A PROBLEM ON THE CONJECTURE CONCERNING THE DISTRIBUTION OF GENERALIZED FERMAT PRIME NUMBERS (A NEW METHOD FOR THE SEARCH FOR LARGE PRIMES)

YVES GALLOT

Abstract. Is it possible to improve the convergence properties of the series for the computation of the C_n involved in the distribution of the generalized Fermat prime numbers? If the answer to this question is yes, then the search for a large prime number P will be $C \cdot \log(P)$ times faster than today, where $C \approx 0.01$.

1. Introduction

In [2], based on Bateman and Horn conjecture [1][11] and on the distribution of the factors of the generalized Fermat numbers [3], Harvey Dubner and the author proposed the following conjecture:

Conjecture 1.1. *If $E_n(B)$ is the number of primes of the form $F_{b,n} = b^{2^n} + 1$ for $2 \leq b \leq B$, then*

$$E_n(B) \sim \frac{C_n}{2^n} \int_2^B \frac{dt}{\log t}$$

where the constant C_n is the infinite product

$$C_n = \prod_{p \text{ odd prime}} \frac{(1 - \frac{a_n(p)}{p})}{(1 - \frac{1}{p})} = \prod_{p \text{ odd prime}} \left(1 - \frac{a_n(p) - 1}{p - 1}\right)$$

and where

$$a_n(p) = \begin{cases} 2^n & \text{if } p \equiv 1 \pmod{2^{n+1}}, \\ 0 & \text{otherwise.} \end{cases}$$

The actual distribution of generalized Fermat primes is in significant agreement with the values predicted by the conjecture for some polynomials of degree as large as 2^{16}.

Today, we know that $C_0 = 1$ and in [9][10] Shanks computed precisely C_1 and C_2. We indicate in this paper a method for the computation of the first C_n; however the method becomes unpractical for $n > 20$. Today, no relation is known for a fast computation of other C_n and we have to search for the smallest primes of the form $k \cdot 2^{n+1} + 1$ to estimate them.

What will be the consequences, if a formula, involving only some functions and series and not the primes of the form $k \cdot 2^{n+1} + 1$, exists to compute precisely C_n?

Date: November 18, 2001; revised March 17, 2003.
2000 *Mathematics Subject Classification.* Primary 11Y11; Secondary 11A41.
Key words and phrases. prime numbers, prime distribution, generalized Fermat numbers.

The search for a large prime of the form $k \cdot 2^n + 1$ will be about $n/200$ times faster than it is today. For $n \approx 10^7$, the search will be 50000 times faster!

The chance for a number of the form $N = k \cdot b^n \pm 1$ to be prime depends on its size but is virtually independent of k, b, n as long as N passed a trial division test up to the bound $\log(N)$. Today, to find a prime, we have to check the primality of all the numbers that passed a trial division test. In practice, we have to test about $0.02 \cdot \log(P)$ numbers to find a prime P.

If C_n can be computed quickly and precisely, the minima of the sequence C_n will indicate to us where the primes of the form $k \cdot 2^n + 1$, with small k, are. For example, the estimates for $\{C_{27}, C_{28}, C_{29}, C_{30}\}$ are $\{19.5, 19.2, 17.8, 22.0\}$: it indicates that it is probably faster to search for a prime of the form $k \cdot 2^n + 1$ for $n = 29 + 1$ rather than for the other values. And we find that the smallest primes of each form are $12 \cdot 2^{28} + 1, 6 \cdot 2^{29} + 1, 3 \cdot 2^{30} + 1$ and $35 \cdot 2^{31} + 1$.

If C_n can be used as an indicator, then we will just have to test two or three numbers to find a prime of the form $3 \cdot 2^n + 1$ or $5 \cdot 2^n + 1$ rather than, today, about $0.02 \log(2)n$ numbers: the search for a large prime number P will be about $0.01 \cdot \log(P)$ times faster if the indicator C_n can be evaluated quickly and if we test the form $k \cdot 2^n + 1$.

The following sections indicate a formula for C_n but that is quickly unpractical for large n. Can you improve this formula and speed up the prime number search?

2. Definitions

Let the infinite products

$$C_n(s) = \prod_{p \text{ odd prime}} \frac{1 - a_n(p)p^{-s}}{1 - p^{-s}}$$

and

$$P_n(s) = \prod_{p \equiv 1 (2^{n+1})} \left(\frac{1 - p^{-s}}{1 + p^{-s}} \right)^{2^{n-1}}.$$

Let χ be a Dirichlet character. The L-series attached to χ is defined by

$$L(s, \chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} = \prod_p (1 - \chi(p)p^{-s})^{-1}, \qquad \mathrm{Re}(s) > 1.$$

Let $X(m)$ be the character group $(Z/2^m Z)^*$.

For $m = 1$, only the trivial character χ_0 is defined and $L(s, \chi_0)$ is the Dirichlet lambda function $\lambda(s) = \sum_{n=0}^{\infty} (2n+1)^{-s} = (1 - 2^{-s})\zeta(s)$.

For $m = 2$, there are two characters: the trivial one and the character χ_4 defined by $\chi_4(n) = (\frac{-4}{n})$, where $(\frac{a}{n})$ is the Kronecker symbol with the definition $(\frac{a}{2}) = 0$ for a even. $L(s, \chi_4) = \sum_{n=0}^{\infty} (-1)^n (2n+1)^{-s}$ is the Dirichlet beta function $\beta(s)$.

For $m \geq 3$, the group $(Z/2^m Z)^*$ is generated by -1 and 5. Thus a character is uniquely determined by its value in -1 and 5. The order of -1 is 2 and the order of 5 is $\varphi(2^m)/2$. For every $a \in \{0, 1\}$ and $b \in \{1, \cdots, \varphi(2^m)/2\}$, we can associate the character $\chi_{a,b}$ uniquely determined by $\chi_{a,b}(-1) = (-1)^a$ and $\chi_{a,b}(5) = \exp(2\pi i b / 2^{m-2})$.

Note that for $m = 3$, the two primitive characters are real. There L-series are $L(s, \chi_{0,1}) = \sum_{n=1}^{\infty} (\frac{2}{n}) n^{-s}$ and $L(s, \chi_{1,1}) = \sum_{n=1}^{\infty} (\frac{-2}{n}) n^{-s}$.

3. Shanks' formula

In [9], Daniel Shanks developed a method to compute with accuracy and efficiently C_1 and in [10], he used a similar method to compute C_2.

Lemma 3.1. *If a is a positive even integer and if $|x| < \frac{1}{a}$, then*

$$1 - ax = \prod_{n=1}^{\infty} \left(\frac{1 - x^n}{1 + x^n} \right)^{b_a(n)}$$

where

$$b_a(n) = \frac{1}{2n} \sum_{\substack{d|n \\ d \text{ odd}}} \mu(d) a^{n/d}. \tag{3.1}$$

Proof. We expand both sides in Maclaurin series and identify the corresponding coefficients. This yields the condition

$$2 \sum_{\substack{d|n \\ d \text{ odd}}} b_a\left(\frac{n}{d}\right) \frac{n}{d} = a^n.$$

Now applying the Möbius inversion formula we obtain (3.1). □

For $s > 1$,

$$\begin{aligned} C_n(s) &= \lambda(s) \prod_{p \equiv 1 (2^{n+1})} \left(1 - \frac{2^n}{p^s}\right) \\ &= \lambda(s) P_n(s) \prod_{p \equiv 1 (2^{n+1})} \left(1 - \frac{2^n}{p^s}\right) \left(\frac{1 + p^{-s}}{1 - p^{-s}}\right)^{2^{n-1}}. \end{aligned}$$

By lemma 3.1 and since $b_{2^n}(1) = 2^{n-1}$, we obtain the relation

$$C_n(s) = \lambda(s) P_n(s) \prod_{p \equiv 1 (2^{n+1})} \prod_{k=2}^{\infty} \left(\frac{1 - p^{-ks}}{1 + p^{-ks}}\right)^{b_{2^n}(k)}.$$

It can be rewritten as

Formula 3.2.

$$C_n(s) = \lambda(s) P_n(s) \prod_{k=2}^{\infty} P_n(ks)^{\frac{b_{2^n}(k)}{2^{n-1}}}.$$

4. Computation of the constant C_1

It is easy to verify that

$$P_1(s) = \frac{\lambda(2s)}{\lambda(s)\beta(s)}.$$

We have from (3.2)

$$C_1(s) = \lambda(s) \frac{\lambda(2s)}{\lambda(s)\beta(s)} \prod_{k=2}^{\infty} \left(\frac{\lambda(2ks)}{\lambda(ks)\beta(ks)}\right)^{b_2(k)}.$$

The product converges for $s=1$, $\lambda(2)=\frac{\pi^2}{8}$ and $\beta(1)=\frac{\pi}{4}$ then

$$C_1 = \frac{\pi}{2}\prod_{k=2}^{\infty}\left(\frac{\lambda(2k)}{\lambda(k)\beta(k)}\right)^{b_2(k)}. \tag{4.1}$$

5. Computation of the constant C_2

It is easy to verify that

$$P_2(s) = \frac{\lambda(2s)^2}{\lambda(s)\beta(s)L(s,\chi_{0,1})L(s,\chi_{1,1})}.$$

We have from (3.2)

$$C_2(s) = \lambda(s)\frac{\lambda(2s)^2}{\lambda(s)\beta(s)L(s,\chi_{0,1})L(s,\chi_{1,1})}\prod_{k=2}^{\infty}\left(\frac{\lambda(2ks)^2}{\lambda(ks)\beta(ks)L(ks,\chi_{0,1})L(ks,\chi_{1,1})}\right)^{\frac{b_4(k)}{2}}.$$

The product converges for $s=1$, $L(1,\chi_{1,1})=\frac{\pi}{2\sqrt{2}}$ and $L(1,\chi_{0,1})=\frac{\log(1+\sqrt{2})}{\sqrt{2}}$ then

$$C_2 = \frac{\pi^2}{4\log(1+\sqrt{2})}\prod_{k=2}^{\infty}\left(\frac{\lambda(2k)^2}{\lambda(k)\beta(k)L(k,\chi_{0,1})L(k,\chi_{1,1})}\right)^{\frac{b_4(k)}{2}}. \tag{5.1}$$

6. Computation of C_n

Pieter Moree indicated to the author [7] a generalization of Shanks' formula:

Theorem 6.1.

$$P_n(s) = \frac{M_n(2s)^2}{L_n(s)}$$

where

$$L_n(s) = \prod_{\chi\in X(n+1)} L(s,\chi)$$

and

$$M_1(s) = \sqrt{\lambda(s)}$$

and for $n \geq 2$

$$M_n(s) = \prod_{\substack{\chi\in X(n)\\ \chi(-1)=1}} L(s,\chi).$$

Proof. An elementary proof (that requires no algebraic number theory) is indicated here.

Let $G(s,\chi)=\sum_p\sum_{k=1}\chi(p^k)\frac{p^{-ks}}{k}$. $G(s,\chi)$ provides an unambiguous definition for $\log L(s,\chi)$ [5, p. 256]. For $n\geq 2$,

$$\begin{aligned}\log\frac{M_n(2s)^2}{L_n(s)} &= 2\sum_{\substack{\chi\in X(n)\\ \chi(-1)=1}} G(2s,\chi) - \sum_{\chi\in X(n+1)} G(s,\chi)\\ &= \sum_p\sum_{k=1}\Bigg(2\sum_{\substack{\chi\in X(n)\\ \chi(-1)=1}}\chi(p^k)\frac{p^{-2ks}}{k} - \sum_{\chi\in X(n+1)}\chi(p^k)\frac{p^{-ks}}{k}\Bigg).\end{aligned}$$

$\sum_{\chi\in X(n+1)}\chi(p^k) = \varphi(2^{n+1})\delta_{2^{n+1}}(1,p^k)$, where $\delta_m(a,b) = 1$ if $a \equiv b \pmod{m}$ and $\delta_m(a,b) = 0$ otherwise. $2\sum_{\substack{\chi\in X(n)\\ \chi(-1)=1}}\chi(p^k) = \sum_{\chi\in X(n)}(\chi(-p^k)+\chi(p^k)) = \varphi(2^n)(\delta_{2^n}(-1,p^k)+\delta_{2^n}(1,p^k)) = \varphi(2^n)\delta_{2^{n+1}}(1,p^{2k})$. Thus,

$$\begin{aligned}\log\frac{M_n(2s)^2}{L_n(s)} &= \sum_p\sum_{k=1}\left(2^n\delta_{2^{n+1}}(1,p^{2k})\frac{p^{-2ks}}{2k} - 2^n\delta_{2^{n+1}}(1,p^k)\frac{p^{-ks}}{k}\right)\\ &= -2^n\sum_{k\text{ odd}}\sum_{p^k\equiv 1(2^{n+1})}\frac{p^{-ks}}{k}.\end{aligned}$$

Let ω be the order of p modulo 2^{n+1}. ω divides $\varphi(2^{n+1}) = 2^n$ and if $p^k \equiv 1 \pmod{2^{n+1}}$, ω divides k odd then $\omega = 1$ and $p \equiv 1 \pmod{2^{n+1}}$. It follows that

$$\begin{aligned}\log\frac{M_n(2s)^2}{L_n(s)} &= -2^n\sum_{p\equiv 1(2^{n+1})}\sum_{k\text{ odd}}\frac{p^{-ks}}{k}\\ &= 2^{n-1}\sum_{p\equiv 1(2^{n+1})}\log\left(\frac{1-p^{-s}}{1+p^{-s}}\right) = \log P_n(s).\end{aligned}$$

□

The product converges for $s = 1$, then we have from (3.2)

Formula 6.2.

$$C_n = \frac{M_n(2)^2}{L_n(1)}\prod_{k=2}^{\infty}\left(\frac{M_n(2k)^2}{L_n(k)}\right)^{\frac{b_{2^n}(k)}{2^{n-1}}},$$

where $L_n(1)$ is the residue of the Dedekind zeta function of $\mathbb{Q}(\zeta_{2^{n+1}})$ at $s = 1$.

7. Estimates of C_n

For the computation of $L_n(k)$, we use the relation

$$L_n(s) = L_{n-1}(s)\prod_{\substack{\chi\in X(n+1)\\ \chi\text{ primitive}}}L(s,\chi)$$

$$L_0(s) = \begin{cases}1 & \text{if } k=1,\\ \lambda(k) & \text{otherwise.}\end{cases}$$

and for the computation of $M_n(k), n \geq 2$

$$M_n(s) = M_{n-1}(s)\prod_{\substack{\chi\in X(n),\ \chi(-1)=1\\ \chi\text{ primitive}}}L(s,\chi)$$

$$M_2(s) = \lambda(k).$$

For $\mathrm{Re}(s) > 1$, $L(s,\chi)$ can be evaluated quickly by the formula

$$L(s,\chi) = f^{-s}\sum_{n=1}^{f}\chi(n)\zeta(s,\frac{n}{f}),$$

where f is the conductor of χ and $\zeta(s,a) = \sum_{n=0}^{\infty}(a+n)^{-s}$ is the Hurwitz zeta function. $L(1,\chi)$ can also be evaluated as a sum of f terms by Theorem 4.9 of [12]:

Theorem 7.1. *Let χ be a non trivial Dirichlet character of conductor f and $\tau(\chi) = \sum_{a=1}^{f} \chi(a) e^{2\pi i a/f}$ be a Gauss sum. Then*

$$L(1,\chi) = \begin{cases} \pi i \frac{\tau(\chi)}{f^2} \sum_{a=1}^{f} \bar{\chi}(a) a & \text{if } \chi(-1) = -1, \\ -\frac{\tau(\chi)}{f} \sum_{a=1}^{f} \bar{\chi}(a) \log|2\sin(\pi a/f)| & \text{if } \chi(-1) = 1. \end{cases}$$

Note that, by remarking that $\prod_{\chi} \frac{\tau(\chi)}{\sqrt{f} i^{\delta}} = 1$, we can exclude the Gauss sums associated to f of the computation.

Because of the cancellation of the series, the usage of high precision is required. We used Pari/GP calculator [8] and GNU MP [4] for the computation.

Table 1. Results

n	$1/L_n(1)$	C_n
1	1.2732395447351626862	1.3728134628182460091
2	1.8393323355189883003	2.6789638797482848822
3	2.1525897547289665031	2.0927941299213300766
4	3.5915460044718845396	3.6714321229370805404
5	3.6517070262282297544	3.6129244862406263646
6	4.1255743008723022645	3.9427412953667399869
7	3.8076566382722473439	3.1089645815159960954
8	7.4360874409142208222	7.4348059978748568639
9	7.5184624012206212999	7.4890662797425630491
10	8.0721025282979537844	8.0193434982306030483
11	7.3647294084873125710	7.2245969049003170901
12	8.5063380378154203965	8.4253498784241795333
13	8.5931795231960285064	8.4678857199473387694
14	8.3718452818332958280	8.0096845351535704233
15	7.0545211775956337581	5.8026588347082479139
16	11.263974068691738207	11.195714229391949615
17	11.189718898237277808	11.004300588768807590
18	13.040977439195566699	
19	13.129323890520994181	

8. Future Studies

The results lead us to propose

Conjecture 8.1.

$$\lim_{n\to\infty} L_n(1) C_n = 1$$

and to use the local maxima of $L_n(1)$ as indicators for the primes of the form $k \cdot 2^{n+1} + 1$.

But if theorem 7.1 is used for the computation, we cannot estimate $L_n(1)$ or C_n in a reasonable amount of time for $n \geq 100$ and today the only probable prime that the computation indicated is $2^{15+1} + 1 = 65537$. What is interesting in the method is that no Euclidean division was required for the computation, except some modulo 2^m for the estimates of the characters. However, to become practical, a fast method for the computation of the residue of $\zeta_{\mathbb{Q}(\zeta_{2^{n+1}})}(s)$ at $s = 1$ is necessary.

Now, if we consider that the primes of the form $k \cdot 2^{n+1} + 1$ are uniformly distributed with a density function defined by the theorem of de la Vallée-Poussin, we have $C_n \approx (n+1)\log 2$ [6]. This result can be used to normalize our indicator.

Table 2. Estimates of $1/L_n(1)$

n	$1/L_n(1)$	$(n+1)\log 2$	$L_n(1)(n+1)\log 2$	first prime $k \cdot 2^{n+1} + 1$
1	1.273240	1.386294	1.088793	$1 \cdot 2^2 + 1$
2	1.839332	2.079442	1.130542	$2 \cdot 2^3 + 1$
3	2.152590	2.772589	1.288025	$1 \cdot 2^4 + 1$
4	3.591546	3.465736	0.964970	$3 \cdot 2^5 + 1$
5	3.651707	4.158883	1.138887	$3 \cdot 2^6 + 1$
6	4.125574	4.852030	1.176086	$2 \cdot 2^7 + 1$
7	3.807657	5.545177	1.456323	$1 \cdot 2^8 + 1$
8	7.436087	6.238325	0.838926	$15 \cdot 2^9 + 1$
9	7.518462	6.931472	0.921927	$12 \cdot 2^{10} + 1$
10	8.072103	7.624619	0.944564	$6 \cdot 2^{11} + 1$
11	7.364729	8.317766	1.129406	$3 \cdot 2^{12} + 1$
12	8.506338	9.010913	1.059318	$5 \cdot 2^{13} + 1$
13	8.593180	9.704061	1.129275	$4 \cdot 2^{14} + 1$
14	8.371845	10.397208	1.241925	$2 \cdot 2^{15} + 1$
15	7.054521	11.090355	1.572092	$1 \cdot 2^{16} + 1$
16	11.263974	11.783502	1.046123	$6 \cdot 2^{17} + 1$
17	11.189719	12.476649	1.115010	$3 \cdot 2^{18} + 1$
18	13.040977	13.169796	1.009878	$11 \cdot 2^{19} + 1$
19	13.129324	13.862944	1.055876	$13 \cdot 2^{20} + 1$

Accorting to results of Table 2, the average behaviour of $L_n(1)$ is $[(n+1)\log 2]^{-1}$ and its behaviour depends mainly on the first prime of the form $k \cdot 2^{n+1} + 1$. We propose

Conjecture 8.2. *Let $\mathcal{R}_n$ be the residue of the Dedekind zeta function $\zeta_{\mathbb{Q}(\zeta_{2^n})}(s)$ at $s = 1$. We have*

$$\lim_{m\to\infty} \frac{1}{m} \sum_{n=1}^{m} \mathcal{R}_n \log 2^n = 1.$$

There exist a constant $0 < c < 1$ and a constant $C > 1$ such that

$$c \leq \mathcal{R}_n \log 2^n \leq C$$

for all n.

References

1. P. T. Bateman and R. A. Horn, *A Heuristic Asymptotic Formula Concerning the Distribution of Prime Numbers*, Math. Comp. **16** (1962), 363–367.
2. H. Dubner and Y. Gallot, *Distribution of generalized Fermat prime numbers*, Math. Comp. **71** (2002), 825–832.
3. H. Dubner and W. Keller, *Factors of generalized Fermat numbers*, Math. Comp. **64** (1995), 397–405.
4. The GMP library, *The GNU MP web pages*, http://www.swox.com/gmp/.
5. K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, 2nd ed., Springer-Verlag, New York, 1990.
6. A. Kulsha, *communication to PrimeNumber egroup*, 24 december 2001.

7. P. Moree, *private communication*, 2002.
8. The PARI Group, *PARI / GP*, http://www.parigp-home.de.
9. D. Shanks, *On the Conjecture of Hardy & Littlewood concerning the Number of Primes of the Form* $n^2 + a$, Math. Comp. **14** (1960), 321–332.
10. D. Shanks, *On Numbers of the Form* $n^4 + 1$, Math. Comp. **15** (1961), 186–189.
11. A. Schinzel and W. Sierpiński, *Sur certaines hypothèses concernant les nombres premiers*, Acta Arith. **4** (1958), 185–208, Erratum **5** (1959), 259.
12. L. C. Washington, *Introduction to Cyclotomic Fields*, 2nd ed., Springer-Verlag, New York, 1997.

E-mail address: galloty@wanadoo.fr