Gaps between generalized Fermat prime numbers

Yves Gallot

August 4, 2020

Let n and b be positive integers, the generalized Fermat number $F_n(b)$ is

$$F_n(b) = b^{2^n} + 1.$$

Assume $b_1 < b_2$. If $F_n(b_1)$ and $F_n(b_2)$ are two prime numbers and $F_n(b)$ is composite for $b_1 < b < b_2$ then $a = b_2 - b_1$ is called the gap between $F_n(b_1)$ and $F_n(b_2)$.

For fixed n, the number of generalized Fermat primes is conjectured to be infinite. For $n = 1$, this open problem is known as Landau's fourth problem.
The distribution of the generalized Fermat prime numbers and of their pairs can be computed assuming Bateman-Horn conjecture [2].

Conjecture (Bateman and Horn).
Let $f_1, f_2, \cdots, f_m$ be a set of m distinct irreducible polynomials with integral coefficients and a positive leading coefficient. Let f be their product and suppose that f does not vanish identically modulo any prime. Let $w(p)$ be the number of solutions to the congruence $f(x) \equiv 0 \pmod p$. An integer n is prime-generating if every polynomial $f_i(n)$ produces a prime number.
If $\pi_f(x)$ is the number of prime-generating integers for $n \leq x$ then

$$\pi_f(x) \sim \frac{C_f}{D_f} \int_2^x \frac{dt}{(\log t)^m}$$

where D_f is the product of the degrees of the polynomials $f_1, f_2, \cdots, f_m$ and

$$C_f = \prod_{p \text{ prime}} \frac{1 - w(p)/p}{(1 - 1/p)^m}.$$

It is interesting to note that Roger Horn used one of the first computers, the ILLIAC I to formulate and check the conjecture. Bateman and Horn computed $\pi_f(x)$ for various $x \leq 113,000$ with $f_1(x) = x$ and $f_2(x) = x^2 + x + 1$ [1]. We are still using computers to check the conjecture but today we can test it with some polynomials of degree 2^{10} and $x \leq 10^9$ or some of degree 2^{20} and $x \leq 10^6$.

If $f_1(x) = x^{2^n} + 1$ and $f_2(x) = (x + a)^{2^n} + 1$, the density of pairs of generalized Fermat primes can be computed. The density of gaps can then be derived.

Number of generalized Fermat prime numbers

Let n be a positive integer and $f(x) = f_1(x) = x^{2^n} + 1$.
The expected number of generalized Fermat primes $b^{2^n} + 1$ for $2 \le b \le x$ is

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

We have $w_n(2) = 1$, $w_n(p) = 2^n$ if $p \equiv 1 \pmod{2^{n+1}}$ and $w_n(p) = 0$ otherwise.

Daniel Shanks computed C_1 [4] and C_2 [5] to high precision. His method can be extended to any C_n. The accelerated product is based on the lemma

Lemma. *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

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

For $s > 1$, let the infinite products

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

and

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

λ is the Dirichlet lambda function $\lambda(s) = \prod_{p \text{ odd}} (1-p^{-s})^{-1} = (1-2^{-s})\,\zeta(s)$.
We have

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

which by the lemma and since $b_{2^n}(1) = 2^{n-1}$ becomes

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

Finally, it can be rewritten as

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

Peter Moree indicated to the author [3] a method for the computation of $P_n(s)$ by representing them as a product of Dirichlet L-series.

Theorem. *Let $X(m)$ be the character group $(Z/2^mZ)^*$, $L(s,\chi)=\sum_{n=1}^{\infty}\frac{\chi(n)}{n^s}$ the L-series attached to a Dirichlet character χ and $L_n(s)=\prod_{\chi\in X(n+1)}L(s,\chi)$.*
Let $M_1(s)=\sqrt{\lambda(s)}$ and for $n\geq 2$, $M_n(s)=\prod_{\substack{\chi\in X(n)\\ \chi(-1)=1}}L(s,\chi)$. Then

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

Now the product converges for $s=1$, then we have

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

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

The first values of C_n can be computed and we find

$$\begin{array}{lcllcl}
C_1 &=& 1.3728134628182460091\ldots & C_{10} &=& 8.0193434982306030482\ldots\\
C_2 &=& 2.6789638797482848821\ldots & C_{11} &=& 7.2245969049003170900\ldots\\
C_3 &=& 2.0927941299213300766\ldots & C_{12} &=& 8.4253498784241795332\ldots\\
C_4 &=& 3.6714321229370805403\ldots & C_{13} &=& 8.4678857199473387694\ldots\\
C_5 &=& 3.6129244862406263646\ldots & C_{14} &=& 8.0096845351535704233\ldots\\
C_6 &=& 3.9427412953667399868\ldots & C_{15} &=& 5.8026588347082479139\ldots\\
C_7 &=& 3.1089645815159960953\ldots & C_{16} &=& 11.195714229391949614\ldots\\
C_8 &=& 7.4348059978748568638\ldots & C_{17} &=& 11.004300588768807590\ldots\\
C_9 &=& 7.4890662797425630490\ldots & C_{18} &=& 13.007846372684611221\ldots
\end{array}$$

Number of pairs of generalized Fermat prime numbers

Let n and a be positive integers, $f_1(x)=x^{2^n}+1$ and $f_2(x)=(x+a)^{2^n}+1$.
The expected number of pairs of generalized Fermat primes $b^{2^n}+1$ and $(b+a)^{2^n}+1$ for $2\leq b\leq x$ is

$$\pi_n(x,a)\sim\frac{C_n(a)}{2^{2n}}\int_2^x\frac{dt}{(\log t)^2}.$$

$w_n(p,a)$ is the number of solutions to $f_1(x)f_2(x)\equiv 0 \pmod p$ therefore

$$\begin{array}{rl}
w_n(p,a)=1 & \text{if } p=2,\\
2^n\leq w_n(p,a)\leq 2^{n+1} & \text{if } p\equiv 1 \pmod{2^{n+1}},\\
w_n(p,a)=0 & \text{otherwise.}
\end{array}$$

Let $W_n(a)\geq 1$ be the weight of a

$$W_n(a)=\prod_{p\equiv 1\ (2^{n+1})}\frac{1-w_n(p,a)/p}{1-2^{n+1}/p}.$$

We have

$$C_n(a)=W_n(a)\,D_n$$

where

$$D_n = 2\prod_{p \text{ odd}} \frac{1-c_n(p)/p}{(1-1/p)^2},$$

and

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

The convergence acceleration method can be applied to D_n and so

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

The constants D_n can be calculated to high precision except for $n = 7$ or $n = 15$. Because of the Fermat prime 2^8+1 and $2^{16}+1$ the rate of convergence of these products is far lower.

$$\begin{array}{lcllcl} D_1 &=& 1.9504911124462870744\ldots & D_8 &=& 109.99349348086997411\ldots \\ D_2 &=& 12.675331810680666700\ldots & D_9 &=& 111.24509446878642902\ldots \\ D_3 &=& 1.7979764627538123244\ldots & D_{10} &=& 126.76821782480192241\ldots \\ D_4 &=& 25.368885312599632538\ldots & D_{11} &=& 99.459383993302618684\ldots \\ D_5 &=& 24.123978296128236459\ldots & D_{12} &=& 138.95762655939650111\ldots \\ D_6 &=& 26.874332041882684906\ldots & D_{13} &=& 138.60142305291187428\ldots \\ D_7 &=& 0.28557\ldots & D_{14} &=& 112.37182014055967024\ldots \end{array}$$

Number of pairs of primes of the form b^2+1

We consider $n = 1$. Let x_0, x_1 be the solutions to $x^2+1 \equiv 0 \pmod{p}$ such that $x_0 < p/2$ and $x_2 = x_0 - a$, $x_3 = x_1 - a$ the solutions to $(x+a)^2+1 \equiv 0 \pmod{p}$.

$x_0 = x_2 \Leftrightarrow p \mid a$ and $x_1 = x_3$.
$x_0 = x_3 \Leftrightarrow a \equiv -2x_0 \pmod{p}$ and $x_2 \equiv -3x_1 \pmod{p}$.
$x_1 = x_2 \Leftrightarrow a \equiv 2x_0 \pmod{p}$ and $x_3 \equiv -3x_0 \pmod{p}$.

Since a is even and $x_0^2+1 \equiv 0 \pmod{p}$, we have
$a \equiv \pm 2x_0 \pmod{p} \Leftrightarrow a^2+4 \equiv 0 \pmod{p}$.
Thus

$$w_1(p,a) = \begin{cases} 2 & \text{if } p \mid a, \\ 3 & \text{if } p \mid a^2+4, \\ 4 & \text{otherwise.} \end{cases}$$

$W_1(a)$ is a rational number that can be calculated with the prime factors $p = 4k+1$ of a and a^2+4:

a	$p \mid a$	$p \mid a^2+4$	$W_1(a)$	$W_1(a) \approx$
2	-	-	1	1.0000
4	-	5	2	2.0000
6	-	5	2	2.0000
8	-	17	14/13	1.0769
10	5	13	10/3	3.3333
12	-	37	34/33	1.0303
14	-	5	2	2.0000
16	-	5, 13	20/9	2.2222
18	-	41	38/37	1.0270
20	5	101	294/97	3.0309
2210	5, 13, 17	181, 3373	32992300/7752069	4.2559

Number of pairs of primes of the form $b^4 + 1$

We consider $n = 2$. Let x_0, x_1, x_2, x_3 be the solutions to $x^4 + 1 \equiv 0 \pmod{p}$ such that $x_1 = x_0^3 \bmod p$, $x_2 = x_0^5 \bmod p = -x_0$ and $x_3 = x_0^7 \bmod p = -x_1$. And let $x_4 = x_0 - a$, $x_5 = x_1 - a$, $x_6 = x_2 - a$ and $x_7 = x_3 - a$ be the solutions to $(x+a)^4 + 1 \equiv 0 \pmod{p}$.

The following table indicates the expression of y such that $a \equiv y \pmod{p}$ if $x_i = x_j$.

	x_4	x_5	x_6	x_7
x_0	0	$x_0^3 - x_0$	$-2x_0$	$-x_0^3 - x_0$
x_1	$-x_0^3 + x_0$	0	$-x_0^3 - x_0$	$-2x_0^3$
x_2	$2x_0$	$x_0^3 + x_0$	0	$-x_0^3 + x_0$
x_3	$x_0^3 + x_0$	$2x_0^3$	$x_0^3 - x_0$	0

Since a is even and $x_0^4 + 1 \equiv 0 \pmod{p}$ we have
$a \equiv \pm 2x_0 \pmod{p} \Leftrightarrow a^4 + 16 \equiv 0 \pmod{p}$,
$a \equiv \pm\left(x_0^3 + x_0\right) \pmod{p} \Leftrightarrow a^2 + 2 \equiv 0 \pmod{p}$,
$a \equiv \pm\left(x_0^3 - x_0\right) \pmod{p} \Leftrightarrow a^2 - 2 \equiv 0 \pmod{p}$.
Thus

$$w_2(p,a) = \begin{cases} 4 & \text{if } p \mid a, \\ 6 & \text{if } p \mid a^2 \pm 2, \\ 7 & \text{if } p \mid a^4 + 16, \\ 8 & \text{otherwise.} \end{cases}$$

$W_2(a)$ is a rational number that can be calculated with the prime factors $p = 8k + 1$ of a, $a^2 \pm 2$ and $a^4 + 16$:

a	$p \mid a$	$p \mid a^2-2$	$p \mid a^2+2$	$p \mid a^4+16$	$W_2(a)$	$W_2(a) \approx$
2	-	-	-	-	1	1.0000
4	-	-	-	17	10/9	1.1111
6	-	17	-	41	34/27	1.2593
8	-	-	-	257	250/249	1.0040
10	-	-	17	313	374/305	1.2262
12	-	-	73	1297	17286/16757	1.0316
34	17	577	193	41761	$\frac{19319589718}{13185388635}$	1.4652

Number of pairs of primes of the form $b^8 + 1$

We consider $n = 3$. Let $x_0, x_1, \cdots, x_7$ be the solutions to $x^8 + 1 \equiv 0 \pmod p$ such that $x_k = x_0^{2k+1} \bmod p$ and $x_{k+8} = x_k - a$ the height solutions to $(x+a)^8 + 1 \equiv 0 \pmod p$.

If $0 \le i, j < 8$ and $x_i = x_{8+j}$, we have $x_0^{2i+1} \equiv x_0^{2j+1} - a \pmod p$. Because $x_0^8 \equiv -1 \pmod p$ we have $x_0^{k+8} \equiv -x_0^k \pmod p$ and $(x_0^5 \pm x_0^3)^2 \equiv -(x_0 \mp x_0^7)^2 \pmod p$, $(x_0^7 \pm x_0^5)^2 \equiv -(x_0^3 \pm x_0)^2 \pmod p$. Then the set of relations is

$a^2 \equiv \{0\,;\, 4x_0^2\,;\, (x_0^3 \pm x_0)^2\,;\, (x_0^5 \pm x_0)^2\,;\, (x_0^7 \pm x_0)^2\,;\, (x_0^7 \pm x_0^3)^2\} \pmod p$.

If we eliminate x_0 we find that p must divide one of the elements of the list a, $a^8 + 256$, $a^8 + 16$, $a^8 + 12a^4 + 4$ and $a^8 - 12a^4 + 4$.

If p divides more than one element $w_3(p, a)$ must be evaluated. Otherwise we have

$$w_3(p,a) = \begin{cases} 8 & \text{if } p \mid a, \\ 14 & \text{if } p \mid a^8+16 \quad \text{or} \quad p \mid a^8 \pm 12a^4 + 4, \\ 15 & \text{if } p \mid a^8 + 256, \\ 16 & \text{otherwise.} \end{cases}$$

$W_3(a)$ is a rational number that can be calculated with the prime factors $p = 16k + 1$ of a, $a^8 + 16$, $a^8 \pm 12a^4 + 4$ and $a^8 + 256$:

a	$p \mid a$	$p \mid a^8+16$	$p \mid a^8-12a^4+4$	$p \mid a^8+12a^4+4$	$p \mid a^8+256$	$W_3(a)$
2	-	17	17	113	-	495/97
4	-	17, 241	97	17, 1009	257	$\frac{907344878}{174459177}$

17 is a Fermat prime and $w_3(17, a) < 16$: $(a^8 - 12a^4 + 4)(a^8 + 12a^4 + 4) \equiv a^{16} - 1 \pmod{17}$. Then if $a \not\equiv 0$, 17 divides $a^8 - 12a^4 + 4$ or $a^8 + 12a^4 + 4$. $(a^8 + 16)(a^8 + 256) \equiv a^{16} - 1 \pmod{17}$. Then if $a \not\equiv 0$, 17 divides $a^8 + 16$ or $a^8 + 256$.
We can check that

$$w_3(17,a) = \begin{cases} 8 & \text{if } \left(\frac{a}{17}\right) = 0, \\ 12 & \text{if } \left(\frac{a}{17}\right) = 1, \\ 13 & \text{if } \left(\frac{a}{17}\right) = -1. \end{cases}$$

Because $\frac{1-13/17}{1-16/17} = 4$ we have $W_3(a) \ge 4$.

Generalisation

Let x_0, $x_1, \cdots, x_{2^n-1}$ be the solutions to $x^{2^n}+1 \equiv 0 \pmod p$ such that $x_k = x_0^{2k+1} \bmod p$ and $x_{k+2^n} = x_k - a$ the 2^n solutions to $(x+a)^{2^n}+1 \equiv 0 \pmod p$.

If $0 \le i, j < 2^n$ and $x_i = x_{2^n+j}$, we have $x_0^{2i+1} \equiv x_0^{2j+1} - a \pmod p$. Using $x_0^{2^n} \equiv -1 \pmod p$ we can eliminate x_0 and we obtain a finite list of polynomials $P(a)$ such that $\deg(P(a)) \le 2^n$. Let $Q(a)$ be their product. We have $w_n(p,a) < 2^{n+1} \Leftrightarrow p \mid Q(a)$.
Hence $W_n(a)$ is a rational number and

$$W_n(a) = \prod_{p \mid Q(a)} \frac{1 - w_n(p,a)/p}{1 - 2^{n+1}/p}.$$

Number of gaps between generalized Fermat prime numbers

a is the gap following the generalized Fermat prime $b^{2^n}+1$ if and only if $(b+a)^{2^n}+1$ is prime and $(b+i)^{2^n}+1$ is composite for $b < i < b+a$. Then b and $b+a$ are a pair but this is not a sufficient condition.
The number of gaps can be calculated iteratively. In a fixed range, we compute the expected number of generalized Fermat primes N and the expected number of pairs $N_p(a)$. The number of gaps is equal to the number of pairs for $a = 2$ then $N_g(2) = N_p(2)$. These gaps are subtracted from N and we calculate $N(2) = N - N_g(2)$.
For $a = 4$ we have $N_g(4) = N_p(4) \cdot N(2)/N$ and $N(4) = N(2) - N_g(4)$. And more generally $N_g(a) = N_p(a) \cdot N(a-2)/N$ and $N(a) = N(a-2) - N_g(a)$.

References

[1] Soren Laing Aletheia-Zomlefer, Lenny Fukshansky and Stephan Ramon Garcia, *The Bateman-Horn Conjecture: Heuristics, History, and Applications*, arXiv: 1807.08899.

[2] P. T. Bateman and R. A. Horn, *A Heuristic Asymptotic Formula Concerning the Distribution of Prime Numbers*, Math. Comp. **16** (1962), 363–367.

[3] P. Moree, *private communication*, 2002.

[4] 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.

[5] D. Shanks, *On Numbers of the Form* $n^4 + 1$, Math. Comp. **15** (1961), 186–189.