MATHEMATICS OF COMPUTATION
Volume 00, Number 0, Xxxx XXXX, Pages 000–000
S 0025-5718(XX)0000-0

ON THE PRIMALITY OF $n! \pm 1$ AND $2 \times 3 \times 5 \times \cdots \times p \pm 1$

CHRIS K. CALDWELL AND YVES GALLOT

ABSTRACT. For each prime p let $p\#$ be the product of the primes less than or equal to p. We have greatly extended the range for which the primality of $n! \pm 1$ and $p\# \pm 1$ are known and have found two new primes of the first form $(6380! + 1, 6917! - 1)$ and one of the second $(42209\# + 1)$. We supply heuristic estimates on the expected number of such primes and compare these estimates to the number actually found.

1. INTRODUCTION

For each prime p, let $p\#$ be the product of the primes less than or equal to p. About 350 BC Euclid proved that there are infinitely many primes by first assuming they are only finitely many, say $2, 3, \ldots, p$, and then considering the factorization of $p\# + 1$. Since then amateurs have expected many (if not all) of the values of $p\# \pm 1$ and $n! \pm 1$ to be prime. Careful checks over the last half-century have turned up relatively few such primes [5, 7, 13, 14, 19, 25, 32, 33]. Using a program written by the second author, we greatly extended the previous search limits [8] from $n \leq 4580$ for $n! \pm 1$ to $n \leq 10000$, and from $p \leq 35000$ for $p\# \pm 1$ to $p \leq 120000$. This search took over a year of CPU time and has yielded three new primes: $6380! + 1$, $6917! - 1$ and $42209\# + 1$. The second of these (with 23560 digits) was the largest known prime for which modular reduction is non-trivial at the time of its discovery. See Table 1 for a complete list of the known primes of these forms.

TABLE 1. Factorial and primorial primes

form	values for which this form is prime	search limit
$n! + 1$	1, 2, 3, 11, 27, 37, 41, 73, 77, 116, 154, 320, 340, 399, 427, 872, 1477 and **6380** (21507 digits)	10000
$n! - 1$	3, 4, 6, 7, 12, 14, 30, 32, 33, 38, 94, 166, 324, 379, 469, 546, 974, 1963, 3507, 3610 and **6917** (23560 digits)	10000
$p\# + 1$	2, 3, 5, 7, 11, 31, 379, 1019, 1021, 2657, 3229, 4547, 4787, 11549, 13649, 18523, 23801, 24029 and **42209** (18241 digits)	120000
$p\# - 1$	3, 5, 11, 13, 41, 89, 317, 337, 991, 1873, 2053, 2377, 4093, 4297, 4583, 6569, 13033 and 15877 (6845 digits)	120000

Received by the editor March 14, 2000.
2000 *Mathematics Subject Classification.* Primary 11A41; Secondary 11N05, 11A51.
Key words and phrases. Prime numbers, factorial primes, primality proving algorithms.
The first author would like to thank the fellow faculty members who allowed us to use their computers' idle time over a period of months, especially David Ray and John Schommer.

In this article we first provide heuristic estimates of how many such primes "should" be found. We next describe the program used and the search procedure, then list several other new record primes found using this same program in related searches.

2. Heuristical Analysis

An obvious question as we undergo a search of this type is how many such primes do we expect? Is there a reasonable number of new primes to find in this range? Heuristically we can offer an educated guess at what the answer to these questions should be. This has often been done for other forms of primes such as those defined by irreducible polynomials (see, for example, [3, 21]) as well as for some non-polynomial forms (e.g., Mersenne [30, 35], Wieferich [11], generalized Fermat [16][1], and primes of the form $k \cdot 2^n + 1$ [4]). We do it here for the first time for the factorial and primorial primes. Even as we offer these heuristics, we must agree heartily with Bach and Shallit as they muse

> Clearly, no one can mistake these probabilistic arguments for rigorous mathematics and remain in a state of grace[2] Nevertheless, they are useful in making educated guesses as to how number-theoretic functions should "behave." ([1, p. 248])

2.1. **Primorial primes.** Primes of the form $p\# \pm 1$ are sometimes called the primorial primes (a term introduced by H. Dubner as a play on the words prime and factorial). Since $\log p\#$ is the Chebyshev theta function, it is well known that asymptotically $\theta(p) = \log p\#$ is approximately p. In fact Dusart [18] has recently shown

$$|\theta(x) - x| \le 0.006788 \frac{x}{\log x} \quad \text{for } x \ge 2.89 \times 10^7.$$

So by the prime number theorem the probability of a "random" number the size of $p\# \pm 1$ being prime is asymptotically $\frac{1}{p}$. However, $p\# \pm 1$ does not behave like a random variable because primes q less than p divide $1/q^{\text{th}}$ of a random set of integers, but can not divide $p\# \pm 1$. So following the pattern of classic papers such as [3] we divide our estimate by $1 - \frac{1}{q}$ for each of these primes q. Mertens' theorem [22, p. 351] states

$$\prod_{\substack{q \le x \\ q \text{ prime}}} \left(1 - \frac{1}{q}\right)^{-1} = e^{\gamma} \log x + O(1),$$

so we adjust the estimate of the probability that $p\# \pm 1$ is prime to $\frac{e^{\gamma} \log p}{p}$.

By this simple model, the expected number of primes $p\# \pm 1$ with $p \le N$ would then be

[1] The authors treated these as polynomials by fixing the exponent and varying the base.

[2] It is probably not a coincidence that this quote is similar to John von Neumann's remark in 1951 "Any one who considers arithmetical methods of producing random digits is, of course, in a state of sin." [24, p. 1]

$$\sum_{p \le N} \frac{e^\gamma \log p}{p} \sim e^\gamma \log N$$

Conjecture 2.1. The expected number of primorial primes of each of the forms $p\# \pm 1$ with $p \le N$ are both approximately $e^\gamma \log N$.

The known, albeit limited, data supports this conjecture. What is known is summarized in Table 2.

TABLE 2. The number of primorial primes $p\# \pm 1$ with $p \le N$

	actual		**expected**
N	$p\# + 1$	$p\# - 1$	(of each form)
10	4	2	4.1
100	6	6	8.2
1000	7	9	12.3
10000	13	16	16.4
100000	19	18	20.5

Remark 2.2. By the above estimate, the n^{th} primorial prime should be about e^{n/e^γ}.

2.2. **Factorial primes.** The primes of the forms $n! \pm 1$ are regularly called the factorial primes, and like the "primorial primes" $p\# \pm 1$, they may owe their appeal to Euclid's proof and their simple form. Even though they have now been tested up to $n = 10000$ (approximately 36000 digits), there are only 39 such primes known (see Table 1). To develop a heuristical estimate we begin with Stirling's formula:

$$\log n! = (n + \frac{1}{2}) \log n - n + \frac{1}{2} \log 2\pi + O\left(\frac{1}{n}\right)$$

or more simply: $\log n! \sim n(\log n - 1)$. So by the prime number theorem the probability a random number the size of $n! \pm 1$ is prime is asymptotically $\frac{1}{n(\log n - 1)}$.

However, $n! \pm 1$ does not behave like a random variable for several reasons. First, primes q less than n divide $1/q$–th of a set of random integers, but can not divide $n! \pm 1$. So we again divide our estimate by $1 - \frac{1}{q}$ for each of these primes q and by Mertens' theorem we first estimate the probability that $n! \pm 1$ is prime to be

$$\frac{e^\gamma \log n}{n(\log n - 1)}. \tag{2.1}$$

To estimate the number of such primes with n less than N, we may integrate this last estimate to get:

Conjecture 2.3. The expected number of factorial primes of each of the forms $n! \pm 1$ with $n \le N$ are both asymptotic to $e^\gamma \log N$

Table 3 shows a comparison of this estimate to the known results.

As an alternate check on this heuristic model, notice that it also applies to the forms $k \cdot n! \pm 1$ (k small). For $1 \le k \le 500$ and $1 \le n \le 100$ the form $k \cdot n! + 1$ is a prime 4275 times, and the form $k \cdot n! - 1$, 4122 times. This yields an average of 8.55 and 8.24 primes for each k, relatively close to the predicted 8.20.

TABLE 3. The number of factorial primes $n! \pm 1$ with $n \le N$

	actual		**expected**
N	$n!+1$	$n!-1$	(of each form)
10	3	4	4.1
100	9	11	8.2
1000	16	17	12.3
10000	18	21	16.4

But what of the other obstacles to $n! \pm 1$ behaving randomly? Most importantly, what effect does accounting for Wilson's theorem have? These turn out not to significantly alter our estimate above. To see this we first we summarize these divisibility properties as follows.

Theorem 2.4. *Let n be a positive integer.*

i) *n divides $1!-1$ and $0!-1$.*
ii) *If n is prime, then n divides both $(n-1)!+1$ and $(n-2)!-1$.*
iii) *If n is odd and $2n+1$ is prime, then $2n+1$ divides exactly one of $n! \pm 1$.*
iv) *If the prime p divides $n! \pm 1$, then $p-n-1$ divides one of $n! \pm 1$.*

Proof. (ii) is Wilson's theorem. For (iii), note that if $2n+1$ is prime, then Wilson's theorem implies

$$-1 \equiv 1 \cdot 2 \cdot \ldots \cdot n \cdot (-n) \cdot \ldots \cdot (-1) \equiv (-1)^n (n!)^2 \pmod{2n+1}.$$

When n is odd this is $(n!)^2 \equiv 1$, so $n! \equiv \pm 1 \pmod{2n+1}$. Finally, to see (iv), suppose $n! \equiv \pm 1 \pmod{p}$. Since $(p-1)! \equiv -1$, this is

$$(p-1)(p-2) \cdot \ldots \cdot (n+1) \equiv (-1)^{p-n-1}(p-n-1)! \equiv \mp 1 \pmod{p}.$$

This shows p divides exactly one of $(p-n-1)! \pm 1$. □

To adjust for the divisibility properties (ii) and (iii), we should multiply our estimate 2.1 by $1 - \frac{1}{\log n}$, which is roughly the probability that $n+1$ or $n+2$ is composite; and then by $1 - \frac{1}{4 \log 2n}$, which is the probability n is odd and $2n+1$ is prime. The other two cases of Theorem 2.4 require no adjustment. This gives us the following estimate of the primality of $n! \pm 1$.

$$\left(1 - \frac{1}{4 \log 2n}\right) \frac{e^\gamma}{n} \tag{2.2}$$

Integrating as above suggests there should be $e^\gamma(\log N - \frac{1}{4} \log\log 2N)$ primes of the forms $n! \pm 1$ with $n \le N$. Since we are using an integral of probabilities in our argument, we can not hope to do much better than an error of $o(\log N)$, so this new estimate is essentially the same as our conjecture above.

Finally, it is reasonable to finish by asking if Theorem 2.4 indeed summarizes all of the important divisibility properties of $n! \pm 1$. In Table 4 we list the values of n for which p divides $n! \pm 1$ (n is given the same sign as the sign in $n! \pm 1$). We notice the prime divisors come in pairs which add to $p-1$ (as shown in Theorem 2.4.iv). The only other apparent property is that given p, we can place a lower bound on the n as mentioned in the following theorem. This again does not alter our conjecture in any significant way.

TABLE 4. Divisors of $n! \pm 1$ not listed in theorem 2.4

prime p	n for which p divides $n! \pm 1$	prime p	n for which p divides $n! \pm 1$
17	-5, -11	269	9, 259
23	-4, -8, 14, 18	271	93, 177
29	-10, 18	277	40, -236
53	-15, -37	293	45, 75, 217, 247
59	15, -18, 40, 43	307	-54, 63, 243, 252
61	8, 16, 18, -42, -44, -52	311	-29, -90, 220, -281
67	18, -48	317	91, 225
71	7, 9, 19, 51, 61, 63	331	-99, -231
73	-17, -55	359	122, -129, -229, -236
79	23, 55	379	35, 343
83	13, 36, -46, 69	383	85, 297
89	-21, -67	389	-158, -190, 198, 230
97	-43, -53	397	93, -174, 222, 303
103	6, -96	401	25, -69, 128, 173, 227,
109	-22, 86		-272, -331, 375
137	16, 35, 101, -120	419	-102, 316
139	16, -122	431	-64, 366
149	-25, 50, -98, -123	439	-37, -401
193	-90, 102	449	74, -121, -327, -374
199	-81, -89, -109, -117	457	-177, -279
227	61, -82, 144, 165	461	-63, -160, 300, -397
233	64, -101, -131, -168	463	151, 311
239	-28, 210	467	-56, -176, 290, 410
251	97, 153	479	15, -153, -325, 463
257	31, 225	499	-98, 400

(The sign of n determines the sign in $p|n! \pm 1$.)

Theorem 2.5. *Let p be a prime. If $p \mid n! \pm 1$ then $p = n+1, n+2$ or $p \geq n+k$ where k is a solution to $\Gamma(k) - k + 1 = n$.*

Proof. Suppose $p \mid n! \pm 1$ and set $p = n + k$. Clearly $k \geq 1$. If $k = 1$ or 2, then we are done, so suppose $k > 2$. By Wilson's theorem $(p-1)! \equiv -1 \pmod{p}$ so

$$(p-1)(p-2) \cdot \ldots \cdot (n+1) \equiv (-1)^{k-1}(k-1)! \equiv \pm 1 \pmod{p},$$

showing $(k-1)! \equiv \pm(-1)^{k-1} \pmod{p}$. This means $\Gamma(k) \pm (-1)^k$ is a non-zero $(k > 2)$ multiple of $p = n + k$, so $\Gamma(k) \pm (-1)^k \geq n + k$. □

3. The programs

The screening for primes had two phases: (1) We first pre-screened using trial division, then each number n was checked for probable-primality. This work was carried out by a program we call Proth.exe. (2) We then used separate programs to verify the primality of the three probable-primes found in the first step.

3.1. **Proth.exe: probable-primality testing.** This program is named Proth.exe because when it was originally written by the second author, it was intended just to find primes of forms covered by Proth's theorem (see [29] or [22, theorem 102]):

Theorem 3.1. *Let $n > 1$, $k < 2^n$ and $N = k \cdot 2^n + 1$ be a quadratic non-residue* (mod a) *for some odd prime a. Then necessary and sufficient condition for N to be a prime is that $a^{(N-1)/2} \equiv -1 \pmod{N}$.*

At that time Proth.exe was written as a Windows program because of the wide installed-base for this operating system, and was made available on the internet [20] to support a variety of distributive computing projects. Because of Proth.exe's success, it has been expanded to cover a variety of other forms (see the list of records below), including probable-primality testing for the primorial and factorial numbers.

Numbers that are not of the form $k \cdot 2^n + 1$, but that satisfy the condition of Proth's theorem (there is an integer a for which $a^{(N-1)/2} \equiv -1 \pmod{N}$) are called Euler probable-primes [31, p. 226]. The evaluation of $a^{(N-1)/2}$ using the left-to-right binary algorithm takes only $\lceil \log_2 n \rceil$ modular squaring operations [9, p. 9], so the key to doing this quickly is in multiplying quickly. Proth.exe multiplies by evaluating the convolution of the polynomials defined by the representation of the numbers in base 2^{16}, and the convolutions are evaluated using real-signal Fast Fourier Transforms implemented with double precision floating-point numbers [34, chapter 20]. In modern microprocessors, accessing the data in the main memory is more than 20 times slower than executing an arithmetic operation, so algorithms such as split-radix FFT, which were developed to minimize the number of multiplications, are no longer the best algorithms. So we used a modified form of the "Four Step" FFT [2]. Only two passes through the main memory are required. Blocks of data, on which a classical FFT is performed, fit in the level 1 cache of the processor. With numbers of about $30,000$ digits, this algorithm is about five times faster than the same algorithm based on an optimized real-data split-radix FFT. Finally, to compute the modular reduction, the value of the reciprocal of n is computed just once using steady-state division as described in [10, p. 9].

As mentioned above, Proth.exe has been used in a variety of distributive computing projects. For example, as of the date we wrote this article, this program was used to find the following record prime numbers: (1) $169719 \cdot 2^{557557} + 1$ (167847 digits), the largest known "non-Mersenne" prime (found by Stephen Scott in 2000); (2) $481899 \cdot 2^{481899} + 1$, the largest known Cullen prime [23] (found by Masakatu Morii in 1998); (3) $151023 \cdot 2^{151023} - 1$, the largest known Woodall prime [23] (found by Kevin O'Hare in 1998); (4) $506664^{16384} + 1$, the largest known Generalized Fermat prime [4, 17] (found by the second author in 2000); and finally (5) $18458709 \cdot 2^{32611} - 1$ the second largest known Sophie Germain prime [15] (found by Charles Kerchner in 1999).

3.2. **Primality Proving.** Since the program Proth.exe did not include the necessary routines for primality proving for numbers of the form $n! \pm 1$ and $p\# \pm 1$, we used two other programs to complete the primality proofs. In both cases the proofs are straight forward with the classical tests of [6]. For the factorial primes $6380! + 1$ and $6917! - 1$ we used a console version of the Dubner Cruncher (cf. [12, 28]). The prime $42209\# + 1$ presented more difficulty because it was necessary to conduct tests at 1339 of the prime divisors of $42209\#$. The verification was completed by Chris Nash using his implementation (called PrimeForm) of these tests based on the same large integer arithmetic library as Proth.exe. (This library, like Proth.exe, was written by the second author.) The 1339 tests together took approximately 15

hours [27], even when they were combined using the technique of Mihailescu [26] (similar to those of [7]).

References

1. E. Back and J. Shallit, *Algorithmic number theory*, Foundations of Computing, vol. I: Efficient Algorithms, The MIT Press, 1996.
2. D. Bailey, *FFTs in external or hierarchical memory*, Journal of Supercomputing **4**:1 (1990), 23–35.
3. P. T. Bateman and R. A. Horn, *A heuristic asymptotic formula concerning the distribution of prime numbers*, Math. Comp. **16** (1962), 363–367.
4. A. Björn and H. Riesel, *Factors of generalized Fermat numbers*, Math. Comp. **67** (1998), 441–446.
5. A. Borning, *Some results for* $k! \pm 1$ *and* $2 \cdot 3 \cdot 5 \cdots p \pm 1$, Math. Comp. **26** (1972), 567–570.
6. J. Brillhart, D. H. Lehmer, and J. L. Selfridge, *New primality criteria and factorizations of* $2^m \pm 1$, Math. Comp. **29** (1975), 620–647.
7. J. P. Buhler, R. E. Crandall, and M. A. Penk, *Primes of the form* $n! \pm 1$ *and* $2 \cdot 3 \cdot 5 \cdots p \pm 1$, Math. Comp. **38** (1982), 639–643. Corrigendum in Math. Comp. **40** (1983), 727.
8. C. Caldwell, *On the primality of* $n! \pm 1$ *and* $2 \cdot 3 \cdot 5 \cdots p \pm 1$, Math. Comp. **64** (1995), 889–890.
9. H. Cohen, *A course in computational algebraic number theory*, Graduate Texts in Mathematics, vol. 138, Springer-Verlag, New York, 1993.
10. R. Crandall, *Topics in advanced scientific computation*, Springer-Verlag, 1996.
11. R. Crandall, K. Dilcher, and C. Pomerance, *A search for Wieferich and Wilson primes*, Math. Comp. **66** (1997), 433–449.
12. H. Dubner, *The development of a powerful low-cost computer for number theory applications*, J. Recreational Math. **18** (1985-86), 81–86.
13. ———, *Factorial and primorial primes*, J. Recreational Math. **19**:3 (1987), 197–203.
14. ———, *A new primorial prime*, J. Recreational Math. **21**:4 (1989), 276.
15. ———, *Large Sophie Germain primes*, Math. Comp. **65** (1996), 393–396.
16. H. Dubner and Y. Gallot, *Distribution of generalized Fermat prime numbers*, Preprint, 1999.
17. H. Dubner and W. Keller, *New Fibonacci and Lucas primes*, Math. Comp. **68** (1999), 417–427.
18. P. Dusart, *The* k^{th} *prime is greater than* $k(\ln k + \ln \ln k - 1)$ *for* $k \geq 2$, Math. Comp. **68** (1999), 411–415.
19. A. Ferrier, *Les nombres premiers*, Librairie Vuibert, Boulevard Saint-Germain, Paris, 1947.
20. Y. Gallot, *Proth.exe: a windows program for finding very large primes*, 1999, http://www.utm.edu/research/primes/programs/gallot/.
21. G. H. Hardy and J. E. Littlewood, *Some problems of 'partitio numerorum': III: On the expression of a number as a sum of primes*, **44** (1922), 1–70, Reprinted in "Collected Papers of G. H. Hardy," Vol. I, pp. 561-630.
22. G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers*, Oxford University Press, 1979.
23. W. Keller, *New Cullen primes*, Math. Comp. **64** (1995), 1733–1741. Supplement S39-S46.
24. D. E. Knuth, *The art of computer programming. Volume 1: Fundamental algorithms*, Addison-Wesley, 1975, 2nd edition.
25. M. Kraitchik, *Introduction à la théorie des nombres*, Gauthier-Villars, Paris, 1952, pp. 2, 8.
26. P Mihailescu and C. Nash, *Binary tree evaluation method for Lucas-Lehmer primality tests*, preprint, 1999.
27. C. Nash, *42209#+1 is prime*, personal communication to the authors, May 1999.
28. I. Peterson, *Dubner's primes*, Science News **144**:21 (1993), 331.
29. F. Proth, *Théorèmes sur Les Nombres Premiers*, C. R. Acad. Sci. Paris **85** (1877), 329–331.
30. M. R. Schroeder, *Where is the next Mersenne prime hiding?*, Math. Intelligencer **5**:3 (1983), 31–33.
31. D. Shanks, *Solved and unsolved problems in number theory*, Chelsea, New York, 1978.
32. W. Sierpinski, *Elementary theory of numbers*, Monografie Mat., vol. 42, PWN, Warsaw, 1964, p. 202.
33. M. Templer, *On the primality of* $k! + 1$ *and* $2 * 3 * 5 * \cdots * p + 1$, Math. Comp. **34** (1980), 303–304.

34. W. Vetterling W. Press, S. Teukolsky and B. Flannery, *Numerical recipes in C: The art of scientific computing*, Cambridge University Press, 1993.
35. S Wagstaff, *Divisors of Mersenne numbers*, Math. Comp. **40** (1983), 385–397.

Department of Mathematics and Computer Science,
University of Tennessee at Martin, Martin, Tennessee 38238
E-mail address: caldwell@utm.edu

Current address: 12 bis rue Perrey, 31400 Toulouse, France
E-mail address: galloty@wanadoo.fr