THE DECEPTIVE PRIMES TO $2 \cdot 10^7$

Richard Francis and Timothy Ray

Abstract. It has been shown that any prime number $p > 5$ divides the repunit number R_{p-1}. The question of whether there are composite numbers n such that $n|R_{n-1}$ has been answered ($n = 91$ is the first such number). We investigate the distribution of these composite numbers, called deceptive primes, for $n \leq 2 \cdot 10^7$, and the conjectures and questions that arise from our search.

1. Introduction. Various tests for primality appear in the literature, including such obvious tests as the sieve of Eratosthenes and Wilson's Theorem [4]. The lack of a clear and discernible pattern in the distribution of the primes makes the quest of primality determination one of immense intrigue. It has recently led mathematicians in diverse paths of numerous conjectures, analytic methods, and probabilistic techniques. Arbitrarily long gaps between consecutive primes, the erratic appearance of twin primes, Bertrand's Conjecture, and limited prime generating expressions all heighten the question of primality classification.

Within the last two centuries, the attention on false primes, composites that have properties in common with primes, has provided a new avenue of exploration. Composite numbers, appearing as counterexamples to the converse of a theorem which necessitates primality in its hypothesis, may provide a key to a further unlocking of the secret of the primes. If, in fact, such counterexamples are relatively scarce, application of the converse generates a class of numbers which are overwhelmingly prime. One such theorem of this kind is often labeled Fermat's "Little Theorem."

<u>Theorem</u>. (Fermat) Let p be prime. If $(a, p) = 1$, then $a^{p-1} \equiv 1 \pmod{p}$.

The first published proof of the theorem was the work of Euler (1736).

Although congruence notation is attributed to Gauss (as in his *Disquisitiones Arithmeticae* of 1801), Fermat's Little Theorem, in some rhetorical–symbolic form, was known to mathematicians of the ancient Orient. Leibniz conjectured the validity of its converse. In 1819, however, it was discovered that the composite 341 ($= 11 \cdot 31$), is a counterexample to this converse for $a = 2$ (i.e. $2^{340} \equiv 1 \pmod{341}$). Such a number is called a pseudoprime to base 2. The French number theorist, Pierre Frederic Sarrus discovered this counterexample, and other pseudoprimes to base 2 soon followed.

The sporadic appearance of these numbers suggests that n is "probably" prime provided n satisfies the condition $2^{n-1} \equiv 1 \pmod{n}$. Significantly, pseudoprimes may appear to any base (e.g. $3^{90} \equiv 1 \pmod{91}$ and $7^{24} \equiv 1 \pmod{25}$). (The term pseudoprime (without a mention of base) is commonly understood to mean pseudoprime to base 2 [15]. For brevity, we will refer to the set of pseudoprimes to an arbitrary base as pseudoprimes, and will specify pseudoprime to base a when alluding to a specific base.) The essential point is that of the relative scarcity of pseudoprimes (though the set is infinite) in which case an argument of probable primality emerges. Today refined tests are well established, including the Lucas Pseudoprime Test, Miller's Test, and Rabin's Probabilistic Primality Test. Some tests are likewise conjectured and include an analytic number theory consequence of the Generalized Riemann Hypothesis.

An unexplored area of primality, paralleling many of the techniques above, is found within the simply described set of repunits.

Definition 1. A repunit, R_n, is an integer consisting entirely of n "ones" in its decimal representation. It is defined algebraically as

$$R_n = \frac{10^n - 1}{9}.$$

For example, $R_2 = 11$ and $R_7 = 1,111,111$. Note that the set of factors of repunits contains all primes except 2 and 5.

The only known repunit primes are R_2, R_{19}, R_{23}, R_{317}, and R_{1031}; the cardinality of the set of repunit primes is unknown. The cardinality of the set of composite numbers R_p for prime p is also unknown. Obviously, the primality of R_n implies the primality of n, but the converse does not hold (e.g. $R_3 = (3)(37)$ and $R_5 = (41)(271)$). Moreover, $a|b$ if and only if $R_a|R_b$.

A corollary to Fermat's Little Theorem establishes our course.

Corollary 2. If $p > 5$ is prime, then $p|R_{p-1}$.

Proof. Let $p > 5$ be prime. By Fermat's Little Theorem, with $a = 10$, $10^{p-1} \equiv 1 \pmod{p}$. Thus, $p|10^{p-1} - 1$, and since $10^p - 1 = 9999 \cdots 9$, the number composed of $(p-1)$ "nines", then $p|9(1111 \ldots 111)$, and therefore $p|R_{p-1}$.

The fact that $p|R_{p-1}$ for all primes $p > 5$ permits another look at the infinitude of the primes, a fact established in ancient times by Euclid and by others of the modern era (as in Dirichlet's Theorem, the Euler Phi–Function Proof, and Tchebychef's Theorem). The more recent proof by Francis is of an indirect kind and first restricts S to the set of primes greater than 5. Suppose that S is finite with a greatest element p_n. Consider n, the number represented by

$$n = R_{3(p_1-1)(p_2-1)(p_3-1)\cdots(p_n-1)}.$$

That is, let n be the triple of a multiple of all primes which exceed 5. Consider next the number $n+2$ (= $11111 \ldots 1113$). Either $n+2$ is prime or it is composite. If

$n+2$ is prime, then a prime larger than p_n has been constructed (a contradiction). If $n+2$ is composite, then by the Fundamental Theorem of Arithmetic, it has a prime factor p_k. Yet no prime in S can divide $n+2$ as a remainder of 2 results each time. Nor can 2, 3 or 5. Accordingly, $n+2$ is neither prime nor composite (a contradiction). Therefore the set of primes is infinite.

As noted above, if $p > 5$ is prime then $p|R_{p-1}$. Does the converse prove valid? This question is strongly reminiscent of the earlier one that provided an ultimate focus on pseudoprimes. Again, the converse is not true; the first counterexample is $91 = 7 \cdot 13$ $(91|R_{90})$. We label these numbers according to the convention adopted by Francis [9].

Definition 2. A composite number n satisfying the condition $n|R_{n-1}$ is called a deceptive prime.

After 91, the next few deceptive primes are 259, 451, 481, 703, and 1729 (which is also a pseudoprime to base 2).

The set of deceptive primes forms an infinite set and again identifies a point of comparison with the pseudoprimes. Consider any deceptive prime n. As $n|R_{n-1}$, it is also the case that $n|10R_{n-1}$. That is, $n|(R_n - 1)$. Accordingly, $R_n|R_{(R_n-1)}$. A highly useful theorem follows.

Theorem 3. If n is a deceptive prime, then R_n is also a deceptive prime.

Such a theorem guarantees not only the infinitude of the set of deceptive primes, but also the infinitude of the set of repunit deceptive primes. Moreover, the proof is constructive, allowing the calculation of a larger deceptive prime. Here the number of "ones" in the deceptive prime's representation is composite, but not all repunit deceptive primes are generated by this construction (e.g., R_5, R_{13}, and R_{17}). Other possibilities stem from direct use of prime subscripts as suggested in the previous three examples.

Theorem 4. If $p \neq 3$ is prime and R_p is composite, then R_p is a deceptive prime.

Proof. Let $p \neq 3$ be prime. If $p = 2$, $R_p = 11$ which is prime. If $p = 5$ then $R_5 = 41 \cdot 271$, and using direct computation we verify below (see page 5) that $R_5|R_{R_5-1}$. If $p > 5$, then $p|R_{p-1}$ which implies that $R_p|R_{R_{p-1}}$, which in turn implies that $R_p|R_{(R_p-1)}$. Therefore, R_p is either a prime or a deceptive prime. Such a construction will generate infinitely many deceptive primes if the cardinality of $\{R_p : p \neq 3 \text{ is prime, and } R_p \text{ is composite }\}$ is infinite.

This result is somewhat analogous to the fact that any Fermat number $F_n = 2^{2^n} + 1$ is either prime or pseudoprime for whole number values of n. Interestingly, the set of repunit primes and the set of Fermat primes are both unclassified as to cardinality (with only five known in each case). Since only five repunit primes R_p

exist for $p < 20,000$, it follows that R_p is a deceptive prime for all primes p such that $1 < p < 20,000$ and $p \neq 2$, 19, 23, 317, and 1031.

Importantly, R_n may be a deceptive prime even if n is not itself a deceptive prime (such as R_{91}), nor a repunit (such as $R_{R_{91}}$), nor an actual prime (such as R_7). The number R_{10} is an example (i.e. $1111111111|R_{1111111110}$).

Definition 3. A prime p is called a primitive divisor of R_n if $p|R_n$ but $p \not| R_m$ for all $m < n$. For example, 11 is a primitive divisor of R_2. Also, $11|R_{10}$ but, since $11|R_2$, 11 is not a primitive divisor of R_{10}. Note that 9091 is a primitive divisor of R_{10}.

It can be shown that every repunit greater than $R_1 = 1$ has a primitive divisor. Let c be a primitive divisor of R_m and d a primitive divisor of R_{2m}. Of course, $c|R_{2m}$ also. Consequently, $cd|R_{2m}$. Since $c|R_{c-1}$ and $d|R_{d-1}$, $c-1$ is a multiple of both m and $2m$ and $d-1$ is a multiple of $2m$. It follows that $c \equiv 1 \pmod{2m}$ and $d \equiv 1 \pmod{2m}$. Multiplication yields $cd \equiv 1 \pmod{2m}$. This means that $2m|(cd-1)$. The relationships $cd|R_{2m}$ and $R_{2m}|R_{cd-1}$ lead by transitivity to the conclusion that $cd|R_{cd-1}$. Thus, the following is established.

Theorem 5. Let $m > 3$ be an integer. If c is a primitive divisor of R_m and d is a primitive divisor of R_{2m}, then cd is a deceptive prime.

This, of course, gives another argument that the set of deceptive primes is infinite. Note the illustration in which 41 is a primitive divisor of R_5 and 9091 is a primitive divisor of R_{10}. As $372,731 = 41 \cdot 9091$ is a divisor of R_{10} and 10 is a divisor of $372,730$ $(= 41 \cdot 9091 - 1)$, then $372,731$ is a divisor of $R_{41 \cdot 9091 - 1}$. This shows that there are infinitely many deceptive primes of exactly two prime factors.

Other modes of constructing deceptive primes exist. The following is proved in a manner quite similar to the above (i.e., replacement of the factor 2 by the factor 1).

Theorem 6. Let p and q be any two distinct primitive divisors of R_n, where $n > 3$ is odd. Then their product, pq, is a deceptive prime.

Such a theorem is illustrated nicely by the numbers 41 and 271 which are the two primitive divisors of R_5. Their product 11111 is clearly a divisor of R_{11110}.

2. Deceptive Primes Less Than $2 \cdot 10^7$.

There are 924 deceptive primes less than $2 \cdot 10^7$. The algorithm employed to find these was a two-step process.

1. Find an odd composite number n using the sieve of Eratosthenes.
2. Using divisibility tests for several small prime factors p, eliminate any n that has such a prime factor p and that fails the corresponding divisibility test. Any remaining numbers n are tested directly with the definition.

Table 1 lists a summary of the results for the deceptive primes between 0 and $2 \cdot 10^7$, including a tally of the number of factors for each deceptive prime.

		Number of Factors			
x	$D(x)$	2	3	4	5
10^2	1	1	0	0	0
10^3	5	5	0	0	0
10^4	20	14	6	0	0
10^5	62	32	26	4	0
10^6	219	110	69	40	0
10^7	668	290	208	157	13
$2 \cdot 10^7$	924	399	276	228	21

Table 1. $D(x)$, the number of deceptive primes $n \leq x$.

The algorithm was written in ANSI-C. Accordingly, each number n tested using the definition of deceptive primes required $O(n)$ integer divisions (we generate the repunit R_{n-1} one digit at a time as we divide by n). (In Knuth, The Art of Computer Programming, volume 2, Seminumerical Algorithms, the binary method for exponentiation is stated in algorithm form (Algorithm A, Section 4.6.3). This method is of order less than $O(n)$, but requires words of length n. Our algorithm works with any C compiler on any computer for numbers n up to the largest integer allowed by the compiler.) In order to speed up the algorithm, we note that if m is the smallest number such that $n|R_m$, then every m digits of R_{n-1} that are divided by n, the remainder is 0. This gives us the following theorem.

Theorem 7. Let n be any odd positive integer, and let $\alpha[n]$ be the integer such that $n|R_{\alpha[n]}$ but $n \not| R_m$ if $m < \alpha[n]$. n is a deceptive prime if and only if $\alpha[n]|n-1$. If $\alpha[n]$ does not exist for some n, n is not a deceptive prime. For example, $R_5|R_5$ and $5|R_5 - 1 = 11110$, so R_5 is a deceptive prime.

This will speed up the algorithm only if $\alpha[n] < n-1$. To measure the decrease in run time we recorded $\alpha[n]$ for each deceptive prime n as we tested it. Computing the factor $n/\alpha[n]$ provides a quantity that indicates the speed up of the algorithm due to the above theorem.

Once a list of deceptive primes is compiled, natural questions arise concerning subsets of this collection. For pseudoprimes, Euler pseudoprimes, strong pseudoprimes and Carmichael numbers are commonly investigated along with pseudoprimes. We define analogous numbers for deceptive primes.

Definition 4. If n is a deceptive prime, and if n is an Euler pseudoprime to base 10, that is, if $(n, 10) = 1$ and if $10^{(n-1)/2} \equiv \left(\frac{10}{n}\right) \pmod{n}$, where $\left(\frac{10}{n}\right)$ is the Jacobi symbol, then n is called an Euler deceptive prime.

Definition 5. If n is a deceptive prime, and if n is a strong pseudoprime to base 10, that is, for s and d such that $n-1=d\cdot 2^s$, d odd, if $10^d \equiv 1 \pmod{n}$, r if $10^{d\cdot 2^r} \equiv -1 \pmod{n}$ for some r, $0 \leq r < s$, then n is called a strong deceptive prime.

Definition 6. If n is a deceptive prime, and if n is a Carmichael number, that is, if n is a pseudoprime to base a for every a prime to n, then n is called a Carmichael deceptive prime.

The first Euler deceptive prime is 91, which is also the first strong deceptive prime. (It has been shown that if n is a strong pseudoprime to base a, then n is an Euler pseudoprime to base a (one proof occurs in [16]). The first Carmichael deceptive prime is 1729. A summary of the number of these three types of numbers is shown in Table 2.

x	$D(x)$	$D_E(x)$	$D_S(x)$	$D_C(x)$
10^2	1	1	1	0
10^3	5	2	1	0
10^4	20	8	6	4
10^5	62	25	14	11
10^6	219	92	59	34
10^7	668	278	155	89
$2\cdot 10^7$	924	397	217	119

Table 2. The number of Euler deceptive primes ($D_E(x)$),
strong deceptive primes ($D_S(x)$),
and Carmichael deceptive primes ($D_E(x)$).

Another obvious question that arises concerns repeated factors. There are only three primes $p < 2^{32}$ for which $p^2 | 10^{p-1}-1$: 3, 487, and $56,598,313$.[13] Of these, $487^2 = 237169$ and $56,598,313^2 = 3,203,369,034,445,969$ are both deceptive primes ($487^2 | R_{486}$ and $56,598,313^2 | R_{56,598,312}$). Clearly, any other $n = p^2$ where p is prime and $p|10^{p-1}-1$ is a deceptive prime. It is not known if there are any deceptive primes with a factor p^k, where p is prime and $k \geq 3$.

3. Comparison with Pseudoprimes. As shown earlier, a deceptive prime d has the property that $d|10^{d-1}-1$. That is, $10^{d-1} \equiv 1 \pmod{d}$. Accordingly, any number n such that $3\not| n$ and which satisfies $10^{n-1} \equiv \pmod{n}$ is a deceptive prime. Such limited pseudoprimes to base ten generate the entirety of the set of deceptive primes.

This result, summarized below, provides a concise look at the comparison between deceptive primes and pseudoprimes.

Theorem 8. If n is a deceptive prime, then n is a pseudoprime to base 10.

Proof. Since n is composite and $n|R_{n-1}$, then $n|9R_{n-1}$. That is, $n|10^{n-1}-1$. Accordingly,

$$10^{n-1} \equiv 1 \pmod{n}.$$

As the set of deceptive primes is infinite, the set of pseudoprimes to base 10 proves infinite. (The set of pseudoprimes to base a is infinite for any a, a result which was known prior to the classification of the set of Carmichael numbers as an infinite set). The discovery of the existence of Carmichael numbers (see Definition 6) was made in 1909 by the American number theorist Robert Daniel Carmichael (1879–1967) [5].

Thus, the deceptive prime test for primality becomes more significant than the pseudoprime test as it rejects multiples of 3 (such as the Carmichael number 561 which is a pseudoprime to every base relatively prime to it, including two and ten). Such a test is even more impressive in the event the set of Carmichael numbers which are multiples of 3 is infinite. (The set of Carmichael numbers is infinite. [1] It is not known whether the set of Carmichael numbers with 3 as a factor is infinite.)

A comparison of the deceptive primes, pseudoprimes to base 10, and pseudoprimes to base 2 is given in Table 3. The Carmichael deceptive primes are also included, along with Carmichael numbers.

	Deceptive Primes				Pseudoprimes		
x	$D(x)$	$D_E(x)$	$D_S(x)$	$D_C(x)$	$P_2(x)$	$P_{10}(x)$	$C(x)$
10^2	1	1	1	0	0	4	0
10^3	5	2	1	0	3	11	1
10^4	20	8	6	4	22	31	7
10^5	62	25	14	11	78	90	16
10^6	219	92	59	34	245	271	43
10^7	668	278	155	89	750	766	105
$2 \cdot 10^7$	924	397	217	119	1016	1048	141

Table 3. Comparison of deceptive primes and their variations with pseudoprimes to base 2 ($P_2(x)$), pseudoprimes to base 10 ($P_{10}(x)$), and Carmichael numbers ($C(x)$).

It appears that there is a widening gap between the size of the set of deceptive primes and the sizes of the sets of pseudoprimes. In the event that the set of pseudoprimes to base 10 with either 3 or 5 as a factor is infinite, this gap will increase without bound.

Further evidence for the superiority of the deceptive prime test can be found by noting that many deceptive primes are also pseudoprimes to base 2. (In the event that the set of pseudoprimes to base 10 that have either 3 or 5 as a factor is infinite, which seems likely, it is more natural to compare deceptive primes with pseudoprimes to base a, where $a \neq 10$. Due to the frequency of pseudoprimes to base 2 in the literature, we choose these for our comparison.) By collecting these (there are 202 deceptive primes less than $2 \cdot 10^7$ that are also pseudoprimes to base 2), we can plot the difference $P_2(x) - D(x)$ versus x, where x is in the intersection set.

Although the amount of data is small (possibly invoking the 'strong law of small numbers' [11]), the abundance of pseudoprimes to base 2 over the deceptive primes seems to be monotonically increasing.

Finally, in addition to the quantitative data pointing to the usefulness of deceptive primes, qualitative evidence comes from studying perfect numbers.

Definition 7. A number n is called perfect if it equals the sum of its positive divisors, excluding itself. If we denote the sum of all the divisors of n (including n) by $\sigma(n)$, then n is perfect if $\sigma(n) = 2n$. In addition, n is called deficient if $\sigma(n) < 2n$, and is called abundant if $\sigma(n) > 2n$.

A prime number p has only two divisors, namely p and 1, so $\sigma(p) = p + 1$ for all primes p. Thus, the set of prime numbers are the 'most deficient' of all positive integers, since $2p - \sigma(p) = p - 1$. A qualitative measure could therefore be made by comparing the deficiency of other sets of positive integers. The set of deceptive primes is the most deficient of all the sets (the set of Carmichael numbers is hard to make a comparison due to the small number of values). Qualitatively, this displays the usefulness of deceptive primes.

Application of the pseudoprime to base 2 test and the deceptive prime test in conjunction may offer some promise in a more reliable classification of primes. Building on randomly based pseudoprime testing in a combined setting resulted in the Lehmer–Solovay–Strassen probabilistic test [17]. Such a powerful test rests on the fact that n, a tested composite number, will be classified as composite for at least one–half of the base values in the interval from 1 to n. Thus, by a haphazard choice of many bases and utilization of the pseudoprime test each time, the probability of a false classification becomes remarkably small. An allied matter concerns the various base possibilities applied separately. In particular, is there a preferred base in pseudoprime testing (in terms of the comparative frequency in which pseudoprimes appear)?

4. Properties of repunits and deceptive primes. The fertile ground from which deceptive primes grow is the set of repunits. Accordingly, properties of this fundamental class are of immediate consequence in the generating of the allied set of deceptive primes. Some concern parallels to other notable number sets and touch on the diverse subjects of distribution, sums of divisors, digital patterns, and repetition of factors.

1. It is well known that between any prime and its double, another prime appears (Corollary to Bertrand's Conjecture–Tchebychev's Theorem). The corresponding statement for deceptive primes is false. Note that between 91 and 259, no deceptive primes appear. Likewise for 703 and 1729.
2. Infinitely many deceptive primes are of the form $4k+3$. This follows by the theorem shown earlier that if n is a deceptive prime, then R_n is also a deceptive prime. Yet all repunits $R_n (n > 1)$ are of the form $4k+3$.
3. A deceptive prime may have a larger multiple which is also a deceptive prime (e.g. 1729 is a multiple of 91 and 63973 is a multiple of 1729). Moreover, it is possible for two deceptive primes to have a deceptive prime product (e.g. $91 \cdot 451 = 41041$).
4. Infinitely many deceptive primes are imperfect. As any odd perfect number must be of the form $4k+1$, yet there is no largest deceptive prime of the form $4k+3$, infinitely many deceptive primes are thus abundant or deficient.
5. The set of deficient deceptive primes is infinite. As shown earlier, there are infinitely many deceptive primes of exactly two odd prime factors. Such numbers are known to be deficient.
6. No even perfect number can have a deceptive prime divisor. This is obvious as an even perfect number has exactly one odd prime divisor (by the Euclid–Euler characterization). Yet all deceptive primes admit at least two prime divisors.
7. Infinitely many repunits are abundant. It is known that $7 \cdot 11 \cdot 13 \cdot 17 \cdot \cdots \cdot 67 \cdot 71 \cdot 73 = 1357656019974967471687377449$ is abundant. Hence, $R_n = R_{6 \cdot 10 \cdot 12 \cdot 16 \cdot \cdots \cdot 66 \cdot 70 \cdot 72}$ is divisible by $(7)(11)(13)(17)\cdots(67)(71)(73)$. As any multiple of an abundant number is abundant, R_n is likewise abundant. Of course, if R_n is abundant, then R_{kn} (a multiple of R_n) is as well. Accordingly, the set of abundant repunits is infinite. This automatically raises the question about the possibility of abundant deceptive primes. Examples similar to the one above could be obtained by use of the odd abundant numbers $(11)(13)(17)(19)\cdots(137)(139)(149)$ and $(13)(17)(19)(23)\cdots(233)(239)(241)$. In all these illustrations, the ellipsis denotes consecutive primes.
8. There are no twin deceptive primes less than $2 \cdot 10^7$. The smallest difference between two deceptive primes, so far, is 8 (6533 and 6541). The pseudoprimes to base 2 do contain twins (4369 and 4371 are the first pair).
9. If $(6k+1)$, $(12k+1)$, and $(18k+1)$ are each prime numbers, their product $(6k+1)(12k+1)(18k+1)$ is a deceptive prime. It is fairly easy to show that the product $(6k+1)(12k+1)(18k+1)$ is a divisor of $R_{(6k+1)(12k+1)(18k+1)-1}$ in which case the divisor itself is a deceptive prime. The result also follows as a consequence of the fact that $(6k+1)(12k+1)(18k+1)$ is known to be an absolute pseudoprime if each of the three factors is prime. A restriction on k so

as to generate only primes in each case poses today an unsolved problem. Nor does Dirichlet's Theorem guarantee the infinitude of the set. Note: a simple example is obtained by letting $k = 1$ in which case the deceptive prime 1729 is formed (also a Carmichael number).

5. Deceptive Primes to Other Bases. We can talk about deceptive primes to other bases, by defining generalized repunits. R_n is a repunit to base a [6] if

$$R_n = \frac{a^n - 1}{a - 1}.$$

A composite n is called a deceptive prime to base a if $n | R_n$, where R_n is a repunit to base a. Of course, the $a - 1$ in the denominator of the above definition causes prime factors p to fail the deceptive prime test if $p | a - 1$. (We already have the fact that primes p such that $(p, a) \neq 1$ also fail the test by Fermat's Little Theorem.) Table 4 counts the number of deceptive primes to base a for $a \leq 100$.

Table 4. $D_a(x)$, the number of deceptive primes $n \leq 2 \cdot 10^4$ to base a.

a	$D_a(2 \cdot 10^4)$	a	$D_a(2 \cdot 10^4)$	a	$D_a(2 \cdot 10^4)$
2	36	17	33	32	80
3	33	18	47	33	35
4	58	19	49	34	36
5	27	20	31	35	22
6	30	21	18	36	42
7	23	22	30	37	51
8	71	23	47	38	45
9	50	24	42	39	25
10	29	25	45	40	33
11	22	26	25	41	35
12	42	27	54	42	29
13	25	28	29	43	39
14	30	29	28	44	48
15	17	30	52	45	28
16	58	31	27	46	45

Table 4a. $D_a(x)$ for $2 \leq a \leq 46$.

a	$D_a(2 \cdot 10^4)$	a	$D_a(2 \cdot 10^4)$	a	$D_a(2 \cdot 10^4)$
47	44	65	35	83	52
48	52	66	21	84	37
49	53	67	41	85	29
50	29	68	81	86	27
51	29	69	31	87	48
52	31	70	29	88	38
53	36	71	23	89	50
54	33	72	38	90	28
55	31	73	36	91	19
56	25	74	41	92	34
57	37	75	48	93	58
58	33	76	32	94	36
59	45	77	25	95	30
60	33	78	20	96	30
61	35	79	32	97	42
62	50	80	50	98	58
63	31	81	57	99	41
64	92	82	54	100	43

Table 4b. $D_a(x)$ for $47 \le a \le 100$.

6. Conjectures. Various conjectures arise as the set of repunits and the associated set of deceptive primes are explored. Many are simply stated and include the following.

1. The intersection of the set of deceptive primes and the set of pseudoprimes (base two) is infinite.
2. Almost all deceptive primes have a terminal digit of 1.
3. Infinitely many deceptive primes are of the form $4k+1$.
4. Any deceptive prime is a divisor of a still larger deceptive prime (in which case it divides infinitely many).
5. A deceptive prime exists having exactly n distinct prime divisors for all n other than 1.
6. All deceptive primes are deficient.
7. Numbers of the form $2^{2^n}+1$, $n!+1$, and 2^n-1 where n is prime cannot be elements of the set of deceptive primes.
8. For all n greater than 1, a deceptive prime exists having exactly n digits.
9. Infinitely many deceptive primes n exist in which n divides no repunit smaller than R_{n-1}.
10. Though the set of twin primes is unclassified as to cardinality, there are no twin deceptive primes (see properties #9).

11. Arbitrarily long intervals between consecutive deceptive primes exist. Of course, this conjecture has a proven counterpart in the case for primes.

As frequently noted in any of the diverse areas of mathematics, the proving of a theorem gives rise to extended questions. A quest for deceptive primes is no exception. The continued quest leads into scattered areas of pursuit. Conjectures such as the above are but the tip of the proverbial iceberg.

7. Conclusion. Deceptive primes concern an area of number theory in which the pseudoprime concept, though highly relevant, makes a scarcely recognizable appearance. Accordingly, probable prime predicaments subtly surround the notion.

Several advantages of the deceptive prime testing technique stand out. Such a technique yields a dividend immediately, namely a repunit, as opposed to the Fermat converse which requires raising a number to a formidable power. The method leads to an easy generation of other numbers of its kind and has an apparent probabilistic edge over the conventional pseudoprime tests used separately. Of course, the deceptive prime method admits a quick and uncomplicated description of its steps and is thus marked by simplification attempts which are quite suggestive of elementary arithmetic.

Acknowledgments. We thank the Department of Computer Science for providing all of the spare, low priority computer cycles on their IBM RS-6800. We also thank Samuel Wagstaff for providing a list of pseudoprimes to base 2, and Richard Pinch for providing lists of pseudoprimes to base 10 and Carmichael numbers. Finally, we thank Carl Pomerance for his amiable help in locating the lists mentioned above, and Richard Guy and Robert Perlis for their helpful comments at Tim Ray's presentation at the Joint Meetings in San Francisco, January, 1995. We thank God for the opportunity to prepare this paper.

References

1. W. R. Alford, A. Granville and C. Pomerance, "There are Infinitely Many Carmichael Numbers," *Annals of Mathematics*, 140 (1994), 703–722.

2. I. O. Angell and H. J. Godwin, "Some Factorizations of $10^n \pm 1$," *Mathematics of Computation*, 28 (1974), 307–308.

3. A. H. Beiler, *Recreations in the Theory of Numbers: The Queen of Mathematics Entertains*, 1964.

4. D. M. Burton, *Elementary Number Theory*, 2nd Ed., Wm. C. Brown, Dubuque, Iowa, 1989.

5. R. D. Carmichael, "On Composite Numbers P Which Satisfy the Fermat Congruence $a^{P-1} \equiv 1 \pmod{P}$," *American Mathematical Monthly*, 19 (1912), 22–27.

6. H. Dubner, "Generalized Repunit Primes," *Mathematics of Computation*, 61 (1993), 927–930.

7. P. Erdǒs, "On the Converse of Fermat's Theorem," *American Mathematical Monthly*, 56 (1949), 623–624.

8. R. L. Francis, "Probable Prime Predicaments," *Missouri Journal of Mathematical Sciences*, 7 (1995), 132–138.

9. R. L. Francis, "Mathematical Haystacks: Another Look at Repunit Numbers," *The College Mathematics Journal*, 19 (1988), 240–246.

10. R. K. Guy, *Unsolved Problems in Number Theory*, 2nd Ed., Springer–Verlag, New York, 1994.

11. R. K. Guy, "The Strong Law of Small Numbers," *American Mathematical Monthly*, 95 (1988), 697–712.

12. D. H. Lehmer, "Test for Primality by the Converse of Fermat's Theorem," *Bulletin of the American Mathematical Society*, 33 (1927), 327.

13. P. L. Montgomery, "New Solutions of $a^{p-1} \equiv 1 \pmod{p^2}$," *Mathematics of Computation*, 61 (1993), 361–363.

14. R. G. E. Pinch, "The Carmichael Numbers Up to 10^{15}," *Mathematics of Computation*, 61 (1993), 381–391.

15. C. Pomerance, "Lecture Notes on Primality Testing and Factoring," *MAA Notes Number 4*, 1984.

16. C. Pomerance, J. L. Selfridge and S. S. Wagstaff, Jr., "The Pseudoprimes to $25 \cdot 10^9$," *Mathematics Computation*, 35 (1980), 1003–1026.

17. R. Solovay and V. Strassen, "A Fast Monte Carlo Test for Primality," *SIAM Journal of Computing*, 6 (1977), 84–85.

18. H. C. Williams, "On Numbers Analogous to the Carmichael Numbers," *Canadian Mathematics Bulletin*, 20 (1977), 133–143.

19. S. Yates, "Peculiar Properties of Repunits," *Journal of Recreational Mathematics*, 2 (1969) 139–146.

20. S. Yates, "Factors of Repunits," *Journal of Recreational Mathematics*, 3 (1970) 114–119.

Richard Francis
Department of Mathematics
Southeast Missouri State University
Cape Girardeau, MO 63701

Timothy Ray
Department of Mathematics
Southeast Missouri State University
Cape Girardeau, MO 63701
email: timray@image.semo.edu