A 6794
etc

Scan

Dubner

JRM 1987

add to 4 seqs

J. RECREATIONAL MATHEMATICS, Vol. 19(3), 1987

FACTORIAL AND PRIMORIAL PRIMES

HARVEY DUBNER
Dubner Computer Systems, Inc.
6 Forest Avenue
Paramus, New Jersey 07652

When looking for large primes it is natural to investigate numbers of the forms factorial N plus or minus one ($N! \pm 1$) and primorial P plus or minus one ($P\# \pm 1$). The primorial function, $P\#$, is defined as the product of all primes up to and including the prime P. Since all four functions cannot have any small factors, the density of primes will be higher than average. Over the years, papers have been published at irregular intervals describing the progress made in investigating these primes [1-4]. As the power of computers increased, larger numbers were tested and larger primes were found. With my special fast computer in my home [5], I often return to this problem for relaxation between other projects.

I recently found two new large primorial plus one primes (see Tables 1 through 4), the two largest known as of this time:

$11549\# + 1$	~~4591~~ digits 4951
$13649\# + 1$	5862 digits.

I also found a new large factorial minus one *probable* prime and two new large primorial minus one *probable* primes:

$1963! - 1$	5614 digits
$13033\# - 1$	5610 digits
$15877\# - 1$	6845 digits.

A5234

Table 1. The Size of $P\# + 1$ Primes
$P\# + 1 = 2 \times 3 \times 5 \times 7 \times \ldots \times P + 1$

P	Number of Digits
2	1
3	1
5	2
7	3
11	4
31	12
379	154
1019	425
1021	428
2657	1115
3229	1368
4547 ~~4587~~	~~1953~~ 1939
4787 ~~4784~~	2038
11549	4951
13649	5862

Tested up to P = 17159, 7035 Digits

~~A5234~~

A2981

Table 2. The Size of $N! + 1$ Primes
$N! + 1 = 1 \times 2 \times 3 \times \ldots \times N + 1$

N	Number of Digits
1	1
2	1
3	1
11	8
27	29
37	44
41	50
73	106
77	114
116	191
154	272
320	665
340	715
399	867
427	940
872	2188
1477	4042

Tested up to N = 2662, 7964 Digits

A2981

Table 3. The Size of $P\# - 1$ Primes
$P\# - 1 = 2 \times 3 \times 5 \times 7 \times \ldots \times P - 1$

P	Number of Digits	Comment
3	1	
5	2	
11	4	
13	5	
41	15	
89	35	
317	131	
337	136	
991	413	
1873	790	
2053	866	
2377	1077	Probable Prime
4093	1750	Probable Prime
4297	1844	Probable Prime
4583	1953	Probable Prime
6569	2811	Probable Prime
13033	5610	Probable Prime
15877	6845	Probable Prime

Tested up to P = 16699, 7195 Digits

A6794

The Density of Factorial Primes

According to the Prime Number Theorem, the density of primes near M is $1/\log M$. Since primorial and factorial primes are special forms, the question arises as to just what is their density of primes? In what follows, we will use appropriate approximations and sacrifice some rigor to arrive at a reasonable answer.

$$N! \approx \left(\frac{N}{e}\right)^N \tag{1}$$

The number of digits $\approx \log_{10}(N!)$

$$\approx N(\log_{10}N - 0.434). \tag{2}$$

$(N! + 1)$ will be prime if it is not divisible by any prime between N and $(N! + 1)^{1/2}$:

Table 4. The Size of $N! - 1$ Primes
$N! - 1 = 1 \times 2 \times 3 \times \ldots \times N - 1$

N	*Number of Digits*	*Comments*
3	1	
4	2	
6	3	
7	4	
12	9	
14	11	
30	33	
32	36	
33	37	
38	45	
94	147	
166	298	
324	675	
379	815	
469	1051	
546	1260	Probable Prime
974	2490	Probable Prime
1963	5614	Probable Prime

Tested up to N = 2063, 5944 Digits

Probability of Prime $\approx \prod \frac{P-1}{P}$, product taken over all primes between N and $(N!+1)^{1/2}$

$$\approx \frac{\operatorname{Log} N}{\operatorname{Log}(N!+1)^{1/2}} = \frac{2 \operatorname{Log} N}{N(\operatorname{Log} N - \operatorname{Log} e)}$$

$$\text{Probability of Prime} \approx 2/N. \qquad (3)$$

The mathematical steps leading to equation (3) are not obvious and are even somewhat controversial, however, I have statistics supporting equation (3) but this is really the subject of another paper.

The expected number of primes from N_1 to N_2 is

$$E = \frac{2}{N_1} + \frac{2}{N_1+1} + \frac{2}{N_1+2} + \cdots + \frac{2}{N_2}$$

$$E \approx \int_{N_1}^{N_2} \frac{2}{N} dN = 2 \operatorname{Log} N \Big|_{N_1}^{N_2} = 2 \operatorname{Log} \frac{N_2}{N_1} . \qquad (4)$$

Thus, we can expect about 1.4 new primes for each doubling of N, and 4.6 primes for each decade of N. $(N! + 1)$ has been tested up to $N = 2662$ with 17 primes found versus a predicted number of 15.8. $(N! - 1)$ has been tested up to $N = 2063$ with eighteen primes found versus a predicted number of 15.3. Both these results are reasonably close to the predictions.

Testing Time

Finding large primes involves two separate processes: first, finding a probable prime; second, verifying primality. Usually, verification takes a small percentage of the total test time, but more about that later. A number, M, is a probable prime if

$$b^{M-1} \equiv 1 (\operatorname{mod} M) \qquad (5)$$

that is, $(b^{M-1} - 1)$ is divisible by M. The choice of b is not important except for some special cases of M for which certain values of b should be avoided. I usually use $b = 3$. Exponentiation, mod M, can be done efficiently using the "binary method" [6] which requires a series of multiple precision squarings and divisions. To test a 6000-digit number, it is necessary to square a 6000-digit number and then divide the 12,000-digit result by a 6000-digit divisor, and repeat this cycle approximately 20,000 times. About another 10,000 "small" multiplications and divisions are needed, but this adds a negligible amount of time to the total. To test if a 6000-digit number is a probable prime takes me about forty-five minutes. Since the time for squaring on my computer varies directly as the square of the number of digits, the time to test if a number is a probable prime varies as the cube of the number of digits.

Next, let's estimate the time to test all the $(N! + 1)$ numbers from N_1 to N_2:

$$\text{Total time} \approx \sum_{N_1}^{N_2} K_1 [N(\operatorname{Log}_{10} N - 0.434)]^3$$

$$\text{Total time} \approx K_2 (N_2^4 - N_1^4) \qquad (6)$$

From equation (4), to find the next factorial prime requires that

$$\frac{N_2}{N_1} = 1.65 .$$

Substituting this into equation (6) shows that it takes about 6.4 times longer to find the next factorial prime as it took to find all previous ones.

The actual cumulative time to test for factorial primes is shown in Table 5. Also shown is calculated times assuming that the total time varies as N^4. The fit is surprisingly good considering the approximations used and the actual overhead that the computer needs. Using this data, I extrapolated the test time and expected number of primes, and this is shown in Table 6. It seems reasonable to

Table 5. Cumulative Test Time for Factorial Primes ($N! + 1$)

N	*Actual Test Time* *Minutes*	*Est. Time* = KN^4 *Minutes*
Set-up	.1	–
100	.38	.06
200	1.97	.96
300	6.33	4.9
400	17.55	15.4
500	41.55	37.7
626	93.00	92.6
650	110.6	107.6
700	145.5	144.8
820	272.6	272.6

Table 6. Estimated Number of Factorial Primes versus Test Time ($N! + 1$)

	Est. Test Time		*Expected*
N	*Hours*	*Years*	*Number of Primes*
1,000	9.8	.0011	13.8
10,000	98,000.0	11.2	18.4
100,000	9.8×10^8	112,000.	23.0
1,000,000	9.8×10^{12}	1.12×10^9	27.6

conjecture that there are an infinite number of such primes, but new ones will be slow in being discovered. Of course, we can always hope for faster, cheaper computers as well as new techniques for speeding up the search for primes.

Performing the same density and time analysis for primorial primes results in exactly the same equations for the density and the same form of equations for time, the only difference being a multiplying constant. In the time it takes to test factorial primes up to $N = 1000$, primorial primes can be tested up to about $P = 5000$. The expected number of primes is still given by equation 4.

Primality Verification

If a large integer, for example an integer with greater than 1000 digits, is probably prime, it is a virtual certainty that it is prime. However, to verify primality mathematically beyond any doubt other tests have to be performed. For integers with thousands of digits the only practical tests are to be found in [7]. These tests principally depend on the ability to factor $(M + 1)$ or $(M - 1)$ which is obviously possible for primorial and factorial probable primes.

There are two distinctly different tests. The first of these applies to $(P\# + 1)$ and $(N! + 1)$ and consists of a series of calculations similar to equation 5. I have this test programmed on my computer and have verified all the new large primes in Tables 1 and 2. However, I do not have the program for the test applicable to $(P\# - 1)$ and $(N! - 1)$. I have been planning to program this for a long time but I have not yet done so. Because of this I have listed the large entries in Tables 3 and 4 as being "probable primes." I would appreciate any help from anyone to prove these prime. Unfortunately, verifying $(P\# - 1)$ for primality is the most time-consuming possible test because $P\#$ has more distinct factors than any other number.

References

1. A. Borning, Some Results for $k! + 1$ and $2 \times 3 \times 5 \times \ldots P + 1$, *Mathematics of Computation, 26*, pp. 567-570, 1972.
2. M. Templer, On the Primality of $k! + 1$ and $2 \times 3 \times 5 \times \ldots P + 1$, *Mathematics of Computation, 34*, pp. 303-304, 1980.
3. J. P. Buhler, R. E. Caandall, and M. A. Peak, Primes of the Form $M! + 1$ and $2 \times 3 \times 5 \times \ldots \times P + 1$, *Mathematics of Computation, 38*, pp. 639-643, 1982.
4. R. Ondrejka, Ten Extraordinary Primes, *Journal of Recreational Mathematics, 18*:2, pp. 87-92, 1985-86.
5. H. Dubner and R. Dubner, The Development of a Powerful Low-Cost Computer for Number Theory Applications, *Journal of Recreational Mathematics, 18*:2, pp. 81-86, 1985-86.
6. D. E. Knuth, *The Art of Computer Programming*, Volume 2, Second Edition, Addison-Wesley Publishing Co., Reading, MA, 1981.
7. J. Brillhard, D. H. Lehmer, and J. L. Selfridge, New Primality Criteria and Factorizations of $2^n + 1$, *Mathematics of Computation, 29*, pp. 620-647, 1975.