Morehead-like restrictions on Fermat divisors

Ravi Fernando – fernando@berkeley.edu

September 3, 2019

1 Introduction

Let F_m denote the mth Fermat number $2^{2^m}+1$, and let p be any prime divisor of F_m. It is a well-known fact that if $m > 1$, then p has the form $k \cdot 2^n + 1$ for some odd k and $n \geq m+2$. Divisors of Fermat numbers are quite hard to find. To date, it is known that F_m is prime for $0 \leq m \leq 4$ and composite for 305 particular other values of m; among the composite ones, two have no known factors and the rest have a total of 349 known factors (listed in [6]), the largest being $(193 \cdot 2^{3329782}+1) | F_{3329780}$. Little else is known about the factorizations of Fermat numbers.

One often searches for Fermat divisors by first looking for prime numbers of the form $p = k \cdot 2^n + 1$ with k reasonably small, and then testing whether these primes divide a Fermat number. This property is easy to check: a prime p divides F_m if and only if the multiplicative order of 2 modulo p is exactly 2^{m+1}; this can be tested with m successive squarings modulo p. In particular, p divides some unspecified Fermat number if and only if the order of 2 modulo p is a power of 2, which happens if and only if 2 is a kth power mod p. Exactly 2^n of the $k \cdot 2^n$ nonzero residues mod p have this property, so a rough heuristic suggests that among primes $p = k \cdot 2^n + 1$ for fixed k, about one out of k should be Fermat divisors.

In 1906, Morehead ([7]) discovered some more subtle behavior for $k = 3$, namely that a prime $p = 3 \cdot 2^n + 1$ with n even cannot be a Fermat divisor. Primes of this form with n odd do seem to follow the 1/3 heuristic, so the true probability of $p = 3 \cdot 2^n + 1$ dividing a Fermat number should be closer to 1/6.[1] Indeed, of the 49 known primes $p = 3 \cdot 2^n + 1$, n is odd in 21 cases, and eight of these are Fermat divisors.

The purpose of this note is to document as many corrections to the $1/k$ heuristic as possible. For some values of k, we will be able to prove Morehead-like results preventing certain primes from being Fermat divisors; for other k, we will state heuristics suggesting some other nonzero probability. We summarize these results in Heuristic 8.1.

Notation. We will always let p denote a prime, and k and n will be the unique integers such that k is odd and $p = k \cdot 2^n + 1$. We will assume throughout that $k > 1$, since a prime $p = 2^n + 1$ is necessarily either a Fermat prime or 2.

[1] A warning though: it's probably not true that half of such primes have n odd, since congruence conditions on n affect the divisibility properties of p. For example, $3 \cdot 2^n + 1$ is divisible by 5 if and only if $n \equiv 3 \pmod 4$.

Acknowledgements. I was introduced to this question by Yves Gallot and Jeppe Stig Nielsen in the context of the distributed computing project PrimeGrid. They also directed me to several of the references and provided other useful comments; Yves in particular provided a large amount of data that has proved useful in making predictions. It is my pleasure to thank both them and the PrimeGrid community.

2 The case of perfect powers

Before discussing Morehead's result, we first mention a more elementary correction to the $1/k$ heuristic for certain perfect powers k.

Lemma 2.1. *As always, let $p = k \cdot 2^n + 1$ be a prime with k odd. Suppose $k = d^{q^m}$, where q is a prime, d is divisible by q, and $m \geq 0$. Then 2 is a q^m-th power modulo p.*

Proof. By definition, we have $d^{q^m} \cdot 2^n \equiv -1 \pmod{p}$. Since q is necessarily odd, -1 is a q^m-th power mod p, so 2^n is as well. But n is not divisible by q: if it were, then p would be a sum of qth powers $(d^{q^{m-1}} 2^{n/q})^q + 1$ and would therefore have the proper factor $d^{q^{m-1}} 2^{n/q} + 1$. This implies that 2 is also a q^m-th power mod p; one way to see this is as follows.

Being a q^m-th power in $\mathbb{Z}/p\mathbb{Z}$ is equivalent to being a $\frac{p-1}{q^m}$-th root of unity. We know that 2^n is a q^m-th power, so $(2^n)^{(p-1)/q^m} \equiv 1 \pmod{p}$, and so the order of 2 mod p divides $n(p-1)/q^m$. But it also divides $p-1$, so it divides $\gcd(n(p-1)/q^m, p-1) = (p-1)/q^m$. So 2 is a q^m-th power. □

Exactly $\frac{p-1}{q^m}$ of the nonzero residues mod p are q^m-th powers,[2] and all elements with power-of-2 order are among them. This suggests that such primes p are q^m times more likely to be Fermat divisors than the $1/k$ heuristic would suggest. This correction can be applied simultaneously for multiple different primes q, leading to the following improved heuristic.

Heuristic 2.2. (Perfect power correction) Suppose $k = d^m$, where d is odd and not itself a perfect power. Factor m as $\prod_i p_i^{e_i} \cdot \prod_j q_j^{f_j}$, where the primes p_i do not divide d and the primes q_j do. Then the probability that a given prime $p = k \cdot 2^n + 1$ is a Fermat divisor should be $\frac{\prod_j q_j^{f_j}}{k}$.

This heuristic predicts, for example, that primes with $k = 3^3 = 27$ have a $1/9$ chance of being Fermat divisors, and primes with $k = 5^5 = 3125$ have a $1/5^4 = 1/625$ chance. We will have more to say about $k = 27$ later, but for now we remark that there are three known Fermat divisors with these values of k: $(3125 \cdot 2^{149} + 1) | F_{147}$, $(27 \cdot 2^{455} + 1) | F_{452}$, and $(27 \cdot 2^{672007} + 1) | F_{672005}$.

3 Reminders on cubic reciprocity

Most of our remaining results will rely on the law of cubic reciprocity, so for easy reference we now collect a few statements of cubic reciprocity in the forms in which it will be used.

[2] It is worth mentioning here that $k = d^{q^m}$ is divisible by q^m, and even by q^{m+1}, as the exponent q^m is greater than or equal to $m + 1$.

Our basic reference for statements of cubic reciprocity is [2], §4A. Note that we follow Cox's definition that a prime $\pi \in \mathbb{Z}[\omega]$ is primary if $\pi \equiv \pm 1 \pmod 3$; this differs from [4] and some other sources, which require $\pi \equiv -1 \pmod 3$.

The law of cubic reciprocity takes place in the ring of Eisenstein integers $\mathbb{Z}[\omega]$; here ω is the cube root of unity $e^{2\pi i/3} = \frac{-1+\sqrt{-3}}{2}$, which satisfies the equation $\omega^2 + \omega + 1 = 0$. The following lemmas follow easily from Theorem 4.12 and the supplement (4.13) in [2].

Lemma 3.1. *Let π be an Eisenstein prime relatively prime to 3. Assume that $\pi \equiv 1 \pmod 2$. Then 2 is a cube modulo π if and only if π is primary.*

Proof. Since π is relatively prime to 3, there is a unique $\zeta \in \{1, \omega, \omega^2\}$ such that $\zeta\pi$ is primary; fix this ζ. Since $\pi \equiv 1 \pmod 2$, we have $N(\zeta\pi) = N(\pi) \neq N(2)$. Then by cubic reciprocity, 2 is a cube in $\mathbb{Z}[\omega]/(\pi) = \mathbb{Z}[\omega]/(\zeta\pi)$ if and only if $\zeta\pi$ is a cube in $\mathbb{Z}[\omega]/(2)$. Since π is a cube modulo 2, this happens if and only if ζ is a cube mod 2. But 1 is a cube in $\mathbb{Z}[\omega]/(2)$, while ω and ω^2 are not. □

Remark: This is equivalent to Proposition 9.6.1 in [4]. A similar statement is true with 2 replaced by any primary Eisenstein prime ρ, provided that $\rho \nmid 3N(\pi)$ and $N(\rho) \not\equiv 1 \pmod 9$ (to ensure that ω and ω^2 are not cubes).

Lemma 3.2. *Suppose m is a positive integer not divisible by 3, and $\pi \in \mathbb{Z}[\omega]$ is a primary prime congruent to 1 modulo m. Then m is a cube modulo π.*

Proof. Factor m as a product $\prod_i \rho_i$, where each ρ_i is a primary prime. (Since m is a rational integer, no nontrivial roots of unity are needed in this factorization.) Then since π is congruent to 1 mod m, it is a cube mod each ρ_i, and it is relatively prime to each $N(\rho_i)$. By cubic reciprocity, it follows that each ρ_i is a cube mod π, so their product m is as well. □

Lemma 3.3. *Let $p = a^2 + 27b^2$ be prime, with $a, b \in \mathbb{Z}$. Then 3 is a cube mod p if and only if b is divisible by 3.*

Proof. First, a cannot be divisible by 3, so by replacing a by $\pm a$ we may assume that $a = 3c-1$ for some $c \in \mathbb{Z}$. Then p factors over the Eisenstein integers as $p = \pi\overline{\pi}$, where π is the primary prime

$$\pi = a + 3b\sqrt{-3} = a + 3b(1+2\omega) = (-1+3c+3b) + 6b\omega. \tag{1}$$

The supplements to cubic reciprocity ([2], 4.13) imply that the cubic residue symbol of $3 = -\omega^2(1-\omega)^2$ mod π is:

$$\begin{aligned} \left(\frac{3}{\pi}\right)_3 &= \left(\frac{-1}{\pi}\right)_3 \cdot \left(\frac{\omega}{\pi}\right)_3^2 \cdot \left(\frac{1-\omega}{\pi}\right)_3^2 && (2)\\ &= 1 \cdot \omega^{2(c+3b)} \cdot \omega^{4(c+b)} && (3)\\ &= \omega^{6c+10b} = \omega^b. && (4) \end{aligned}$$

So 3 is a cube in $\mathbb{Z}[\omega]/(\pi)$, or equivalently in $\mathbb{Z}/p\mathbb{Z}$, if and only if b is divisible by 3. □

4 The case $k = 3d^2$

We now turn to Morehead's theorem. It has been observed by Golomb ([3], §4) and Suyama ([9]) that Morehead's result generalizes to integers $k = 3d^2$ provided that d is not divisible by 3. For completeness, we give the proof, which is essentially a translation of Morehead's original argument into more modern language.

Theorem 4.1. *Suppose $p = k \cdot 2^n + 1$ is prime, where n is even and $k = 3d^2$. Then 2 is a cube modulo p if and only if d is divisible by 3. In particular, if d is not divisible by 3, then p cannot divide a Fermat number.*

Proof. Let p be as above, and set $m = n/2$. Recall that p divides a Fermat number if and only if 2 is a kth power modulo p. Since k is a divisible by 3, a necessary condition for this is that 2 must be a cube mod p. We will check whether this is true using cubic reciprocity combined with an understanding of how p splits in $\mathbb{Z}[\omega]$.

We have $p = 1 + 3(d \cdot 2^m)^2 = (1 + d \cdot 2^m\sqrt{-3})(1 - d \cdot 2^m\sqrt{-3})$, where $\sqrt{-3} = 1 + 2\omega \in \mathbb{Z}[\omega]$. Call these two factors π and $\overline{\pi}$ respectively. Notice that $\pi \equiv 1 \pmod 2$, since $m > 0$. By Lemma 3.1, it follows that 2 is a cube in $\mathbb{Z}/p\mathbb{Z} = \mathbb{Z}[\omega]/(\pi)$ if and only if π is primary. But π is congruent to 1 modulo $\sqrt{-3}$, so it is primary if and only if it is congruent to 1 modulo 3. This happens if and only if $3|d$. □

When d is divisible by 3, this does not determine whether 2 is a kth power, and in particular whether p divides a Fermat number.[3] In this case, we get the following heuristic:

Heuristic 4.2. (Cubic reciprocity correction) If $p = 3d^2 \cdot 2^{2m} + 1$ with d odd and divisible by 3, then the probability that p is a Fermat divisor should be the probability that a randomly chosen cube modulo p is a kth power, namely $3/k = 1/d^2$.

One can combine this correction in the obvious way with the perfect power correction for primes $q > 3$, for example when $k = 75^5$ and n is even. However, when the perfect power correction applies with $q = 3$, that already tells us that 2 is a cube mod p, so it subsumes the present correction. In §6, we will identify some more subtle behavior in this case.

5 The case $k = 9d^4$

Theorem 5.1. *Suppose $p = 9d^4 \cdot 2^n + 1$ is prime, where $n \equiv 2 \pmod 4$. Then 2 is a cube mod p if and only if d is divisible by 3. In particular, if $3 \nmid d$, then p is not a Fermat divisor.*

Proof. Set $n = 4m + 2$. In order to use cubic reciprocity, we take advantage of a different factorization in $\mathbb{Z}[\omega]$. Set

$$\pi = (1 - 3d^2 \cdot 2^{2m+1}) + 2^{m+1}d\sqrt{-3} \in \mathbb{Z}[\omega], \tag{5}$$

[3] Indeed, the prime number $243 \cdot 2^4 + 1 = 3889$ does not divide a Fermat number, while $243 \cdot 2^{495732} + 1$ divides F_{495728}.

and let $\overline{\pi}$ be its complex conjugate. Then one can check that $p = \pi\overline{\pi}$. We also have $\pi \equiv 1 \pmod 2$, so by Lemma 3.1 it follows that 2 is a cube modulo π if and only if π is primary. But π is congruent to 1 modulo $\sqrt{-3}$, so π is primary if and only if it is congruent to 1 modulo 3, which happens if and only if $3|d$. □

Remark 5.2. If $n \equiv 0 \pmod 4$ and $5 \nmid d$, then $9d^4 \cdot 2^n + 1$ cannot be prime, as it is divisible by 5. So the conclusion of Theorem 5.1 remains true under the hypothesis that n is even and d is divisible by neither 3 nor 5.

Aside. The factorization $p = \pi\overline{\pi}$ above is a special case of the aurifeuillean factorization $4x^4 + 1 = (2x^2 + 2x + 1)(2x^2 - 2x + 1)$. In a certain sense, it is a shadow of a factorization in the larger field $\mathbb{Q}(\zeta_{12}) = \mathbb{Q}(i, \sqrt{-3})$, and for this reason the proof of Theorem 5.1 may be regarded as an instance of dodecic (12th-degree) reciprocity rather than "only" cubic reciprocity.

To explain this, set $\rho = 1 + 2^m d(1 + i)\sqrt{-3} \in \mathbb{Q}(\zeta_{12})$. The norm of ρ is the product of its four algebraic conjugates:

$$\begin{aligned} N_{\mathbb{Q}(\zeta_{12})/\mathbb{Q}}(\rho) &= (1 + 2^m d(1 + i)\sqrt{-3})(1 + 2^m d(1 - i)\sqrt{-3}) \\ &\qquad (1 - 2^m d(1 + i)\sqrt{-3})(1 - 2^m d(1 - i)\sqrt{-3}) \qquad (6) \\ &= 1 + 9d^4 2^{4m+2} = p. \qquad (7) \end{aligned}$$

Combining the first two and last two terms (or equivalently norming down to $\mathbb{Q}(\sqrt{-3})$) recovers the factorization $p = \pi\overline{\pi}$. Similarly, combining terms in the other possible pairings yields the factorizations of p in $\mathbb{Q}(i)$ and $\mathbb{Q}(\sqrt{3})$:

$$\begin{aligned} p &= (1 + 3d^2 2^{2m+1} i)(1 - 3d^2 2^{2m+1} i) \qquad (8) \\ &= \left((1 + 2^{2m+1} \cdot 3d^2) - 2^{m+1} d\sqrt{3}\right)\left((1 + 2^{2m+1} \cdot 3d^2) + 2^{m+1} d\sqrt{3}\right). \qquad (9) \end{aligned}$$

When d is divisible by 3, Theorem 5.1 suggests the following heuristic:

Heuristic 5.3. (Dodecic reciprocity correction) If $p = 9d^4 \cdot 2^{4m+2} + 1$ with d odd and divisible by 3, then the probability that p is a Fermat divisor should be the probability that a randomly chosen cube modulo p is a kth power, namely $3/k = 1/3d^4$.

6 Overlap cases

In this section, we will take a closer look at the situations where more than one of our corrections apply to the same value of k. For convenience, we first introduce the following notation. Given a prime $p = k \cdot 2^n + 1$, we say that the "perfect power case" **PP** applies for some odd prime q if k is a q-th power that is divisible by q. We say that the "cubic reciprocity case" **CR** applies if n is even and k is 3 times a square, and we say that the "dodecic reciprocity case" **DR** applies if $n \equiv 2 \pmod 4$ and k is 9 times a fourth power.

Note that the cases **CR** and **DR** cannot overlap, as $3d^2$ is never a square and $9d^4$ always is. Moreover, both of these corrections are independent of the case **PP** for $q \neq 3$. So we will only need to study how the case **PP** with $q = 3$ interacts with **CR** and **DR**. In each case, we will prove an analogue of Morehead's result for a new infinite class of values of k, and we will state an improved heuristic in the remaining cases.

6.1 The case $k = 27d^6$

If the cases **PP** with $q = 3$ and **CR** apply simultaneously, then k must have the form $27d^6$ for some odd d. Our first result in this case is as follows.

Theorem 6.1.1. *Let p be a prime of the form $27d^6 2^n + 1$, where n is even and d is not divisible by 3. Then 2 is not a ninth power modulo p, and in particular p does not divide a Fermat number.*

Proof. Suppose for the sake of contradiction that 2 is a ninth power mod p. Then 2^n is as well, and so is $-1/2^n \equiv 27d^6$. Then at least one of the cube roots of $27d^6$ in $\mathbb{Z}/p\mathbb{Z}$ is a cube. But $\mathbb{Z}/p\mathbb{Z}$ has a full set of ninth roots of unity, so in fact all three cube roots are cubes, including in particular $3d^2$. Applying Lemma 3.2 with $\pi = 1 + 3d^3 2^{n/2}\sqrt{-3}$ and $m = d$ tells us that d is a cube in $\mathbb{Z}[\omega]/(\pi) = \mathbb{Z}/p\mathbb{Z}$. But applying Lemma 3.3 with $a = 1$ and $b = d^3 2^{n/2}$ tells us that 3 is not a cube. This is a contradiction. $\square$

To state our next correction, we record a converse of sorts to Theorem 6.1.1:

Proposition 6.1.2. *Suppose $p = k \cdot 2^n + 1$ is a prime with $k = (3d^2)^{3^s}$ and n even, where $d, s \geq 1$. Suppose also that either $3|d$ or $s > 1$. Then 2 is a 3^{s+1}-st power mod p.*

Proof. By construction, $k = 3^{3^s} d^{2\cdot 3^s}$ can be expressed as $27c^2$, where $c = 3^{(3^s-3)/2} d^{3^s}$. The condition that either $3|d$ or $s > 1$ means that c is a multiple of 3. So Lemma 3.3 with $a = 1$ and $b = c \cdot 2^{n/2}$ tells us that 3 is a cube mod p, and as before Lemma 3.2 tells us that d is as well. Thus $3d^2$ is a cube, and so k is a 3^{s+1}-st power. We have $2^n \equiv -1/k \pmod{p}$ by the definition of p, so 2^n is also a 3^{s+1}-st power, and as in the proof of Lemma 2.1 it follows that 2 is as well. $\square$

Heuristic 6.1.3. (Hybrid perfect power-cubic reciprocity correction) If $p = 27d^6 2^n + 1$ where n is even and d is divisible by 3, the probability that p divides a Fermat number should be three times the probability given by the perfect power correction.

The reason for this is that Proposition 6.1.2 applies under these hypotheses, and it gives us one more power of 3 than Lemma 2.1 did.

6.2 The case $k = 729d^{12}$

If the cases **PP** with $q = 3$ and **DR** apply simultaneously, then k must have the form $729d^{12}$ for some odd d. In this case we will be able to imitate all of our results for $k = 27d^6$. The proofs will be similar.

Theorem 6.2.1. *Suppose $p = k \cdot 2^n + 1$ is a prime with $k = 729d^{12}$ and $n = 4m + 2$, where d is not divisible by 3. Then 2 is not a ninth power mod p, and in particular p is not a Fermat divisor.*

Proof. Suppose for the sake of contradiction that 2 is a ninth power mod p. Then 2^n is as well, and so is $-1/2^n \equiv 729d^{12} \pmod{p}$. Then at least one of the cube roots of $729d^{12}$ in $\mathbb{Z}/p\mathbb{Z}$ is a cube. But $\mathbb{Z}/p\mathbb{Z}$ has a full set of ninth roots of unity, so in fact all three cube roots are cubes, including in particular $9d^4$.

Since $p = 9 \cdot (3d^3)^4$, the factorization (5) above takes the form $p = \pi\overline{\pi}$, where π is the primary prime

$$\pi = (1 - 27d^6 \cdot 2^{2m+1}) + 2^{m+1} \cdot 3d^3\sqrt{-3}. \tag{10}$$

Applying Lemma 3.2 with this π and $m = d$ tells us that d is a cube in $\mathbb{Z}[\omega]/(\pi) = \mathbb{Z}/p\mathbb{Z}$. But applying Lemma 3.3 with $a = 1 - 27d^6 \cdot 2^{2m+1}$ and $b = 2^{m+1} \cdot d^3$ tells us that 3 is not a cube. It follows that d^4 is a cube but 9 is not, which contradicts the fact that $9d^4$ is a cube. □

As before, we have a "converse" proposition which leads to an improved heuristic when $3|d$:

Proposition 6.2.2. *Suppose $p = k \cdot 2^n + 1$ is a prime with $k = (9d^4)^{3^s}$ and $n = 4m + 2$, where $d, s \geq 1$. Suppose also that either $3|d$ or $s > 1$. Then 2 is a 3^{s+1}-st power mod p.*

Proof. We first rewrite k as $729c^4$, where $c = 3^{(3^s-3)/2}d^{3^s}$. Then the factorization (5) takes the form $p = \pi\overline{\pi}$, where π is the primary prime

$$\pi = (1 - 27c^2 \cdot 2^{2m+1}) + 2^{m+1} \cdot 3c\sqrt{-3}. \tag{11}$$

In particular, we have $p = a^2 + 27b^2$ with $a = 1 - 27c^2 \cdot 2^{2m+1}$ and $b = 2^{m+1}c$; notice that the condition that $3|d$ or $s > 1$ implies that $3|c$ and therefore $3|b$. By Lemma 3.3, it follows that 3 is a cube mod p. By Lemma 3.2, d is as well. So $9d^4$ is a cube mod p, and therefore $k = (9d^4)^{3^s}$ is a 3^{s+1}-st power. Then modulo p we have $2^n \equiv -1/k$, so 2^n is also a 3^{s+1}-st power. But as before, n cannot be divisible by 3, since if it were then p would be a sum of cubes and would therefore be composite. It follows that 2 is a 3^{s+1}-st power modulo p, as desired. □

Heuristic 6.2.3. (Hybrid perfect power-dodecic reciprocity correction) If $p = 729d^{12}2^n + 1$ where $n \equiv 2 \pmod{4}$ and d is divisible by 3, the probability that p divides a Fermat number should be three times the probability given by the perfect power correction.

7 Other reciprocity laws

In this section, we will argue that in a certain limited sense, the cubic and dodecic reciprocity methods we have used do not generalize to any other higher-degree reciprocity laws. Before making this precise, we attempt to briefly explain what makes the number 3 special.

The proof of Morehead's theorem relied on the convenient coincidence that $\mathbb{Q}(\sqrt{-3}) = \mathbb{Q}(\zeta_3)$. The former is where the primes $p = 3 \cdot 2^{2m} + 1$ factor algebraically, and the latter is where cubic reciprocity takes place. In order to mimic the proof for primes of some form $k \cdot 2^{am+b} + 1 = (k \cdot 2^b)(2^m)^a + 1$ with a, b, k fixed and m varying, we would need to be able to explicitly write down a prime divisor $\pi | p$ in some suitable cyclotomic field, where π has norm p.[4]

In general, we can factor $(k \cdot 2^b)(2^m)^a + 1$ by extracting a-th roots of $-k \cdot 2^b$, but the field $\mathbb{Q}(\sqrt[a]{-k \cdot 2^b})$ will typically have little to do with $\mathbb{Q}(\zeta_k)$. Besides $\mathbb{Q}(\sqrt{-3}) = \mathbb{Q}(\zeta_3)$, however, there is also the curious equality of fields $\mathbb{Q}(\sqrt[4]{-36}) = \mathbb{Q}(\zeta_{12})$. This gives rise to the dodecic reciprocity argument for primes of the form $p = 36d^4 2^{4m} + 1 = 9d^4 2^{4m+2} + 1$.

We now specify what kind of generalization we would like. Suppose we are given an odd integer k and a congruence condition $n \equiv b \pmod{a}$, and we want to study whether primes $p = k \cdot 2^n + 1$ are Fermat divisors using degree-r Eisenstein reciprocity for some r. Recall that $p = k \cdot 2^n + 1$ is a Fermat divisor if and only if 2 is a k-th power modulo p, so degree-r reciprocity can only be useful if $\gcd(r, k) > 1$. Because k is odd, this implies that r is not a power of 2.

Since degree-r reciprocity takes place in the cyclotomic integer ring $\mathbb{Z}[\zeta_r]$, $\zeta_r = e^{2\pi i/r}$, we would like to be able to factor our primes algebraically in this ring. By "factoring" we mean exhibiting a prime element $\pi \in \mathbb{Z}[\zeta_r]$ with

$$N(\pi) = \prod_{\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_r)/\mathbb{Q})} \sigma(\pi) = p, \tag{12}$$

so that $\mathbb{Z}[\zeta_r]/(\pi) = \mathbb{Z}/p\mathbb{Z}$. By "algebraically" we mean that this factorization should be given by polynomials that are uniform across all $n \equiv b \pmod{a}$.

More precisely, let $f(x)$ be the polynomial $Nx^a + 1$, where N is the positive integer $k \cdot 2^b$. Then the prime candidates $p = k \cdot 2^{am+b} + 1 = (k \cdot 2^b)(2^m)^a + 1$ are the values of $f(x)$ at $x = 2^m$. We assume that $f(x)$ is irreducible, as otherwise at most finitely many of its values will be prime. We want to have a polynomial $g(x) \in \mathbb{Z}[\zeta_r][x]$ such that

$$\prod_{\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_r)/\mathbb{Q})} g^\sigma(x) = f(x), \tag{13}$$

where g^σ denotes the polynomial g with coefficients twisted by σ. (This product can be interpreted as the norm in the extension of function fields $\mathbb{Q}(\zeta_r, x)/\mathbb{Q}(x)$.) Then we could recover π as $g(2^m)$. Notice that this algebraic integer π necessarily generates the field $\mathbb{Q}(\zeta_r)$, since otherwise its norm p would be a perfect power.

The following conditions seem to be necessary to give us a generalization of Morehead's theorem. The first condition makes it possible (but does not guarantee) that infinitely many p are prime; the second gives an explicit factorization of p in $\mathbb{Q}(\zeta_r)$, so that degree-r Eisenstein reciprocity can be used; and the third ensures that the r-th power character of 2 modulo p provides information about its k-th power character.

Question 7.1. *For what triples of positive integers (r, a, N) do the following conditions hold?*

[4] Class field theory guarantees the existence of an ideal of norm p—and $\mathbb{Q}(\zeta_r)$ has class number 1 for some small r, making this ideal principal—but we really need to be able to write π down.

1. *The polynomial $f(x) = Nx^a + 1$ is irreducible over $\mathbb{Q}$.*
2. *There exists a polynomial $g(x) \in \mathbb{Q}(\zeta_r)[x]$ such that $\prod_{\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_r)/\mathbb{Q})} g^\sigma(x) = f(x)$.*
3. *The integers r and N have a nontrivial odd common factor.*

We will answer this question only in the case where the polynomial $g(x)$ is linear. In this situation, we can essentially say what $g(x)$ is: since the roots of $f(x)$ are the a-th roots of $-1/N$, it follows that (up to scaling and choice of a root) we have $g(x) = 1 - \sqrt[a]{-N}x$. Since the field $\mathbb{Q}(\zeta_r)$ is generated by $g(2^m) = 1 - \sqrt[a]{-N} \cdot 2^m$ for some m, it follows that it is also generated by the single element $\sqrt[a]{-N}$. We now claim that this almost never happens:

Proposition 7.2. *Suppose r, a, and N are positive integers such that the polynomial $f(x) = Nx^a + 1$ is irreducible over $\mathbb{Q}$, r is not a power of 2, and the field $K = \mathbb{Q}(\zeta_r)$ is generated by a single a-th root of $-N$. Then we must have $(r, a, N) = (3, 2, 3d^2), (6, 2, 3d^2)$, or $(12, 4, 36d^4)$ for some d.*

Proof. First we assume that r is even, which sacrifices no generality because we have $\mathbb{Q}(\zeta_r) = \mathbb{Q}(\zeta_{2r})$ when r is odd. (In particular, the cases $r = 3$ and $r = 6$ both correspond to cubic reciprocity, and the case $r = 12$ corresponds to dodecic reciprocity.) Calculating the degree $[K : \mathbb{Q}]$ in two ways gives us $\varphi(r) = a$, where φ is Euler's totient. Since K is Galois over $\mathbb{Q}$, it must contain all of the a-th roots of $-N$, and by dividing these it must contain all a-th roots of unity. So we have $\mathbb{Q}(\zeta_a) \subseteq \mathbb{Q}(\zeta_r)$. Since $\mathbb{Q}(\zeta_r)$ contains only r roots of unity (this uses our assumption that r is even), we have $a|r$. So in fact r is divisible by $\varphi(r)$.

We claim that the condition $\varphi(r)|r$ implies that r is not divisible by any primes other than 2 and 3. To prove this, suppose r has prime factorization $\prod_i q_i^{e_i}$, and recall that $\varphi(r) = r \cdot \prod_i \frac{q_i - 1}{q_i}$. The given condition implies that the ratio $\frac{r}{\varphi(r)} = \prod_i \frac{q_i}{q_i - 1}$ is an integer. The numerator of this fraction is squarefree, so the denominator must not be divisible by 4. But every odd q_i contributes at least a factor of 2 to the denominator, so there can be at most one odd q_i. If there is such an odd prime q, then the denominator $q - 1$ must divide $2q$. Since $q - 1$ is coprime to q, it must also divide 2, and so $q = 3$.

We now know that r can be divisible by only the two primes 2 and 3, and since it is even and not a power of 2 it must be divisible by both. So $a = \varphi(r) = r/3$. Next we suppose that $3|a$. In this case, if N is a cube, then $Nx^a + 1$ is a sum of cubes and therefore reducible. But if N is not a cube, then $K = \mathbb{Q}(\sqrt[a]{-N})$ contains $\mathbb{Q}(\sqrt[3]{-N})$, which is not Galois because it has one real and two complex embeddings. This implies that it cannot be contained in the abelian number field K, which is a contradiction. So we must not have $3|a$. This leaves us with the case where a is a power of 2 and $r = 3a$.

Say $a = 2^t$ and $r = 3a$. We are given that $\sqrt[a]{-N}$ lies in $\mathbb{Q}(\zeta_r)$. But $\sqrt[a]{-N}$ is just $\sqrt[a]{N}$ multiplied by some primitive $2a$-th root of unity. It follows that $\sqrt[a]{N}$ lives in some cyclotomic field, namely the $\mathrm{lcm}(r, 2a)$-th. It is proved in [10] that a root higher than the second of an integer $N > 1$ can essentially never be in a cyclotomic field—namely, it cannot be in a cyclotomic field unless N is a perfect power and the root simplifies trivially. In our situation, it follows that

N must be a 2^{t-1}-st power. Moreover, if q is a prime such that q divides N and q^a does not, then q is ramified in $\mathbb{Q}(\sqrt[a]{-N}) = \mathbb{Q}(\zeta_r)$, so $q|r$ and thus $q = 2$ or 3. Since $\sqrt[a]{-d^a N}$ generates the same field as $\sqrt[a]{-N}$, we may now assume without loss of generality that $N = 1, 2^{t-1}, 3^{t-1}$, or 6^{t-1}. The upshot of this is that $\sqrt[a]{-N}$ appears in the following list:

$$\begin{aligned} \sqrt[a]{-N} &= \zeta_{2a}\sqrt[a]{N} && (14)\\ &\in \{\zeta_{2^{t+1}}, \zeta_{2^{t+1}}\sqrt{2}, \zeta_{2^{t+1}}\sqrt{3}, \zeta_{2^{t+1}}\sqrt{6}\}. && (15)\end{aligned}$$

Now, $\zeta_{2^{t+1}}$ does not live in $\mathbb{Q}(\zeta_r)$. But $\sqrt{2}$, $\sqrt{3}$, and $\sqrt{6}$ are in $\mathbb{Q}(\zeta_{24})$, and therefore in $\mathbb{Q}(\zeta_r)$ if $t \geq 3$, because we have:

$$\begin{aligned} \sqrt{2} &= \zeta_8 + \zeta_8^{-1}, && (16)\\ \sqrt{3} &= \frac{\zeta_3 - \zeta_3^{-1}}{i}, \text{ and} && (17)\\ \sqrt{6} &= \sqrt{2}\cdot\sqrt{3}, && (18)\end{aligned}$$

for suitable choices of roots of unity. If $t \geq 3$, it follows that none of our four choices are in the desired field $\mathbb{Q}(\zeta_r)$, which is a contradiction. This forces $(r, a) = (6, 2)$ (which we recall is equivalent to $(3, 2)$) or $(12, 4)$. To complete the proof, we examine which N can appear in these two cases. Among the elements

$$\zeta_4, \zeta_4\sqrt{2}, \zeta_4\sqrt{3}, \zeta_4\sqrt{6}, \tag{19}$$

only $\zeta_4\sqrt{3} = \sqrt{-3}$ is in $\mathbb{Q}(\zeta_6) = \mathbb{Q}(\zeta_3)$. Similarly, among

$$\zeta_8, \zeta_8\sqrt{2}, \zeta_8\sqrt{3}, \zeta_8\sqrt{6}, \tag{20}$$

only $\zeta_8\sqrt{2} = \sqrt[4]{-4}$ and $\zeta_8\sqrt{6} = \sqrt[4]{-36}$ are in $\mathbb{Q}(\zeta_{12})$. The first of these does not satisfy our conditions because $f(x) = 4x^4 + 1$ factors as $(2x^2 + 2x + 1)(2x^2 - 2x + 1)$, but the second does. □

Remark 7.3. It may seem somewhat artificial for us to require r and N to share an *odd* factor in Question 7.1. In fact, degree-r reciprocity can still say something interesting about the order of 2 modulo p when r is a power of 2. But it will only tell us about how 2-divisible this order is. Accordingly, it would tell us about which Fermat numbers a given prime may divide, but not about whether it may divide one at all.

In fact, we have already alluded to an example of this: the proof that Fermat divisors $p = (k \cdot 2^n + 1)|F_m$ must satisfy $n \geq m + 2$ when $m > 1$ follows from a supplement to quadratic reciprocity. More generally, the triple $(r, a, N) = (2^{t+1}, 2^t, d^{2^t})$ for $t \geq 0$, $d \geq 1$ satisfies the first two conditions of Question 7.1, and this can tell us about the order of 2 modulo primes of the form $p = (d \cdot 2^m)^{2^t} + 1$.

8 Summary

We now collect all our results into one "master heuristic", which summarizes our corrections to the $1/k$ heuristic in the cases **PP**, **CR**, and **DR** defined in §6, as well as the various interactions between them.

Heuristic 8.1. Let $p = k \cdot 2^n + 1$ be a prime, with $k > 1$ odd. The probability that p is a Fermat divisor should be as follows:

- If none of **PP**, **CR**, and **DR** applies, then probability $1/k$.
- If only **PP** applies, then the probability given by Heuristic 2.2.
- If **CR** applies, then **DR** cannot. In this case:
    - If $27 \nmid k$, then p is not a Fermat divisor by Theorem 4.1.
    - Otherwise, if **PP** does not apply, then probability $3/k$ as in Heuristic 4.2.
    - If **PP** applies for some q but not for $q = 3$, then 3 times the result of Heuristic 2.2.
    - If **PP** applies for $q = 3$, then $k = 27d^6$ for some d. Then:
        - If $3 \nmid d$, then p is not a Fermat divisor by Theorem 6.1.1.
        - Otherwise, 3 times the result of Heuristic 2.2, according to Heuristic 6.1.3.
- If **DR** applies, then:
    - If $729 \nmid k$, then p is not a Fermat divisor by Theorem 5.1.
    - Otherwise, if **PP** does not apply, then probability $3/k$ as in Heuristic 5.3.
    - If **PP** applies for some q but not for $q = 3$, then 3 times the result of Heuristic 2.2.
    - If **PP** applies for $q = 3$, then $k = 729d^{12}$ for some d. Then:
        - If $3 \nmid d$, then p is not a Fermat divisor by Theorem 6.2.1.
        - Otherwise, 3 times the result of Heuristic 2.2, according to Heuristic 6.2.3.

Moreover, this probability should not depend on any congruence conditions on n beyond the conditions mod 2 and 4 in the definitions of the cases **CR** and **DR**.

We now ask whether the heuristic above is the best one possible; that is, whether it predicts the true proportion of Fermat divisors among the primes with a given k and a given congruence condition on n.

Question 8.2. *Fix a positive odd integer k and a congruence class $b \mod a$, with $4|a$. Suppose there exist infinitely many primes $k \cdot 2^n + 1$ with $n \equiv b \pmod a$. Does Heuristic 8.1 correctly predict the asymptotic proportion of these that are Fermat divisors?*

Remark 8.3. It seems extremely difficult to prove that there are infinitely many primes $p = k \cdot 2^n + 1$ for any single value of k, and we are not aware of any k for which this has been done. There are however infinitely many values of k, called Sierpiński numbers, for which there are no primes. It is also believed that there are only finitely many primes with $k = 1$, namely 2 and the five known Fermat primes.

9 Further directions

Most searches for Fermat divisors have been optimized according to the $1/k$ heuristic. That is, one estimates the probability that $k \cdot 2^n + 1$ is a prime Fermat divisor in terms of the prime number theorem and the $1/k$ heuristic, and one tests the ordered pairs (k, n) in order of largest expected payoff per unit computational cost. The corrections to the heuristic that we have discussed suggest some modifications to this way of searching for special values of k. For example, our heuristics predict that primes with $k = 27$ and n odd should have a $1/9$ chance of being Fermat divisors. So it may be worth searching more deeply for such primes, compared to other nearby values of k. It is apparently a lucky coincidence that numbers $27 \cdot 2^n + 1$, along with $27 \cdot 2^n - 1$ and $121 \cdot 2^n \pm 1$, have indeed been tested especially deeply.

Another interesting value of k is $3^9 = 19683$—the smallest k to which Heuristic 6.1.3 applies. Primes of the form $3^9 \cdot 2^n + 1$ should have a $1/3^7$ chance of being Fermat divisors when n is odd and $1/3^6$ when n is even. It is unclear how far the sequence $3^9 \cdot 2^n + 1$ has been tested for primality to date. A search using the program OpenPFGW shows that $3^9 \cdot 2^n + 1$ is prime for

$$n = 1, 5, 8, 32, 50, 400, 536, 592, 676, 866, 1157, 1300, 1661, 1730, 2440, 7046,\\ 9698, 16180, 16226, 22330, 26990, 206005, 238780, 278941,$$

and no other $n \leq 300000$. None of these are Fermat divisors. But it may be worth searching further.

It would be interesting to know if one can prove Morehead-like results for other values of k, either increasing or excluding the chance that certain primes are Fermat divisors. It has been observed, for example, that nine of the 25 known primes $p = 5 \cdot 2^n + 1$ are Fermat divisors, which is almost double the expected $1/5$ proportion. The likelihood of this happening by chance is about 4.7%. However, these Fermat divisors don't exhibit any obvious patterns modulo any small number, aside for the congruence conditions that are necessary for p to be prime. For example, both Fermat divisors and non-divisors appear among every permissible residue class mod 2, 3, 4, and 5.[5] So if there is a reason for the relative abundance of Fermat divisors with $k = 5$, it seems that it would have to be an entirely different reason from those discussed here.

Yves Gallot also reports some interesting behavior for $k = 25$ and 49. For $k = 25$, there are 28 primes with $n < 10^5$, and in only two cases is 2 even a fifth power modulo p. For $k = 49$, there are 19 primes with $n < 1.5 \cdot 10^6$, and 2 is not a seventh power modulo any of them. Each of these has around a 5% likelihood of happening by chance, and together they may suggest some more interesting behavior when $k = q^2$ for a prime $q > 3$.

When studying the statistics of Fermat divisors, one practical difficulty is that collecting more

[5] There are no primes $p = 5 \cdot 2^n + 1$ with n even or congruent to $2 \pmod 3$, and only the prime 11 with $n \equiv 1 \pmod 5$, because those congruence conditions imply that p is divisible by 3, 7, or 11 respectively. Looking at some slightly larger moduli, the two known primes with $n \equiv 2 \pmod 7$ are both Fermat divisors; and in the residue classes 3 mod 7, 6 mod 7, 4 mod 9, and 6 mod 9 there are respectively one, two, two, and three known primes but no Fermat divisors.

data requires finding prime numbers of the form $p = k \cdot 2^n + 1$, often with n very large. There are at least two distributed computing projects currently searching for such primes. PrimeGrid searches those with $3 \leq k \leq 9999$ and n in the millions, as well as primes of various other forms. FermatSearch searches specifically for Fermat divisors in a wide range of k- and n-values. We hope that the data produced by both of these projects will shed more light on the subject.

References

[1] Ray Ballinger and Wilfrid Keller, “List of primes $k \cdot 2^n + 1$ for $k < 300$”. Updated July 15, 2019. Available at `http://www.prothsearch.com/riesel1.html`.

[2] David A. Cox, *Primes of the Form* $x^2 + ny^2$ (2nd edition), 2013.

[3] Solomon W. Golomb, “Properties of the sequence $3 \cdot 2^n + 1$”. *Mathematics of Computation*, vol. 30, no. 135 (July 1976), 657-663.

[4] Kenneth Ireland and Michael Rosen, *A Classical Introduction to Modern Number Theory* (2nd edition), 1990.

[5] I. Jiménez Calvo, “A note on factors of generalized Fermat numbers”. *Applied Mathematics Letters* 13 (2000), 1-5.

[6] Wilfrid Keller, “Prime factors $k \cdot 2^n + 1$ of Fermat numbers F_m and complete factoring status”. Updated May 3, 2019. Available at `http://www.prothsearch.com/fermat.html`.

[7] J. C. Morehead, “Note on the factors of Fermat’s numbers”. *Bulletin of the American Mathematical Society*, vol. 12, no. 9 (June 1906), 449-451.

[8] OpenPFGW, developed by Chris Nash and Jim Fougeron, and maintained and improved by Mark Rodenkirch. Current version available at `https://sourceforge.net/projects/openpfgw/`.

[9] H. Suyama, “A note on the factors of Fermat numbers II”. *Abstracts of Papers Presented to the American Mathematical Society*, vol. 5 (1984), 132.

[10] Rajat Tandon, “Roots are not contained in cyclotomic fields”, *Resonance*, vol. 6, no. 4 (April 2001), 78-83.