565176606796246116539879102679112551711989609870138625681237	COMPOSITE
968680567337736025579279251869625175073083190309207442144190145719989775771	COMPOSITE
276820352461423845969955129373252528458178428717700930235552488220747726163	COMPOSITE
921000501101902754994543123813656435454319416110137378084604541876441241093	COMPOSITE
229507719917297438912472059206988035251354948877653723141643899059593435837	COMPOSITE
325278660470276270301974600412254732946947831239261798671871927685114474981	COMPOSITE
227824204026644670313902441104263943047199976769342971436899759050675027213	COMPOSITE
176309626327360179453218945472178879755291519414788664856583424279419961401	COMPOSITE
707419490133711840932341286585064095713982840076337131824498977805782681223	COMPOSITE
725811415127502599554394234264113489881696005022521986848722563683075054397	COMPOSITE
590746789745253471200820054407150984607849230365753975665917595377961101011	COMPOSITE
968993646021033457343647104807995398786371686514846175927700779872171810457	COMPOSITE
935493606193478885632021970035270979160666081111681065966223538063557738857	COMPOSITE
845267997174875615632348625968654519981888725952299796914876271668703086487	COMPOSITE
269397052947619814946559210340915544032849092956497133437110369287147087209	COMPOSITE
446399773300050394064789677236672470865390841869730496838586188468992159701	COMPOSITE
238357270919387884000855484790214170291038504195808841677185090232069055957	COMPOSITE
278548420360165537014545680314716621411895474856821931772803435828648997117	COMPOSITE
171338752657341818112966350741440086448392974981664405464781082620601090207	COMPOSITE
406664738097067829208228604342442292254427013178831490721040544843852060961	COMPOSITE
686536761031490414645016830733458165079008436682158473235739320412410316441	COMPOSITE
642464144166149621068456332391289148324199728460455944091302949067893417431	COMPOSITE
113235363399531500643876331629698970584734620763038473100576110912857707787	COMPOSITE
866915130631461218189138401947416760786452974801648261868095316019956040211	COMPOSITE
857297844127693460029420645144535087129533567953114877554301359552723932279	COMPOSITE
942800096484169649994245382357948007809653596068429817074088130134861438463	COMPOSITE
495052829380775474738079194142899182688952678633922807847662556269259964233	COMPOSITE
679889074764287604023063238786045526927651955415713653645218674058850333921	COMPOSITE
301541885959621856787387431571599969628872708648558923924825414148559869827	COMPOSITE
704709334612276697930958225260265059412498456544269525214404102928791646931	COMPOSITE
807972449389504442934269692230596957699314756799191930247885261436227988439	COMPOSITE
602156734411276661573002081409254487130830784440520587480345214784169106697	PRIME
845031089906849847602314615210192563657720381253631517953100077144073586109	COMPOSITE
480212300013089582308153698879427793488560667461462792592747747075172840369	COMPOSITE
140028682540553757515893257472315587262841181221405047965573102651541295227	COMPOSITE
985584339032359760631223540197605124584962207439192162622114212601216633313	COMPOSITE