LMS J. Comput. Math. 18 (1) (2015) 148–169
doi:10.1112/S1461157014000436

Squarefree values of trinomial discriminants

David W. Boyd, Greg Martin and Mark Thom

Abstract

The discriminant of a trinomial of the form $x^n \pm x^m \pm 1$ has the form $\pm n^n \pm (n-m)^{n-m}m^m$ if n and m are relatively prime. We investigate when these discriminants have nontrivial square factors. We explain various unlikely-seeming parametric families of square factors of these discriminant values: for example, when n is congruent to 2 (mod 6) we have that $((n^2-n+1)/3)^2$ always divides $n^n - (n-1)^{n-1}$. In addition, we discover many other square factors of these discriminants that do not fit into these parametric families. The set of primes whose squares can divide these sporadic values as n varies seems to be independent of m, and this set can be seen as a generalization of the Wieferich primes, those primes p such that 2^p is congruent to 2 (mod p^2). We provide heuristics for the density of these sporadic primes and the density of squarefree values of these trinomial discriminants.

1. *Introduction*

The prime factorization of the discriminant of a polynomial with integer coefficients encodes important arithmetic information about the polynomial, starting with distinguishing those finite fields in which the polynomial has repeated roots. One important datum, when the monic irreducible polynomial $f(x)$ has the algebraic root θ, is that the discriminant of $f(x)$ is a multiple of the discriminant of the number field $\mathbb{Q}(\theta)$, and in fact their quotient is the square of the index of $\mathbb{Z}[\theta]$ in the full ring of integers $\mathcal{O}$ of $\mathbb{Q}(\theta)$. In particular, if the discriminant of $f(x)$ is squarefree, then $\mathcal{O} = \mathbb{Z}[\theta]$ is generated by the powers of the single element θ (see [**2**, solution to Exercise 4.2.8, p. 210]) and is thus said to be 'monogenic'. (Of course the discriminant being squarefree is not necessary for the ring of integers to be monogenic; it is simply a convenient sufficient condition.) The rings of integers $\mathcal{O}$ in such fields are well suited to computation, all the more so when the polynomial $f(x)$ is particularly simple.

These considerations motivated us to consider trinomials such as $x^n - x - 1$, the discriminant of which (see Lemma 2.2) is $n^n + (-1)^n(n-1)^{n-1}$. Indeed, $x^n - x - 1$ is always irreducible (see Lemma 4.1), and its Galois group is always S_n [**13**, Theorem 1]. Lagarias [**8**] asked whether, for each positive integer n, there is an irreducible polynomial of degree n with Galois group S_n for which the ring of integers of the field generated by one of its roots is monogenic. By the above discussion, we can answer Lagarias's question in the affirmative for any integer $n \geqslant 2$ for which $n^n + (-1)^n(n-1)^{n-1}$ is squarefree. (As it happens, his question was answered positively for all n by Kedlaya [**7**], but by then our investigation into the squarefreeness of these values had yielded mathematics that was of independent interest.)

Most of the integers $n^n + (-1)^n(n-1)^{n-1}$ seem squarefree, but there are a few sporadic exceptions, the first being $130^{130} + 129^{129}$ which is divisible by 83^2; the other exceptions for $n \leqslant 1000$ are $n \in \{257, 487, 528, 815, 897\}$, each of which has $n^n + (-1)^n(n-1)^{n-1}$ divisible by 59^2. We remark that it is easy to test the other 994 values for divisibility by the squares of specific primes (and we have done so for the first 10 000 primes), making it extremely likely

Received 21 March 2014; revised 8 August 2014.

2010 Mathematics Subject Classification 11N32, 11N25, 11N05 (primary), 11R29 (secondary).

that they are indeed squarefree; but this sequence of integers grows so quickly that only the first few dozen values are verifiably squarefree. Nevertheless, we believe that the squarefree values in this sequence have a limiting density which we can calculate extremely accurately, despite the very limited data.

CONJECTURE 1.1. The set of positive integers n such that $n^n+(-1)^n(n-1)^{n-1}$ is squarefree has density $0.993\,446\,6\ldots$, correct to that many decimal places.

In Proposition 6.3 we obtain the rigorous upper bound $0.993\,446\,74$ for this density, and the rest of § 6 contains our reasoning for the conjecture as stated.

We can show that only certain primes have the property that their squares can divide an integer of the form $n^n+(-1)^n(n-1)^{n-1}$; indeed, 59, 79, and 83 are the smallest primes with this property. It turns out that the theoretical investigation of primes with this property is even tidier if we widen slightly the class of primes. Given $\varepsilon \in \{-1, 1\}$ and positive integers $n > m$, define

$$D_\varepsilon(n, m) = n^n + \varepsilon(n-m)^{n-m}m^m. \tag{1}$$

These quantities are closely related to discriminants of trinomials of the form $x^n \pm x^m \pm 1$. We note for future use that if a prime p divides $D_\varepsilon(n, m)$, then p divides either all of n, m, and $n-m$ or none of them.

Now define

$$\mathcal{P}_\varepsilon = \{p \text{ prime}\colon \text{there exist positive integers } n, m \text{ with } p \nmid m \text{ such that } p^2 \mid D_\varepsilon(n, m)\}, \tag{2}$$

the restriction $p \nmid m$ being present to avoid high powers of p dividing $D_\varepsilon(n, m)$ for trivial reasons. (We will also write $\mathcal{P}_+$ for $\mathcal{P}_1$ and $\mathcal{P}_-$ for $\mathcal{P}_{-1}$, and similarly for $D_+(n, m)$ and $D_-(n, m)$.) We saw earlier, for example, that $83 \in D_+(n, m)$ and $59 \in D_\varepsilon(n, m)$ for both $\varepsilon \in \{-1, 1\}$. The smallest prime in both $\mathcal{P}_+$ and $\mathcal{P}_-$ turns out to be 7, as witnessed by 49 dividing both $D_+(5, 1) = 5^5 + 4^4$ and $D_-(10, 2) = 10^{10} - 8^8 2^2$.

A set of primes with a different definition will also be relevant to this story: define

$$\mathcal{P}_{\text{cons}} = \{p \text{ prime}\colon \text{there exist consecutive nonzero } p\text{th powers modulo } p^2\}. \tag{3}$$

One way to look at $\mathcal{P}_{\text{cons}}$ is as a vast generalization of Wieferich primes, that is, primes p for which $2^{p-1} \equiv 1 \pmod{p^2}$. Indeed, if p is a Wieferich prime, then $1^p \equiv 1 \pmod{p^2}$ and $2^p \equiv 2 \pmod{p^2}$ are consecutive nonzero pth powers modulo p^2. The smallest prime in $\mathcal{P}_{\text{cons}}$ turns out to be 7, as witnessed by $2^7 \equiv 30 \pmod{49}$ and $3^7 \equiv 31 \pmod{49}$.

The introduction of $\mathcal{P}_{\text{cons}}$ might seem unmotivated from our discussion of trinomial discriminants; in fact, it is extremely relevant, as the following surprising theorem (established in § 3) demonstrates.

THEOREM 1.2. *We have* $\mathcal{P}_+ = \mathcal{P}_- = \mathcal{P}_{\text{cons}}$.

Our proof that each of $\mathcal{P}_\pm$ is equal to $\mathcal{P}_{\text{cons}}$ is explicit and constructive, in that we provide an algorithm (see the bijections treated in Theorem 3.6) for starting with integers n and m for which p^2 divides $D_\pm(n, m)$ and constructing consecutive pth powers modulo p^2, and vice versa. Indeed, these bijections are very important to the computations we have done to determine the density asserted in Conjecture 1.1.

We remark that we have prohibited certain trivial divisibilities in the definitions of these sets of primes, namely, p dividing m (and hence n) in the definition of $\mathcal{P}_\pm$, and the consecutive pth powers $(-1)^p, 0^p, 1^p$ modulo p^2; these trivialities correspond to each other under our bijections. It turns out that there is another patterned way for primes to be included in $\mathcal{P}_\pm$ and $\mathcal{P}_{\text{cons}}$

https://doi.org/10.1112/S1461157014000436 Published online by Cambridge University Press

that is related to sixth roots of unity; we show in Theorem 4.6 that the bijections remain valid for the more restrictive sets of primes formed by prohibiting these further 'trivialities'. As a lagniappe, these divisibilities are interesting and unexpected in their own right; for example, we can prove that for any nonnegative integer k,

$$(12k^2+6k+1)^2 \quad \text{divides} \quad (6k+2)^{6k+2}-(6k+1)^{6k+1}. \tag{4}$$

We find this divisibility statement (which is equivalent to Proposition 4.3) to be unlike anything we have encountered prior to this work. In Proposition 4.8, we show how this divisibility can be leveraged into the construction of '*abc* triples' whose quality is on par with the best known elementary constructions.

The set $\mathcal{P}_{\text{cons}}$ has a reasonably natural definition, and as is our custom we can ask quantitative questions about it, such as how likely it is for a prime to appear in $\mathcal{P}_{\text{cons}}$. Recall that the relative density of any set $\mathcal{P}$ of primes is defined to be

$$\lim_{x\to\infty}\frac{\#\{p\leqslant x : p\in\mathcal{P}\}}{\#\{p\leqslant x : p \text{ prime}\}}=\lim_{x\to\infty}\frac{\#\{p\leqslant x : p\in\mathcal{P}\}}{\pi(x)},$$

where as usual $\pi(x)$ denotes the number of primes not exceeding x. We believe the following assertion to be true.

CONJECTURE 1.3. The relative density of $\mathcal{P}_{\text{cons}}$ within the primes equals $1-\frac{1}{2}e^{-1/6}\approx 57.68\%$.

We defend this belief in § 5. It is easy to see that the family of polynomials

$$f_p(x)=\frac{(x+1)^p-x^p-1}{p} \tag{5}$$

detects consecutive pth powers modulo p^2 (see Lemma 2.5); these polynomials have appeared in similar contexts, as we remark at the end of § 5, and go all the way back to Cauchy's work. As it happens, the roots of each of these polynomials come in sets of six (except for a few explicit exceptions; see Proposition 5.3), which we have dubbed 'six-packs'. This structure is crucial to our justification of Conjecture 1.3; in fact, it allows us to make a more refined assertion (Conjecture 5.4) about the distribution of the number of pairs of consecutive pth powers modulo p^2, rather than simply the presence or absence of such.

After setting out some preliminary lemmas in § 2, we provide in § 3 the details of the bijections that underlie our proof of Theorem 1.2. Section 4 contains results concerning cyclotomic factors of trinomials (and corresponding 'trivial' memberships in $\mathcal{P}_{\pm}$) and the presence of sixth roots of unity in $\mathcal{P}_{\text{cons}}$, as well as the material that relates to the *abc* conjecture. We recall the symmetries among the roots of the polynomials f_p in § 5 and use them to formulate Conjecture 1.3 and its refinement. Finally, we return to the density of squarefree values of $n^n+(-1)^n(n-1)^{n-1}$ in § 6, describing the computations we performed to arrive at the value given in Conjecture 1.1.

2. *Preliminary lemmas*

In this section we record several simple statements that will be useful to us during the proofs of our main results. We begin by discussing discriminants and resultants of polynomials of one variable. Let $\operatorname{Disc} g$ denote the discriminant of the polynomial $g(x)$, and let $\operatorname{Res}(g,h)$ denote the resultant of $g(x)$ and $h(x)$. The following formula for the discriminant of the product of two polynomials is classical [**4**, Chapter 12, equation (1.32)].

https://doi.org/10.1112/S1461157014000436 Published online by Cambridge University Press

LEMMA 2.1. *For any two polynomials g and h,*

$$\operatorname{Disc}(gh) = (-1)^{\deg(g)\deg(h)} \operatorname{Disc}(g) \operatorname{Disc}(h) \operatorname{Res}(g,h)^2.$$

The formula for the discriminant of a trinomial is also classical; the following lemma is a special case of [4, Chapter 12, equation (1.38)]. Recall that $D_\varepsilon(n,m)$ was defined in equation (1).

LEMMA 2.2. *Let $n > m$ be positive integers with $(n,m) = 1$, and let $a, b \in \{-1, 1\}$. Then $|\operatorname{Disc}(x^n + ax^m + b)| = D_\varepsilon(n,m)$, where $\varepsilon = (-1)^{n-1} a^n b^{n-m}$.*

We remark that a formula for the discriminant of the trinomial $x^n + ax^m + b$ is known even when n and m are not relatively prime [19, Theorem 2]. Only the values $D_\pm(m,n)$ with $(n,m) = 1$ are directly relevant to discriminants of these trinomials; nevertheless, for most of this paper we shall investigate all the values $D_\pm(m,n)$ without the coprimality restriction.

We continue by proving a few basic facts from elementary number theory to be used later. An integer x is a *pth power modulo p^2* if $x \equiv a^p \pmod{p^2}$ for some integer a; if in addition $x \not\equiv 0 \pmod{p}$, we call x a *nonzero pth power modulo p^2*. Two pth powers x and y modulo p^2 are *consecutive modulo p^2* if $y - x \equiv \pm 1 \pmod{p^2}$.

LEMMA 2.3. *Let p be a prime, and let x be an integer.*

(a) *x is a nonzero pth power modulo p^2 if and only if $x^{p-1} \equiv 1 \pmod{p^2}$.*
(b) *There exists a unique pth power modulo p^2 that is congruent to x modulo p.*
(c) *When $p \nmid x$, the order of x modulo p is the same as the order of x^p modulo p^2.*

Proof. Part (a) follows directly from the fact that $(\mathbb{Z}/p^2\mathbb{Z})^\times$ is cyclic of order $p(p-1)$. The existence in part (b) comes from setting $y = x^p$, so that y is a pth power modulo p^2 and $y \equiv x \pmod{p}$ by Fermat's little theorem. As for uniqueness, suppose that z is any pth power modulo p^2 with $z \equiv x \pmod{p}$. Since $z \equiv y \pmod{p}$, write $z = y + kp$ for some integer k. Then

$$z \equiv z \cdot z^{p-1} = z^p = (y + kp)^p \equiv y^p = y \cdot y^{p-1} \equiv y \pmod{p^2},$$

where the first and last congruences follow from part (a) and the middle congruence follows from the binomial expansion of $(y + kp)^p$. (We should not have invoked part (a) when $x \equiv 0 \pmod{p}$, but the assertion of part (b) is trivial in that case.)

As for part (c), if $(x^p)^t \equiv 1 \pmod{p^2}$, then certainly $x^t \equiv (x^p)^t \equiv 1 \pmod{p}$ as well by Fermat's little theorem. Conversely, if $x^t \equiv 1 \pmod{p}$, then $(x^p)^t \equiv x^t \equiv 1 \pmod{p}$ as well. But then $(x^p)^t = (x^t)^p$ is a pth power modulo p^2 that is congruent to 1 modulo p; but 1 itself is also a pth power congruent to 1 modulo p^2. Therefore $(x^p)^t \equiv 1 \pmod{p^2}$ by part (b). In particular, the orders of $x \pmod{p}$ and $x^p \pmod{p^2}$ coincide. □

LEMMA 2.4. *For any prime p, consecutive pth powers modulo p^2 must be pth powers of consecutive residue classes modulo p.*

Proof. If $x \equiv a^p \pmod{p^2}$ and $y \equiv b^p \pmod{p^2}$ are consecutive pth powers modulo p^2, then $\pm 1 \equiv y - x \equiv b^p - a^p \pmod{p^2}$. Hence certainly $\pm 1 \equiv b^p - a^p \equiv b - a \pmod{p}$ by Fermat's little theorem, which establishes the lemma. □

We can now understand why the polynomial f_p defined in equation (5) is relevant to the study of consecutive pth powers modulo p^2.

LEMMA 2.5. *For any prime p, the roots of f_p are in one-to-one correspondence with pairs of consecutive pth powers modulo p^2. Moreover, 0 and -1 are always roots of f_p, and any*

https://doi.org/10.1112/S1461157014000436 Published online by Cambridge University Press

remaining roots are in one-to-one correspondence with pairs of consecutive nonzero pth powers modulo p^2.

Proof. By Lemma 2.3(a), we see that if x and $x+1$ are pth powers modulo p^2, then $(x+1)^p - x^p - 1 \equiv (x+1) - x - 1 \equiv 0 \pmod{p^2}$, or $f_p(x) \equiv 0 \pmod{p}$. Conversely, if $f_p(a) \equiv 0 \pmod{p}$ then $(a+1)^p - a^p - 1 \equiv 0 \pmod{p^2}$, showing that a^p and $(a+1)^p$ are consecutive pth powers modulo p^2. Therefore the roots of f_p are in one-to-one correspondence with residue classes $a \pmod{p}$ such that a^p and $(a+1)^p$ are consecutive $\pmod{p^2}$; and Lemma 2.4 tells us that such pairs are the only possible consecutive pth powers modulo p^2. The roots 0 and -1 of f_p obviously correspond to the pairs $0, 1$ and $-1, 0$ of consecutive pth powers modulo p^2. □

We conclude this section with two specific results that will keep later proofs from becoming mired in elementary details.

LEMMA 2.6. *Let p be an odd prime and x a pth power modulo p^2. Suppose that y is an integer such that $x^k \equiv \pm y^m \pmod{p^2}$ for some integers k and m with $p \nmid m$. Then y is a pth power modulo p^2.*

Proof. We know that $x^{p-1} \equiv 1 \pmod{p^2}$ from Lemma 2.3(a), and so

$$1 \equiv x^{k(p-1)} \equiv (\pm y^m)^{p-1} = (y^m)^{p-1} \pmod{p^2}$$

since p is odd. The order of y modulo p^2 thus divides $m(p-1)$; but this order also divides $\phi(p^2) = p(p-1)$. Since $p \nmid m$, the greatest common divisor of $m(p-1)$ and $p(p-1)$ equals $p-1$, and so the order of y modulo p^2 divides $p-1$. In other words, $y^{p-1} \equiv 1 \pmod{p^2}$, and so y is a pth power modulo p^2 by Lemma 2.3(a) again. □

LEMMA 2.7. *Let p be a prime. For any integers x, y, and z with $x + pz > 0$,*

$$(x+py)^{x+pz} \equiv x^{x+pz}(1+py) \pmod{p^2}.$$

Moreover, if x is a pth power modulo p^2, then

$$(x+py)^{x+pz} \equiv x^{x+z}(1+py) \pmod{p^2}.$$

Proof. Using the binomial theorem and discarding multiples of p^2,

$$\begin{aligned}(x+py)^{x+pz} &= \sum_{j=0}^{x+pz} \binom{x+pz}{j} x^{x+pz-j}(py)^j \\ &\equiv \binom{x+pz}{0} x^{x+pz} + \binom{x+pz}{1} x^{x+pz-1} py \\ &= x^{x+pz} + (x+pz)x^{x+pz-1}py \equiv x^{x+pz}(1+py) \pmod{p^2},\end{aligned}$$

establishing the first claim. If x is a pth power modulo p^2, then $x^{pz} = (x^{p-1})^z x^z \equiv x^z \pmod{p^2}$ by Lemma 2.3(a), establishing the second claim. □

3. *Correspondence between roots of f_p and pairs (n, m)*

The main goal of this section is to establish Theorem 1.2, which asserts that the sets $\mathcal{P}_+$ and $\mathcal{P}_-$ defined in equation (2) are both equal to the set $\mathcal{P}_{\text{cons}}$ defined in equation (3). While the

https://doi.org/10.1112/S1461157014000436 Published online by Cambridge University Press

proofs in this section are all elementary, it is not particularly straightforward to come up with the precise formulations of the statements that will lead to the final bijections.

First we give two lemmas showing that certain divisibilities by square factors depend only upon the residue classes of the variables to particular moduli.

LEMMA 3.1. *Let p be a prime, and let m and n be integers not divisible by p. Suppose that m' and n' are integers satisfying $m' \equiv m \pmod{p(p-1)}$ and $n' \equiv n \pmod{p(p-1)}$. Then $p^2 \mid D_\pm(n,m)$ if and only if $p^2 \mid D_\pm(n',m')$.*

REMARK. We have defined $D_\pm(n,m)$ only when $n > m$ are positive integers. However, this lemma tells us that the property $p^2 \mid D_\pm(n,m)$ depends only upon the residue classes of n and m modulo $p(p-1)$. Therefore, if we ever write $p^2 \mid D_\pm(n,m)$ when $m \leqslant 0$ or $m \geqslant n$, what we mean is that $p^2 \mid D_\pm(n',m')$ for positive $m' \equiv m \pmod{p(p-1)}$ and sufficiently large $n' \equiv n \pmod{p(p-1)}$.

Proof of Lemma 3.1. Write $n' = n + kp(p-1)$ for some integer k. Then by Lemma 2.7 with $y = k(p-1)$,

$$\begin{aligned} D_\pm(n',m) &= (n+kp(p-1))^{n+kp(p-1)} \pm (n-m+kp(p-1))^{n-m+kp(p-1)} m^m \\ &\equiv n^{n+kp(p-1)}(1+kp(p-1)) \pm (n-m)^{n-m+kp(p-1)}(1+kp(p-1))m^m \pmod{p^2}. \end{aligned}$$

If $p^2 \mid D_\pm(n,m)$, then p cannot divide $n-m$ (or else it would divide n, contrary to assumption). Thus $n^{p(p-1)}$ and $(n-m)^{p(p-1)}$ are congruent to 1 (mod p^2) by Euler's theorem, and so

$$\begin{aligned} D_\pm(n',m) &\equiv n^n(1+kp(p-1)) \pm (n-m)^{n-m}(1+kp(p-1))m^m \\ &\equiv (1+kp(p-1))D_\pm(n,m) \pmod{p^2}; \end{aligned}$$

in particular, $p^2 \mid D_\pm(n,m)$ implies $p^2 \mid D_\pm(n',m)$. The roles of n and n' are symmetric, and so we conclude that $p^2 \mid D_\pm(n,m)$ if and only if $p^2 \mid D_\pm(n',m)$. Finally, a similar argument shows that $p^2 \mid D_\pm(n',m)$ if and only if $p^2 \mid D_\pm(n',m')$, which completes the proof of the lemma. □

LEMMA 3.2. *Let p be a prime, and let m, n, and ℓ be integers. Let r be any integer congruent to n modulo p. Then p^2 divides $r^n + \ell(r-m)^{n-m}$ if and only if p^2 divides $n^n + \ell(n-m)^{n-m}$.*

REMARK. One must avoid the pitfall of changing the occurrences of n in the exponents to r: it would be false to claim that $p^2 \mid (r^r + \ell(r-m)^{r-m})$ is equivalent to $p^2 \mid (n^n + \ell(n-m)^{n-m})$.

Proof. Writing $r = n + kp$ for some integer k, we have, by Lemma 2.7,

$$\begin{aligned} r^n + \ell(r-m)^{n-m} &= (n+kp)^n + \ell(n+kp-m)^{n-m} \\ &\equiv n^n(1+kp) + \ell(n-m)^{n-m}(1+kp) \\ &\equiv (1+kp)(n^n + \ell(n-m)^{n-m}) \pmod{p^2}. \end{aligned}$$

Since $1+kp$ is invertible modulo p^2, we conclude that $r^n + \ell(r-m)^{n-m} \equiv 0 \pmod{p^2}$ if and only if $n^n + \ell(n-m)^{n-m} \equiv 0 \pmod{p^2}$, as desired. □

Our next goal is the construction of a bijection (Theorem 3.6) between $\mathcal{A}_{p,m,\varepsilon}$, a set defined in equation (8) that indicates membership in $\mathcal{P}_\varepsilon$, and $\mathcal{B}_{p,m,\varepsilon}$, a set defined in equation (9) that is related to $\mathcal{P}_{\text{cons}}$.

https://doi.org/10.1112/S1461157014000436 Published online by Cambridge University Press

PROPOSITION 3.3. *Let p be prime, let m be a positive integer not divisible by p, and fix $\varepsilon \in \{1,-1\}$. Given any residue class $n \pmod{p(p-1)}$ such that $p^2 \mid D_\varepsilon(n,m)$, set $k \equiv m-n \pmod{p(p-1)}$, and let x be any integer satisfying $x \equiv 1 - mn^{-1} \pmod{p}$. Then $x^k \equiv -\varepsilon(1-x)^m \pmod{p^2}$.*

Proof. Note that the congruence $x \equiv 1 - mn^{-1} \pmod{p}$ is well defined because p cannot divide n; also, $1 - x \not\equiv 0 \pmod{p}$ because p cannot divide m, and so $1-x$ is invertible modulo p^2. Set $r \equiv m(1-x)^{-1} \pmod{p^2}$, so that $x \equiv 1 - mr^{-1} \pmod{p^2}$. Also note that $x \equiv (n-m)n^{-1} \pmod{p^2}$ is invertible modulo p^2 because p cannot divide $n-m$; in particular, $x^{p(p-1)} \equiv 1 \pmod{p^2}$ and hence $x^k \equiv x^{m-n} \pmod{p^2}$. Consequently, $r - m \equiv xr \pmod{p^2}$ is invertible. Therefore we can factor out powers of r and $r-m$ to obtain

$$\begin{aligned} x^k + \varepsilon(1-x)^m &\equiv (1-mr^{-1})^{m-n} + \varepsilon(mr^{-1})^m \\ &\equiv r^{-m}(r-m)^{m-n}(r^n + \varepsilon(r-m)^{n-m}m^m) \pmod{p^2}. \end{aligned} \tag{6}$$

Since $p^2 \mid D_\varepsilon(n,m)$ by assumption, we have $n^n + \varepsilon(n-m)^{n-m}m^m \equiv 0 \pmod{p^2}$; therefore $r^n + \varepsilon(r-m)^{n-m}m^m \equiv 0 \pmod{p^2}$ by Lemma 3.2, and hence $x^k + \varepsilon(1-x)^m \equiv 0 \pmod{p^2}$ by the congruence (6). □

COROLLARY 3.4. *Let p be an odd prime, let m be a positive integer not divisible by p, and let $\varepsilon \in \{1,-1\}$. Given any residue class $n \pmod{p(p-1)}$ such that $p^2 \mid D_\varepsilon(n,m)$, set $k \equiv m-n \pmod{p(p-1)}$, and define x to be the unique pth power modulo p^2 such that $x \equiv 1 - mn^{-1} \pmod{p}$. Then $x^k \equiv -\varepsilon(1-x)^m \pmod{p^2}$. In particular, $x-1$ is also a pth power modulo p^2.*

REMARK. In the statement of the corollary, k is determined modulo $p(p-1)$; however, any integer $k' \equiv k \pmod{p-1}$ also satisfies $x^{k'} \equiv -\varepsilon(1-x)^m \pmod{p^2}$, by Lemma 2.3(a). We also remark that $x \not\equiv 1 \pmod{p}$ since $p \nmid n$.

Proof. Proposition 3.3 tells us that the congruence $x^k \equiv -\varepsilon(1-x)^m \pmod{p^2}$ holds for any integer x such that $x \equiv 1 - mn^{-1} \pmod{p}$. When we add the condition that x be a pth power modulo p^2, Lemma 2.3(b) implies that x is unique $\pmod{p^2}$. Finally, since x is a pth power modulo p^2 and $x^k \equiv ((-1)^{m+1}\varepsilon)(x-1)^m \pmod{p^2}$, we conclude from Lemma 2.6 that $x-1$ is also a pth power modulo p^2. □

PROPOSITION 3.5. *Let p be an odd prime, let $\varepsilon \in \{1,-1\}$, and let k and m be integers. Suppose that x is a pth power modulo p^2 that satisfies $x^k \equiv -\varepsilon(1-x)^m \pmod{p^2}$. Set $n = (m-k)p - m(1-x)^{-1}(p-1)$, where $(1-x)^{-1}$ is any integer satisfying $(1-x)^{-1}(1-x) \equiv 1 \pmod{p^2}$. Then $p^2 \mid D_\varepsilon(n,m)$.*

REMARK. Notice that the congruence $x^k \equiv -\varepsilon(1-x)^m \pmod{p^2}$ implies that neither x nor $1-x$ can be divisible by p. The fact that $(1-x)^{-1}$ is determined modulo p^2 implies that the definition of n is determined as a single residue class modulo $p^2(p-1)$; however, Lemma 3.1 implies that any integer n' that is congruent to n modulo $p(p-1)$ also satisfies $p^2 \mid D_\varepsilon(n',m)$. Note also that the hypotheses determine k only modulo $p-1$; this is again fine, as changing n by a multiple of $p(p-1)$ does not affect whether $p^2 \mid D_\varepsilon(n,m)$.

Proof of Proposition 3.5. Write $n = m(1-x)^{-1} + p((m-k) - m(1-x)^{-1})$. By Lemma 2.7,

$$\begin{aligned} n^n &\equiv (m(1-x)^{-1})^n(1 + p((m-k) - m(1-x)^{-1})) \\ &\equiv m^n(1-x)^{-n}(1 + n - m(1-x)^{-1}) \pmod{p^2}. \end{aligned}$$

https://doi.org/10.1112/S1461157014000436 Published online by Cambridge University Press

Similarly, $n-m=(m(1-x)^{-1}-m)+p((m-k)-m(1-x)^{-1})$, and so

$$\begin{aligned}(n-m)^{n-m}m^m &\equiv (m(1-x)^{-1}-m)^{n-m}(1+p((m-k)-m(1-x)^{-1}))m^m\\ &\equiv m^n((1-x)^{-1}-1)^{n-m}(1+n-m(1-x)^{-1}) \pmod{p^2}.\end{aligned}$$

Consequently,

$$\begin{aligned}D_\varepsilon(n,m) &= n^n+\varepsilon(n-m)^{n-m}m^m\\ &\equiv m^n(1+n-m(1-x)^{-1})((1-x)^{-n}+\varepsilon((1-x)^{-1}-1)^{n-m}) \pmod{p^2}. \qquad (7)\end{aligned}$$

Since x is a nonzero pth power modulo p^2 and $n-m+k\equiv(m-k)-m+k\equiv 0 \pmod{p-1}$, Lemma 2.3(a) tells us that $x^{n-m+k}\equiv 1 \pmod{p^2}$. By hypothesis, this can be written as

$$x^{n-m}(-\varepsilon(1-x)^m)\equiv 1 \pmod{p^2},$$

which we rearrange into the more complicated

$$1+\varepsilon(1-(1-x))^{n-m}(1-x)^m\equiv 0 \pmod{p^2}.$$

Dividing through by $(1-x)^n$, we obtain $(1-x)^{-n}+\varepsilon((1-x)^{-1}-1)^{n-m}\equiv 0 \pmod{p^2}$, which together with equation (7) shows that $D_\varepsilon(n,m)\equiv 0 \pmod{p^2}$ as desired. □

Given an odd prime p, an integer m not divisible by p, and $\varepsilon\in\{1,-1\}$, define a set of residue classes

$$\mathcal{A}_{p,m,\varepsilon}=\{n \pmod{p(p-1)} : p^2 \mid D_\varepsilon(n,m)\} \qquad (8)$$

and a set of ordered pairs of residue classes

$$\begin{aligned}\mathcal{B}_{p,m,\varepsilon}=\{&(x \pmod{p^2}, k \pmod{p-1}) :\\ &x \text{ is a nonzero } p\text{th power modulo } p^2 \text{ and } x^k\equiv -\varepsilon(1-x)^m \pmod{p^2}\}. \qquad (9)\end{aligned}$$

For any (x,k) in the latter set, note that x and $x-1$ are consecutive nonzero pth powers modulo p^2, by the argument in the proof of Corollary 3.4. Also define functions $\alpha_{p,m,\varepsilon}:\mathcal{A}_{p,m,\varepsilon}\to\mathcal{B}_{p,m,\varepsilon}$ and $\beta_{p,m,\varepsilon}:\mathcal{B}_{p,m,\varepsilon}\to\mathcal{A}_{p,m,\varepsilon}$ by

$$\begin{aligned}&\alpha_{p,m,\varepsilon}(n \pmod{p(p-1)})\\ &\quad=(\text{the } p\text{th power } x \pmod{p^2} \text{ such that } x\equiv 1-mn^{-1} \pmod{p},\ m-n \pmod{p-1})\end{aligned}$$

and

$$\beta_{p,m,\varepsilon}(x \pmod{p^2}, k \pmod{p-1})=(m-k)p-m(1-x)^{-1}(p-1) \pmod{p(p-1)}.$$

Lemma 2.3(b), Corollary 3.4, and Proposition 3.5 (and the remarks following their statements) ensure that these functions are well defined.

THEOREM 3.6. *Let p be an odd prime, let m be an integer not divisible by p, and let $\varepsilon\in\{1,-1\}$. There is a one-to-one correspondence between $\mathcal{A}_{p,m,\varepsilon}$ and $\mathcal{B}_{p,m,\varepsilon}$, given by the bijections $\alpha_{p,m,\varepsilon}$ and $\beta_{p,m,\varepsilon}$ which are inverses of each other.*

REMARK. The exact correspondence is important computationally, but the underlying qualitative statement alone is simple and surprising.

https://doi.org/10.1112/S1461157014000436 Published online by Cambridge University Press

Proof. It remains only to check the assertion that $\alpha_{p,m,\varepsilon}$ and $\beta_{p,m,\varepsilon}$ are inverses of each other. For example, note that

$$\beta_{p,m,\varepsilon}(x,k) \equiv (m-k)1 - m(1-x)^{-1}0 = m-k \pmod{p-1}$$
$$\beta_{p,m,\varepsilon}(x,k) \equiv (m-k)0 - m(1-x)^{-1}(-1) = m(1-x)^{-1} \pmod{p}.$$

Therefore for any $n \in \mathcal{A}_{p,m,\varepsilon}$,

$$\beta_{p,m,\varepsilon} \circ \alpha_{p,m,\varepsilon}(n) \equiv m - (m-n) = n \pmod{p-1}$$
$$\beta_{p,m,\varepsilon} \circ \alpha_{p,m,\varepsilon}(n) \equiv m(1-(1-mn^{-1}))^{-1} = n \pmod{p},$$

and so $\beta_{p,m,\varepsilon} \circ \alpha_{p,m,\varepsilon}(n) \equiv n \pmod{p(p-1)}$ as required. Verifying that $\alpha_{p,m,\varepsilon} \circ \beta_{p,m,\varepsilon}(x,k) = (x,k)$ for every $(x,k) \in \mathcal{B}_{p,m,\varepsilon}$ is similarly straightforward. □

With this bijection in hand, we need only one more lemma before being able to fully establish Theorem 1.2.

LEMMA 3.7. *Suppose that $p \in \mathcal{P}_{\text{cons}}$. Then there exists an integer x such that x and $1-x$ are nonzero pth powers modulo p^2 and $1-x$ has even order* (mod p^2).

Proof. By Lemma 2.5, the fact that $p \in \mathcal{P}_{\text{cons}}$ implies that there exists $y \not\equiv 0 \pmod{p}$ such that $f_p(y) \equiv 0 \pmod{p}$. Set $z \equiv y^{-1} \pmod{p}$; Lemma 5.1 confirms that $f_p(z) \equiv 0 \pmod{p}$ as well. In other words, we have both $(y+1)^p \equiv y^p + 1 \pmod{p^2}$ and $(z+1)^p \equiv z^p + 1 \pmod{p^2}$.

Lemma 2.3(c) tells us that for any integer $a \not\equiv 0 \pmod{p}$, the order of $a^p \pmod{p^2}$ is the same as the order of $a \pmod{p}$. Hence if $y+1$ has even order modulo p, set $x \equiv (-y)^p \pmod{p^2}$. If $-y$ has even order modulo p, then set $x \equiv (y+1)^p \pmod{p^2}$. If both $y+1$ and $-y$ have odd order modulo p, then their quotient $-(y+1)z = -(1+z)$ also has odd order modulo p; but then $1+z$ has even order modulo p, whence we set $x \equiv (-z)^p \pmod{p^2}$. □

Proof of Theorem 1.2. It is easy to see from the definitions of $\mathcal{P}_{\text{cons}}$ and $\mathcal{P}_\varepsilon$ that the prime 2 is not in any of these sets; henceforth we may assume that p is odd.

Given $\varepsilon \in \{1,-1\}$, suppose that $p \in \mathcal{P}_\varepsilon$, so that there exist positive integers n, m with $p \nmid m$ such that $p^2 \mid D_\varepsilon(n,m)$. By Corollary 3.4, there exists a nonzero pth power $x \pmod{p^2}$ such that $x-1$ is also a nonzero pth power modulo p^2; therefore $p \in \mathcal{P}_{\text{cons}}$ as well.

Conversely, suppose that $p \in \mathcal{P}_{\text{cons}}$. By Lemma 3.7, we can choose x such that x and $1-x$ are both nonzero pth powers modulo p^2 and $1-x$ has even order modulo p^2. Fix a primitive root $g \pmod{p^2}$, and choose integers $1 \leqslant j,k \leqslant p-2$ such that $x \equiv g^{pj} \pmod{p^2}$ and $1-x \equiv g^{pk} \pmod{p^2}$. We know that the order of $1-x \equiv g^{pk}$ is even, so let $2t$ denote that order, noting that $1 \leqslant t \leqslant (p-1)/2$ by Lemma 2.3(a). Then $((g^{pk})^t)^2 \equiv 1 \pmod{p^2}$ but $(g^{pk})^t \not\equiv 1 \pmod{p^2}$, and hence we must have $g^{pkt} \equiv -1 \pmod{p^2}$.

- If $\varepsilon = -1$, then setting $m = j$ yields $x^k \equiv (g^{pm})^k = -\varepsilon(g^{pk})^m \equiv -\varepsilon(1-x)^m \pmod{p^2}$.
- If $\varepsilon = 1$, then setting $m = j - t$ yields $x^k \equiv (g^{pm+pt})^k = (g^{ptk})\varepsilon(g^{pk})^m \equiv -\varepsilon(1-x)^m \pmod{p^2}$. Note that $|m| \leqslant p-2$; if $m = 0$, then by Lemma 2.3(a) we can replace m by $p-1$.

In either case, Proposition 3.5 tells us that $p^2 \mid D_\varepsilon(n,m)$, and in all cases we know that $p \nmid m$. Therefore, $p \in \mathcal{P}_\varepsilon$ as desired. □

In the introduction we saw that $59 \in \mathcal{P}_\pm$, and so by Theorem 1.2 we must have $59 \in \mathcal{P}_{\text{cons}}$ as well; the consecutive residue classes $3^{59} \equiv 298 \pmod{59^2}$ and $4^{59} \equiv 299 \pmod{59^2}$ witness this membership (in fact there are 14 pairs of consecutive 59th powers modulo 59^2). On the other hand, Wieferich primes are obviously in $\mathcal{P}_{\text{cons}}$, and so they must be in each of $\mathcal{P}_\pm$ as well. One can work through the bijections in this section to see that if p is a Wieferich prime,

https://doi.org/10.1112/S1461157014000436 Published online by Cambridge University Press

then p^2 divides $D_+(2p-1,1) = (2p-1)^{2p-1} + (2p-2)^{2p-2}$, for example. (Once discovered, this divisibility can also be proved more straightforwardly using Lemma 2.7.)

4. *Reducible trinomials*

We continue to investigate the parallels between square divisors of $D_\pm(n,m)$ and pairs of consecutive pth powers modulo p^2. We have already ruled out trivial occurrences of both objects: when p divides n and m we trivially have $p^2 \mid D_\pm(n,m)$, while $-1, 0, 1$ are trivial consecutive pth powers for any prime. As it happens, however, there are more subtle examples of 'trivial' occurrences of both objects, which turn out to correspond to each other. In the first instance, we find predictable square divisors of $D_\pm(n,m)$ when a corresponding trinomial $x^n \pm x^m \pm 1$ is reducible with cyclotomic factors; in the second instance, we find that sixth roots of unity are predictable consecutive pth powers modulo p^2. Once these predictable occurrences are excluded, we see (Theorem 4.6) that the 'sporadic' occurrences are again in perfect correspondence.

Ljunggren [**10**, Theorem 3] established that trinomials of the form $x^n \pm x^m \pm 1$ are irreducible, except for certain explicit situations when they have known cyclotomic factors. Since the statement below requires both greatest common divisors and ordered pairs, we shall temporarily write $\gcd(m,n)$ explicitly.

LEMMA 4.1 (Ljunggren). *Let $n > m$ be positive integers, and let $\varepsilon, \varepsilon' \in \{-1, 1\}$.*

(a) *Suppose that $\gcd(n,m) = 1$. The trinomial $x^n + \varepsilon x^m + \varepsilon'$ is irreducible except in the following situations:*
   (i) *if $(n,m) \equiv (1,5) \pmod 6$ or $(n,m) \equiv (5,1) \pmod 6$, and $\varepsilon = 1$, then $x^n + \varepsilon x^m + \varepsilon' = g(x)h(x)$ where $g(x) = x^2 + \varepsilon' x + 1$ and $h(x)$ is irreducible;*
   (ii) *if $(n,m) \equiv (2,1) \pmod 6$ or $(n,m) \equiv (4,5) \pmod 6$, and $\varepsilon' = 1$, then $x^n + \varepsilon x^m + \varepsilon' = g(x)h(x)$ where $g(x) = x^2 + \varepsilon x + 1$ and $h(x)$ is irreducible;*
   (iii) *if $(n,m) \equiv (1,2) \pmod 6$ or $(n,m) \equiv (5,4) \pmod 6$, and $\varepsilon = \varepsilon'$, then $x^n + \varepsilon x^m + \varepsilon' = g(x)h(x)$ where $g(x) = x^2 + \varepsilon x + 1$ and $h(x)$ is irreducible.*

(b) *Suppose that $\gcd(n,m) = d > 1$. If the trinomial $x^{n/d} + \varepsilon x^{m/d} + \varepsilon'$ factors as $g(x)h(x)$ according to one of the situations in part* (a)*, then $x^n + \varepsilon x^m + \varepsilon'$ factors as $g(x^d)h(x^d)$ and $h(x^d)$ is irreducible; otherwise, $x^n + \varepsilon x^m + \varepsilon'$ is irreducible.*

REMARK. In part (b), the other factor $g(x^d)$ might not be irreducible; but since $g(x)$ is a cyclotomic polynomial, $g(x^d)$ will be a product of cyclotomic polynomials (of order dividing $6d$) that is easy to work out.

LEMMA 4.2. *Let m and n be positive integers and set $\gcd(n,m) = d$, and let $\varepsilon, \varepsilon' \in \{-1, 1\}$. Suppose that $x^n + \varepsilon x^m + \varepsilon'$ is reducible, and let $g(x)$ and $h(x)$ be the polynomials described in Lemma 4.1, so that $x^n + \varepsilon x^m + \varepsilon' = g(x^d)h(x^d)$. Then*

$$\operatorname{Res}(g(x^d), h(x^d)) = \left(\frac{n^2 - mn + m^2}{3d^2}\right)^d.$$

Proof. We include only the proof of a single representative case, since the full proof contains no new ideas but a lot of repetition. Suppose that $n \equiv 1 \pmod 6$ and $m \equiv 5 \pmod 6$, that $(n,m) = 1$, and that $\varepsilon = \varepsilon' = 1$, so that $x^n + x^m + 1 = (x^2 + x + 1)h(x)$ by Lemma 4.1; we need to show that $\operatorname{Res}(x^2 + x + 1, h(x)) = (n^2 - mn + m^2)/3$. Let $\zeta = e^{2\pi i/3}$, so that the roots of $x^2 + x + 1$ are ζ and $\bar{\zeta}$; then by the definition of the resultant,

$$\operatorname{Res}(x^2 + x + 1, h(x)) = h(\zeta)h(\bar{\zeta}).$$

https://doi.org/10.1112/S1461157014000436 Published online by Cambridge University Press

By L'Hôpital's rule, we have

$$h(\zeta) = \lim_{z\to\zeta} \frac{f(z)}{g(z)} = \lim_{z\to\zeta} \frac{f'(z)}{g'(z)} = \frac{f'(\zeta)}{g'(\zeta)} = \frac{n\zeta^{n-1} + m\zeta^{m-1}}{2\zeta + 1} = \frac{n + m\zeta}{i\sqrt{3}}$$

by the congruence conditions on n and m. Consequently,

$$h(\zeta)h(\bar{\zeta}) = h(\zeta)\overline{h(\zeta)} = \frac{n + m\zeta}{i\sqrt{3}} \frac{n + m\bar{\zeta}}{-i\sqrt{3}} = \frac{n^2 + mn(\zeta + \bar{\zeta}) + m^2\zeta\bar{\zeta}}{3} = \frac{n^2 - mn + m^2}{3},$$

as claimed. □

As a concrete application, we are now able to describe a parametric family of square divisors of $D_-(n, 1)$.

PROPOSITION 4.3. *If* $n \equiv 2 \pmod 6$, *then*

$$\left(\frac{n^2 - n + 1}{3}\right)^2 \quad \textit{divides} \quad n^n - (n-1)^{n-1}. \tag{10}$$

REMARK. Setting $n = 6k + 2$ shows that this result is equivalent to equation (4). Once discovered, that divisibility can be proved directly using the easily-verified congruences

$$-(6k+2)^3 \equiv 1 - (18k+9)(12k^2 + 6k + 1) \pmod{(12k^2 + 6k + 1)^2},$$
$$(6k+1)^3 \equiv 1 + 18k(12k^2 + 6k + 1) \pmod{(12k^2 + 6k + 1)^2},$$

which hint at the connection to sixth roots of unity. Of course, this elementary proof sheds little light upon the true reason for the existence of the divisibility.

Proof of Proposition 4.3. When $n \equiv 2 \pmod 6$, Lemma 2.2 (with $m = \varepsilon = \varepsilon' = 1$) tells us that $|\mathrm{Disc}(x^n + x + 1)| = D_-(n, 1) = n^n - (n-1)^{n-1}$. On the other hand, we see from Lemma 4.1 that $x^n + x + 1 = (x^2 + x + 1)h(x)$ for some polynomial $h(x)$. Therefore the square of the resultant of $x^2 + x + 1$ and $h(x)$ divides $n^n - (n-1)^{n-1}$ by Lemma 2.1; and Lemma 4.2 tells us that this resultant is exactly $(n^2 - n + 1)/3$. □

REMARK. Many divisibility statements similar to (10) can be established using the same method, starting with special cases of Lemma 4.1 other than $n \equiv 2 \pmod 6$, $m = 1$, and $\varepsilon = \varepsilon' = 1$.

We now show that these particular divisibilities are intimately related to the primitive sixth roots of unity modulo p^2, when they exist. This relationship will allow us to classify certain square divisors of $D_\pm(m, n)$, and certain consecutive nonzero pth powers modulo p^2, as 'trivial' and to give an equivalence (Theorem 4.6) between the modified versions of $\mathcal{P}_\pm$ and $\mathcal{P}_{\mathrm{cons}}$ defined in equations (11) and (12) below.

LEMMA 4.4. *Let* $p \equiv 1 \pmod 6$ *be a prime, and let* x *be a primitive sixth root of unity modulo* p^2. *Then* $x - 1$ *is a primitive cube root of unity modulo* p^2. *In particular,* $x - 1$ *and* x *are consecutive* p*th powers modulo* p^2.

Proof. The primitive sixth root of unity x is a root of the polynomial congruence $x^2 - x + 1 \equiv 0 \pmod p$, which means that $x - 1 \equiv x^2 \pmod p$; since x^2 has order 3 when x has order 6, we conclude that $x - 1$ is a primitive cube root of unity modulo p^2. Since $3 \mid 6 \mid (p-1)$, both x^{p-1} and $(x-1)^{p-1}$ are congruent to 1 $\pmod{p^2}$, and so both x and $x - 1$ are pth powers modulo p^2 by Lemma 2.3(a). □

https://doi.org/10.1112/S1461157014000436 Published online by Cambridge University Press

LEMMA 4.5. *Let n and m be relatively prime integers, and let p be a prime not dividing n. Set $x \equiv 1 - mn^{-1} \pmod{p}$. Then x is a primitive sixth root of unity modulo p^2 if and only if $p^2 \mid (n^2 - mn + n^2)$.*

REMARK. It is easy to derive the fact that the lemma is still valid if $(n, m) > 1$, provided that the expression $n^2 - mn + m^2$ is replaced by $(n^2 - mn + m^2)/(n, m)^2$.

Proof. We begin by noting that x being a primitive sixth root of unity modulo p^2 is equivalent to $x^2 - x + 1 \equiv 0 \pmod{p^2}$, which in turn is equivalent to $x(1 - x) \equiv 1 \pmod{p^2}$. By the definition of x,

$$x(1-x) \equiv (1 - mn^{-1})mn^{-1} = (mn - m^2)n^{-2} = 1 - (n^2 - mn + m^2)n^{-2} \pmod{p^2}.$$

This congruence shows that $x(1-x) \equiv 1 \pmod{p^2}$ if and only if $n^2 - mn + m^2 \equiv 0 \pmod{p^2}$, which is equivalent to the statement of the lemma (in light of the first sentence of this proof). □

For $\varepsilon \in \{-1, 1\}$, define

$$\tilde{\mathcal{P}}_\varepsilon = \Bigg\{ p \text{ prime: there exist positive integers } n, m \text{ with } p \nmid m \text{ such that } p^2 \mid D_\varepsilon(n, m) \text{ but } p^2 \nmid \frac{n^2 - mn + m^2}{(m, n)^2} \Bigg\} \quad (11)$$

and

$$\tilde{\mathcal{P}}_{\text{cons}} = \{p \text{ prime: there exist consecutive nonzero } p\text{th powers modulo } p^2, \text{ other than } (x-1, x) \text{ where } x \text{ is a primitive sixth root of unity}\}. \quad (12)$$

For example, $\mathcal{P}_{\text{cons}}$ contains every prime congruent to 1 (mod 6) by Lemma 4.4; however, the smallest two primes in $\tilde{\mathcal{P}}_{\text{cons}}$ are 59 and 79. Note that $79 \equiv 1 \pmod{6}$ is still in $\tilde{\mathcal{P}}_{\text{cons}}$: even though we have ruled out the sixth roots of unity, there are still other pairs of consecutive nonzero 79th powers modulo 79^2. The intuition is that once all trivial square divisibilities (including those arising from cyclotomic factors) and trivial consecutive pth powers modulo p^2 (including those arising from primitive sixth roots of unity) have been accounted for, the sets $\tilde{\mathcal{P}}_\varepsilon$ and $\tilde{\mathcal{P}}_{\text{cons}}$ record only 'sporadic' square factors and consecutive pth powers.

The techniques of § 3, together with the additional results in this section, allow us to establish the following variant of Theorem 1.2; we omit the mostly redundant details.

THEOREM 4.6. *We have $\tilde{\mathcal{P}}_+ = \tilde{\mathcal{P}}_- = \tilde{\mathcal{P}}_{\text{cons}}$.*

The relationship between primitive sixth roots of unity and certain nonsquarefree values of $D_\pm(n, m)$ is not only an interesting and unexpected pattern, it also reduces the amount of explicit computation we have to do in subsequent sections.

We conclude this section by applying the strange divisibility in Proposition 4.3 to the construction of a new family of '*abc* triples'. Let $R(n)$ denote the radical of n, that is, the product of all the distinct primes dividing n, without multiplicity. Recall that the *abc conjecture* states that if a, b, c are relatively prime positive integers satisfying $a + b = c$, then $c \ll_\varepsilon R(abc)^{1+\varepsilon}$ for every $\varepsilon > 0$, or equivalently $R(abc) \gg_\varepsilon c^{1-\varepsilon}$ for every $\varepsilon > 0$. It is known that the more wishful inequality $R(abc) \geqslant \eta c$ is false for every constant $\eta > 0$, and it is useful to have simple families of examples that demonstrate its falsity. It turns out that we can construct such examples out of the divisibility exhibited in Proposition 4.3.

https://doi.org/10.1112/S1461157014000436 Published online by Cambridge University Press

LEMMA 4.7. *7^{k+1} divides $8^{7^k} - 1$ for any nonnegative integer k.*

Proof. We proceed by induction on k; the case $k = 0$ is trivial. When $k \geqslant 1$, we can write

$$8^{7^k} - 1 = (8^{7^{k-1}} - 1)(8^{6\cdot 7^{k-1}} + 8^{5\cdot 7^{k-1}} + \ldots + 8^{7^{k-1}} + 1).$$

The first factor on the right-hand side is divisible by 7^k by the induction hypothesis, while the second factor is congruent to $1+1+1+1+1+1+1$ (mod 7) and hence is divisible by 7. □

Note that simply setting $(a, b, c) = (1, 8^{7^k} - 1, 8^{7^k})$ yields

$$R(abc) = R(a)R(b)R(c) = 2R(b) \leqslant 2b/7^k < 2c/7^k = (2\log 8)c/\log c, \tag{13}$$

which (taking k large enough in terms of η) is enough to falsify any wishful inequality $R(abc) \geqslant \eta c$. The similar example $(a, b, c) = (1, 3^{2^k} - 1, 3^{2^k})$, attributed to Jastrzebowski and Spielman (see [**9**, pp. 40–41]), yields the inequality $R(abc) < (\frac{3}{2}\log 3)c/\log c$ that has a slightly better leading constant. We now give a new construction, different from the ones currently appearing in the literature, that results in an inequality of the same order of magnitude as these examples, but with a slightly worse leading constant. The specific form for n in the following construction was suggested by Carl Pomerance.

PROPOSITION 4.8. *Given any positive integer k, define $n = 8^{7^k}$ and*

$$a = (n-1)^{n-1}, \quad b = n^n - (n-1)^{n-1}, \quad c = n^n,$$

so that a, b, and c are pairwise relatively prime and $a + b = c$. Then $R(abc) < 6b/7^k n$. In particular,

$$R(abc) < 6\log 8\,\frac{c}{\log c}. \tag{14}$$

Proof. It suffices to establish the first inequality, since the second one follows upon noting that $b < c$ and $\log c = n\log n = n \cdot 7^k \log 8$. Obviously $R(c) = 2$; also, $R(a) = R(n-1)$, but $7^{k+1} \mid (n-1)$ by Lemma 4.7, and so $R(n-1) \leqslant (n-1)/7^k$. Equation (10) tells us that $((n^2 - n + 1)/3)^2$ divides b (note that $n \equiv 2$ (mod 6) because 7^k is odd), and so $R(b)$ is at most $b/((n^2 - n + 1)/3)$. Since a, b, and c are pairwise relatively prime, we conclude that

$$R(abc) = R(a)R(b)R(c) \leqslant \frac{n-1}{7^k}\,\frac{b}{(n^2-n+1)/3}\cdot 2 < \frac{6b}{7^k n}$$

as claimed. □

There do exist constructions of *abc* triples with noticeably smaller radicals (see the seminal paper [**18**] in this regard), although the methods to produce such triples are far more complicated than the elementary arguments given above.

5. *Orbits of roots*

In this section, we recall that a certain small group of automorphisms preserves the roots of the polynomial $f_p(x) = ((x+1)^p - x^p - 1)/p$ defined in equation (5). We then use this structure to justify a significant refinement of Conjecture 1.3, which we compare to data obtained from calculation.

LEMMA 5.1. *Let p be an odd prime, and let x be an integer such that $f_p(x) \equiv 0$ (mod p). Then $f_p(-x-1) \equiv 0$ (mod p). Furthermore, if $p \nmid x$ then $f_p(x^{-1}) \equiv 0$ (mod p), where x^{-1} is any integer satisfying $xx^{-1} \equiv 1$ (mod p).*

https://doi.org/10.1112/S1461157014000436 Published online by Cambridge University Press

Proof. Both assertions follow from the rational function identities

$$f_p(-x-1) = \frac{((-x-1)+1)^p - (-x-1)^p - 1}{p} = \frac{(-x)^p + (x+1)^p - 1}{p} = f_p(x)$$

and

$$x^p f_p(x^{-1}) = x^p \frac{(x^{-1}+1)^p - (x^{-1})^p - 1}{p} = \frac{(1+x)^p - 1 - x^p}{p} = f_p(x). \qquad \square$$

Each map $x \mapsto -x-1$ and $x \mapsto 1/x$ is an involution of $\mathbb{Z}(x)$, and it turns out that their composition has order 3. They therefore generate a group of six automorphisms of $\mathbb{Z}(x)$, characterized by their images of x:

$$x \mapsto x, \quad x \mapsto -x-1, \quad x \mapsto -\frac{1}{x+1}, \quad x \mapsto -\frac{x}{x+1}, \quad x \mapsto -\frac{x+1}{x}, \quad x \mapsto \frac{1}{x}.$$

One can also consider these as automorphisms of $\mathbb{Z}/p\mathbb{Z} \cup \{\infty\}$; the following proposition characterizes when some of the corresponding six images coincide. These observations have been made before, see for example [**14**, Lecture VIII, equation (1.3)].

LEMMA 5.2. *Let p be an odd prime, and let $x \in \mathbb{Z}/p\mathbb{Z} \cup \{\infty\}$. The orbit*

$$\left\{x, -x-1, -\frac{1}{x+1}, -\frac{x}{x+1}, -\frac{x+1}{x}, \frac{1}{x}\right\} \subset \mathbb{Z}/p\mathbb{Z} \cup \{\infty\}$$

consists of six distinct values except in the following cases:

- *every prime p has the orbit $\{0, -1, -1, 0, \infty, \infty\}$;*
- *every prime p has the orbit $\{1, -2, -2^{-1}, -2^{-1}, -2, 1\}$;*
- *every prime $p \equiv 1 \pmod 6$ has the orbit $\{\zeta, \zeta^{-1}, \zeta, \zeta^{-1}, \zeta, \zeta^{-1}\}$, where ζ is a primitive cube root of unity modulo p.*

These orbits are called the trivial orbit, the Wieferich orbit, and the cyclotomic orbit, respectively.

Proof. The lemma is easy to verify by setting the various pairs of images equal and solving for x, recalling that primitive cube roots of unity are precisely roots of the polynomial $x^2 + x + 1$. $\square$

Given an odd prime p, define a *six-pack* to be a set of six distinct elements of $\mathbb{F}_p$, of the form $\{x, -x-1, -1/(x+1), -x/(x+1), -(x+1)/x, 1/x\}$ all of which are roots of $f_p(x)$. Also recall that a *Wieferich prime* is a prime p for which $p^2 \mid (2^p - 2)$. To date, exhaustive computational search [**1**] up to 6.7×10^{15} has yielded only two Wieferich primes, namely 1093 and 3511. (An ongoing computational project [**17**] has extended this range to nearly 1.5×10^{17} as of August 2014.)

PROPOSITION 5.3. *When $p \equiv 1 \pmod 6$, the set of roots of $f_p(x)$ modulo p consists of $\{0, -1, \zeta, \zeta^{-1}\}$ together with zero or more disjoint six-packs, where ζ is a primitive cube root of unity; when $p \equiv 5 \pmod 6$, the set of roots of $f_p(x)$ modulo p consists of $\{0, -1\}$ together with zero or more disjoint six-packs. The only exceptions are Wieferich primes, for which $f_p(x)$ also has the roots $\{1, -2, -2^{-1}\}$ in addition to those described above.*

Proof. First, it is easy to check that 0, -1, and ζ and ζ^{-1} (when they exist) are indeed roots of $f_p(x)$; for the latter pair, it is useful to note that the converse of Lemma 4.4 also holds, namely that $\zeta + 1$ and $\zeta^{-1} + 1$ are primitive sixth roots of unity. Moreover, p divides $f_p(1) = (2^p - 2)/p$ if and only if p is a Wieferich prime. Therefore $f_p(x)$ has $\{1, -2, -2^{-1}\}$ as

https://doi.org/10.1112/S1461157014000436 Published online by Cambridge University Press

roots if and only if p if a Wieferich prime; here we use Lemmas 5.1 and 5.2 to justify that 1, -2, and -2^{-1} are either all roots or all nonroots of $f_p(x)$. Finally, by the same two lemmas, all remaining roots of $f_p(x)$ must come in six-packs. □

By Lemma 5.2, depending on whether $p \equiv 1 \pmod 6$ or $p \equiv 5 \pmod 6$, there are exactly $(p-7)/6$ or $(p-5)/6$ orbits in $\mathbb{F}_p$ other than the trivial, Wieferich, and cyclotomic orbits. For each such orbit, the values of f_p at the six elements of the orbit are all determined by any one of those values; in particular, the six values are simultaneously zero or simultaneously nonzero. Seeing no reason to think otherwise, we adopt the heuristic that each value has a $1/p$ probability of equaling any given element of $\mathbb{F}_p$, including 0.

What does this heuristic predict for the probability that f_p will have no six-packs of roots? Each of the $(p-7)/6$ or $(p-5)/6$ orbits has a $1-1/p$ probability of containing no roots of f_p. Under the further heuristic that these events are independent, we predict that the probability of f_p having no six-packs should be

$$\left\{\left(1-\frac{1}{p}\right)^{(p-7)/6} \text{ or } \left(1-\frac{1}{p}\right)^{(p-5)/6}\right\} \approx e^{-1/6}$$

when p is large. Indeed, a straightforward elaboration of this heuristic predicts that the number of six-packs for f_p should be given by a Poisson distribution with parameter $\frac{1}{6}$, that is, the probability of f_p having exactly k six-packs is $(\frac{1}{6})^k e^{-1/6}/k!$.

Furthermore, we predict that the number of six-packs for f_p is completely independent of whether p is congruent to 1 or 5 (mod 6). We additionally invoke the known heuristic that the Wieferich primes have density 0 within the primes. (Indeed, the number of Wieferich primes is suspected to go to infinity extremely slowly. Note, however, that we cannot even prove at this point that infinitely many primes are *not* Wieferich primes! See, for example, [**15**, Chapter 5, § III] and [**16**].) Together, these heuristics support the following conjecture.

Conjecture 5.4. Define $\rho(m)$ to be the relative density of the set of primes p for which f_p has exactly m roots (equivalently, for which there are exactly m pairs of consecutive pth powers modulo p^2). Then for every $k \geqslant 0$,

$$\rho(6k+2) = \frac{1}{2e^{-1/6}k!6^k} \quad \text{and} \quad \rho(6k+4) = \frac{1}{2e^{-1/6}k!6^k},$$

while $\rho(m) = 0$ for all $m \not\equiv 2, 4 \pmod 6$.

In particular, the relative density of $\tilde{\mathcal{P}}_{\text{cons}}$ within the primes is $1 - e^{-1/6} \approx 0.153\,518$, while the relative density of $\mathcal{P}_{\text{cons}}$ within the primes is $1 - \frac{1}{2}e^{-1/6} \approx 0.576\,759$.

As we see from its last assertion, Conjecture 5.4 is a significant refinement of Conjecture 1.3. Very little has been proved about the number of roots of f_p; the best that is known is that the number of roots is at most $2p^{2/3} + 2$ (see [**12**, Theorem 1], and check that the $L(x)$ therein equals our $f_p(-x)$; see also [**5**, Lemma 4]).

Table 1 shows that Conjecture 5.4 compares favorably with a calculation of all the roots of f_p for all odd primes p up to 1 million. (Note that the two known Wieferich primes 1093 and 3511 have 2 and 0 six-packs, respectively, as indicated by the single primes shown with $m = 19$ and $m = 7$.) This calculation of the roots of $f_p(x)$ was done simply by brute force, testing each of the p possibilities; each test can be done by raising both $x+1$ and x to the pth power modulo p^2, using fast modular exponentiation, and seeing whether $(x+1)^p - x^p$ is congruent to 1 (mod p^2).

We remark here on the importance of six-packs to the formulation of our conjecture. We started with the natural assumption that every x (mod p) has its own $1/p$ chance of being a

https://doi.org/10.1112/S1461157014000436 Published online by Cambridge University Press

TABLE 1. *Empirical evidence supporting Conjecture 5.4.*

Number of six-packs (k)	Number of roots of f_p (m)	Predicted frequency of f_p having m roots ($\rho(m)$)	Predicted number of primes $3 \leqslant p < 10^6$ with f_p having m roots	Actual number of primes $3 \leqslant p < 10^6$ with f_p having m roots
0	2	$\frac{1}{2}e^{-1/6} \approx 42.3\%$	33 223.1	33 316
	4	$\frac{1}{2}e^{-1/6} \approx 42.3\%$	33 223.1	33 387
	7	0	0	1
1	8	$\frac{1}{12}e^{-1/6} \approx 7.1\%$	5 537.2	5 477
	10	$\frac{1}{12}e^{-1/6} \approx 7.1\%$	5 537.2	5 356
2	14	$\frac{1}{144}e^{-1/6} \approx 0.59\%$	461.4	444
	16	$\frac{1}{144}e^{-1/6} \approx 0.59\%$	461.4	465
	19	0	0	1
3	20	$\frac{1}{2592}e^{-1/6} \approx 0.033\%$	25.6	29
	22	$\frac{1}{2592}e^{-1/6} \approx 0.033\%$	25.6	19
$\geqslant 4$	$\geqslant 26$	$\approx 0.0028\%$	2.2	2

root of $f_p(x)$. This led to the prediction that the relative density of $\tilde{\mathcal{P}}_{\text{cons}}$ within the primes would be $1-e^{-1} \approx 63.21\%$ rather than the figure 15.35% given in Conjecture 5.4. However, our initial computations of the zeros of $f_p(x)$ for primes less than 3000 showed that this prediction was badly off the mark. We noticed from this computation that the zeros of $f_p(x)$ generally occur in blocks of size six, and it was then easy to identify these as orbits of the little six-element group (abstractly S_3) described in Lemma 5.2. This naturally led to a revision of the probabilistic heuristic and to the revised Conjecture 5.4. Now that we have a conjecture that is empirically supported, it is amusing to reflect that our initially conjectured density was no more accurate than a random number chosen uniformly between 0 and 1.

The fact that the zeros of $f_p(x)$ generally occur in blocks of six has been known for some time. The polynomials $f_p(x)$ occur naturally in the study of the so-called 'first case' of Fermat's last theorem. In this connection, they were studied by Mirimanoff [**11**] who described explicitly the action of S_3 on the zeros. Helou [**6**] defined the Cauchy–Mirimanoff polynomial $E_n(x)$ to be the nontrivial factor of $(x+1)^n - x^n - 1$ that remains after removing any divisors among x, $x+1$, and x^2+x+1; he studied the question of whether $E_n(x)$ is irreducible over $\mathbb{Q}$, as have others (see, for example, [**21**]). Here $n \geqslant 2$ can be any integer, not necessarily prime. Helou gives a thorough discussion of the action of S_3 on the zeros of $E_n(x)$ when n is odd. These polynomials $E_n(x)$ themselves had already been defined for odd n by Cauchy in 1839 (see the references in [**6**]), but in those papers Cauchy did not discuss the action of S_3 on their zeros.

6. *Estimating the density of squarefree* $n^n + (-1)^n(n-1)^{n-1}$

In this section we concentrate on the quantity $D_{(-1)^n}(n,1) = n^n + (-1)^n(n-1)^{n-1}$, which as we have seen is the discriminant of the trinomial $x^n - x - 1$. There are sporadic nonsquarefree values in this sequence, as noted in the introduction, the first being $130^{130} + 129^{129}$ which is divisible by 83^2. Of course, by Lemma 3.1, any such example generates an entire residue class of examples (in this case, $83^2 \mid (n^n + (n-1)^{n-1})$ for all $n \equiv 130 \pmod{83 \cdot 82}$); in particular, a positive proportion of these values $n^n + (-1)^n(n-1)^{n-1}$ are not squarefree. Our goal for

https://doi.org/10.1112/S1461157014000436 Published online by Cambridge University Press

this section is to justify Conjecture 1.1, that the proportion of these values that are squarefree is 0.993 446 6 . . . .

DEFINITION 6.1. Define $\mathcal{S}$ to be the set of integers $n \geqslant 2$ for which $n^n + (-1)^n(n-1)^{n-1}$ is squarefree. For any real number $x > 2$, define $\mathcal{S}(x)$ to be the set of integers $n \geqslant 2$ for which $n^n + (-1)^n(n-1)^{n-1}$ is not divisible by the square of any prime less than x.

Let $\delta(\mathcal{A})$ denote the (natural) density of a set $\mathcal{A}$ of positive integers. We certainly have $\mathcal{S} \subseteq \mathcal{S}(x)$ for any $x > 2$, and thus $\delta(\mathcal{S}) \leqslant \delta(\mathcal{S}(x))$ for any x. We can rigorously bound $\delta(\mathcal{S}(x))$ using a finite computation and inclusion–exclusion, as we now describe.

For any distinct primes p and q, define the finite sets

$$\mathcal{C}_p = \{a \in \mathbb{Z}/p(p-1)\mathbb{Z} : a^a + (-1)^a(a-1)^{a-1} \equiv 0 \pmod{p^2}\} \tag{15}$$

(note that $\mathcal{C}_p$ is well defined by Lemma 3.1; the $(-1)^a$ factor causes no trouble since $p(p-1)$ is even) and

$$\mathcal{D}_{p,q} = \{(a,b) \in \mathcal{C}_p \times \mathcal{C}_q : \gcd(p(p-1), q(q-1)) \mid (a-b)\}. \tag{16}$$

The set $\mathcal{C}_p$ is similar to the sets $\mathcal{A}_{p,1,\varepsilon}$ defined in equation (8), although the factor $(-1)^a$ in the definition of $\mathcal{C}_p$ keeps the two objects from being identical; however, we certainly have $\mathcal{C}_p \subseteq \mathcal{A}_{p,1,+} \cup \mathcal{A}_{p,1,-}$.

PROPOSITION 6.2. *For any $x > 2$,*

$$1 - \sum_{p<x} \frac{\#\mathcal{C}_p}{p(p-1)} + \sum_{p<q<x} \frac{\#\mathcal{D}_{p,q}}{\operatorname{lcm}[p(p-1), q(q-1)]} - \sum_{p<q<r<x} \frac{\#\mathcal{D}_{p,q}\#\mathcal{C}_r}{\operatorname{lcm}[p(p-1), q(q-1), r(r-1)]}$$
$$\leqslant \delta(\mathcal{S}(x)) \leqslant 1 - \sum_{p<x} \frac{\#\mathcal{C}_p}{p(p-1)} + \sum_{p<q<x} \frac{\#\mathcal{D}_{p,q}}{\operatorname{lcm}[p(p-1), q(q-1)]},$$

where the variables p, q, and r run over primes satisfying the indicated inequalities.

Proof. For any integer d, define the set

$$\mathcal{M}_d = \{n \geqslant 2 : d^2 \mid (n^n + (-1)^n(n-1)^{n-1})\}.$$

Then by inclusion–exclusion,

$$\delta(\mathcal{S}(x)) = 1 - \sum_{p<x} \delta(\mathcal{M}_p) + \sum_{p<q<x} \delta(\mathcal{M}_{pq}) - \sum_{p<q<r<x} \delta(\mathcal{M}_{pqr}) + \ldots + (-1)^{\pi(x)} \delta(\mathcal{M}_{\prod_{p<x} p}).$$

(Inclusion–exclusion is most safely applied to finite counting problems rather than densities of infinite sets, but there are only finitely many sets in the above equation, so applying inclusion–exclusion to the densities is valid. In fact, every set in the above equation is a union of arithmetic progressions modulo $\prod_{p<x} p(p-1)$ by Lemma 3.1, and so their densities reduce to counting finitely many residue classes anyway.) More saliently, the Bonferroni inequalities [**3**, Chapter IV, § 5] provide the upper and lower bounds

$$1 - \sum_{p<x} \delta(\mathcal{M}_p) + \sum_{p<q<x} \delta(\mathcal{M}_{pq}) - \sum_{p<q<r<x} \delta(\mathcal{M}_{pqr})$$
$$\leqslant \delta(\mathcal{S}(x)) \leqslant 1 - \sum_{p<x} \delta(\mathcal{M}_p) + \sum_{p<q<x} \delta(\mathcal{M}_{pq}). \tag{17}$$

https://doi.org/10.1112/S1461157014000436 Published online by Cambridge University Press

Because $\mathcal{M}_p$ is a union of $\#\mathcal{C}_p$ residue classes modulo $p(p-1)$ by Lemma 3.1, the density of $\mathcal{M}_p$ equals $\delta(\mathcal{M}_p) = \#\mathcal{C}_p/p(p-1)$. Since $\mathcal{M}_{pq} = \mathcal{M}_p \cap \mathcal{M}_q$ when p and q are distinct primes, each pair of residue classes $a \pmod{p(p-1)}$ and $b \pmod{q(q-1)}$ either intersects in an arithmetic progression modulo $\operatorname{lcm}[p(p-1), q(q-1)]$ or else not at all; the former happens precisely when $a-b$ is divisible by $\gcd(p(p-1), q(q-1))$, which is exactly the condition for membership in $\mathcal{D}_{p,q}$. Consequently, the density of $\mathcal{M}_{pq}$ equals $\delta(\mathcal{M}_p) = \#\mathcal{D}_{p,q}/\operatorname{lcm}[p(p-1), q(q-1)]$ as well. We now see that the upper bound in equation (17) is equal to the upper bound in the statement of the proposition; also, all but the last sums in the lower bounds have also been evaluated.

Finally, a similar argument shows that $\mathcal{M}_{pqr}$, for distinct primes p, q, r, is the union of certain residue classes modulo $\operatorname{lcm}[p(p-1), q(q-1), r(r-1)]$; a given residue class in $\mathcal{D}_{p,q}$ combines with a given residue class in $\mathcal{C}_r$ to yield either one or zero such residue classes modulo $\operatorname{lcm}[p(p-1), q(q-1), r(r-1)]$. We obtain the upper bound $\#\mathcal{D}_{p,q}\#\mathcal{C}_r$ for the number of such residue classes simply by forgetting to check whether the residue classes in $\mathcal{D}_{p,q}$ and C_r are compatible. Thus we obtain the upper bound

$$\delta(\mathcal{M}_{pqr}) \leqslant \frac{\#\mathcal{D}_{p,q}\#\mathcal{C}_r}{\operatorname{lcm}[p(p-1), q(q-1), r(r-1)]},$$

which shows that the lower bound in equation (17) does imply the lower bound asserted in the proposition. □

We turn now to a description of how we calculated the sets $\mathcal{C}_p$ and $\mathcal{D}_{p,q}$ defined in equations (15) and (16). Calculating $\mathcal{C}_p$ directly from its definition would require testing $p(p-1)$ elements for every prime p; this quadratic growth would severely limit how many primes p we could calculate $\mathcal{C}_p$ for. Instead we use the bijections given in Theorem 3.6 to reduce the amount of computation necessary.

We begin by calculating, for a given prime p, all of the roots of $f_p(x)$, by brute force as described near the end of § 5. For each such root x, we replace x and $x-1$ with their pth powers modulo p^2, which will remain consecutive. We then test whether x is an element of $\mathcal{B}_{p,1,+} \cup \mathcal{B}_{p,1,-}$; that is, we check whether there exist integers $1 \leqslant k \leqslant p-1$ for which $x^k \equiv \pm(1-x) \pmod{p}^2$. Again we do this by brute force, checking each integer k in turn until we come to the order of x modulo p^2, which is a divisor of $p-1$. Once we have listed all the elements of $\mathcal{B}_{p,1,+} \cup \mathcal{B}_{p,1,-}$, we use the bijections of Theorem 3.6 to find all the elements of $\mathcal{A}_{p,1,+} \cup \mathcal{A}_{p,1,-}$, and finally we check each resulting element a individually to see whether the parity is appropriate—namely, whether $a^a + (-1)^a(a-1)^{a-1} \equiv 0 \pmod{p^2}$.

This calculation of $\mathcal{C}_p$ uses p (computationally easy) tests, followed by at most $p-1$ tests per root of f_p. Indeed, we may discard the trivial and cyclotomic roots of f_p, since we know from the earlier theory that these roots will never lead to prime squares dividing $n^n + (-1)^n(n-1)^{n-1}$; we need investigate only the sporadic roots. The number of sporadic roots of f_p is always small in practice: about 1 on average, and never more than 30 during our calculations.

Once the sets $\mathcal{C}_p$ had been calculated, we simply tested each element of every $\mathcal{C}_p \times \mathcal{C}_q$ directly to see whether it qualified for inclusion in $\mathcal{D}_{p,q}$. We carried out the above computations for all odd primes p and q less than 1 million; there are slightly fewer than 80 000 such primes, leading to the need to investigate a little over 3 billion pairs $\{p, q\}$.

With this information in hand, we calculate that

$$1 - \sum_{p<10^6} \frac{\#\mathcal{C}_p}{p(p-1)} + \sum_{p<q<10^6} \frac{\#\mathcal{D}_{p,q}}{\operatorname{lcm}[p(p-1), q(q-1)]} = 0.993\,446\,73\ldots$$

https://doi.org/10.1112/S1461157014000436 Published online by Cambridge University Press

while

$$\sum_{p<q<r<10^6} \frac{\#\mathcal{D}_{p,q}\#\mathcal{C}_r}{\operatorname{lcm}[p(p-1),q(q-1),r(r-1)]} < 5\times 10^{-9}.$$

In particular, the following inequalities follow from Proposition 6.2 and the fact that $\mathcal{S}\subseteq \mathcal{S}(10^6)$.

PROPOSITION 6.3. *The density $\delta(\mathcal{S}(10^6))$ of the set of positive integers n such that $n^n+(-1)^n(n-1)^{n-1}$ is not divisible by the square of any prime less than 1 million satisfies*

$$0.993\,446\,68 < \delta(\mathcal{S}(10^6)) < 0.993\,446\,74.$$

In particular, the density $\delta(\mathcal{S})$ of the set of positive integers n such that $n^n+(-1)^n(n-1)^{n-1}$ is squarefree satisfies

$$\delta(\mathcal{S}) < 0.993\,446\,74.$$

We cannot rigorously establish any nontrivial lower bound for $\delta(\mathcal{S})$; indeed, we cannot even prove that $n^n+(-1)^n(n-1)^{n-1}$ is squarefree infinitely often. Moreover, since the numbers $n^n+(-1)^n(n-1)^{n-1}$ grow so quickly that we cannot determine by direct factorization whether they are actually squarefree, direct numerical evidence on the density of squarefree values in this sequence is not available. However, we now present a heuristic that suggests that the upper bound for $\delta(\mathcal{S})$ in Proposition 6.3 is rather close to the truth.

CONJECTURE 6.4. The set $\mathcal{C}_p$ has one element on average over the primes, that is, $\sum_{p<x}\#\mathcal{C}_p\sim\pi(x)$.

Before justifying this last conjecture, we work out its implication for the density of $\mathcal{S}$. An argument similar to the proof of Proposition 6.2 convinces us that

$$1-\sum_{p>10^6}\frac{\#\mathcal{C}_p}{p(p-1)} \lesssim \frac{\delta(\mathcal{S})}{\delta(\mathcal{S}(10^6))} \lesssim 1-\sum_{p>10^6}\frac{\#\mathcal{C}_p}{p(p-1)}+\sum_{q>p>10^6}\frac{\#\mathcal{D}_{p,q}}{\operatorname{lcm}[p(p-1),q(q-1)]}.$$

Of course there will be some interaction between the specific residue classes in $\mathcal{C}_p$ for $p>10^6$ and the residue classes modulo smaller primes that we have already sieved out, just as for the intersection of two residue classes to any moduli s and t: most of the time they will not intersect at all, but $1/(s,t)$ of the time they will intersect in a total of (s,t) residue classes modulo st, so there is one residue class modulo st on average in the intersection. Therefore we find it a reasonable approximation to assume that the residue classes in $\mathcal{C}_p$ for these larger primes p are independent, on average, of the structure of $\mathcal{S}(10^6)$. By similar reasoning, we can simplify the last sum by postulating the same independence:

$$\begin{aligned}1-\sum_{p>10^6}\frac{\#\mathcal{C}_p}{p(p-1)} \lesssim \frac{\delta(\mathcal{S})}{\delta(\mathcal{S}(10^6))} &\lesssim 1-\sum_{p>10^6}\frac{\#\mathcal{C}_p}{p(p-1)}+\sum_{q>p>10^6}\frac{\#\mathcal{C}_p\#C_q}{p(p-1)q(q-1)}\\ &< 1-\sum_{10^6<p<10^9}\frac{\#\mathcal{C}_p}{p(p-1)}+\frac{1}{2}\Bigg(\sum_{p>10^6}\frac{\#\mathcal{C}_p}{p(p-1)}\Bigg)^2.\end{aligned}$$

Moreover, Conjecture 6.4 suggests that we can replace $\#\mathcal{C}_p$ by 1 on average, and so our estimates become

$$1-\sum_{p>10^6}\frac{1}{p(p-1)} \lesssim \frac{\delta(\mathcal{S})}{\delta(\mathcal{S}(10^6))} \lesssim 1-\sum_{10^6<p<10^9}\frac{1}{p(p-1)}+\frac{1}{2}\Bigg(\sum_{p>10^6}\frac{1}{p(p-1)}\Bigg)^2.$$

https://doi.org/10.1112/S1461157014000436 Published online by Cambridge University Press

A short computation yields

$$\sum_{10^6<p<10^9} \frac{1}{p(p-1)} \approx 6.773\,06 \times 10^{-8},$$

while

$$\sum_{p>10^9} \frac{1}{p(p-1)} < \sum_{n>10^9} \frac{1}{n(n-1)} = \frac{1}{10^9}.$$

We therefore estimate that

$$1 - 7 \times 10^{-8} \lesssim \frac{\delta(\mathcal{S})}{\delta(\mathcal{S}(10^6))} \lesssim 1 - 6 \times 10^{-8} + \frac{1}{2}(7 \times 10^{-8})^2.$$

Multiplying through by $\delta(\mathcal{S}(10^6))$ and using the bounds from Proposition 6.3, we conclude that

$$0.993\,446\,61 \lesssim \delta(\mathcal{S}) \lesssim 0.993\,446\,69,$$

which is the source of our belief in Conjecture 1.1.

Justification of Conjecture 6.4. By Theorem 3.6, the number of residue classes in $\mathcal{A}_{p,1,\pm}$ is the same as the number of ordered pairs $(x \pmod{p^2}, k \pmod{p-1})$, where x is a nonzero pth power modulo p^2 and $x^k \equiv \pm(x-1) \pmod{p^2}$. We expect the set $\mathcal{C}_p$ to comprise half of $\mathcal{A}_{p,1,\pm}$ on average, since there is one parity condition that must be checked. Since our heuristic will give the same answer for each choice of $\pm$ sign, we concentrate on the congruence $x^k \equiv x-1 \pmod{p^2}$ for the purposes of exposition; we expect the number of such pairs (x,k) to be equal to the cardinality of $\mathcal{C}_p$ on average.

The congruence $x^k \equiv x-1 \pmod{p^2}$ implies that $x-1$ is also a pth power modulo p^2, by Lemma 2.6. Also, since $x^n - x - 1$ is always irreducible by Lemma 4.1(a), we never have cyclotomic factors and thus (by Theorem 4.6) can ignore sixth roots of unity among our pairs of consecutive pth powers modulo p^2. Therefore, the discussion leading up to Conjecture 5.4, where we posit that the probability of f_p having exactly k six-packs of nontrivial roots is $(\frac{1}{6})^k e^{-1/6}/k!$, implies that the expected number of pairs of nontrivial consecutive pth powers modulo p^2 is

$$\sum_{k=1}^{\infty} \frac{1}{6^k e^{1/6} k!} \cdot 6k = \frac{1}{e^{1/6}} \sum_{k=1}^{\infty} \frac{1}{6^{k-1}(k-1)!} = 1.$$

Given a pth power $x \pmod{p^2}$ such that $x-1$ is also a pth power, it remains to investigate the expected number of $k \pmod{p-1}$ such that $x^k \equiv x-1 \pmod{p^2}$.

Note that the set of nonzero pth powers modulo p^2 is a cyclic subgroup of $(\mathbb{Z}/p^2\mathbb{Z})^\times$ of order $p-1$. In any given isomorphism between this subgroup and $\mathbb{Z}/(p-1)\mathbb{Z}$, we have no reason to believe that the images (discrete logarithms) of x and $x-1$ are correlated. Therefore, we assume that the expected number of such k is equal to the expected number of $k \pmod{p-1}$ such that $ky \equiv z \pmod{p-1}$, where y and z are chosen independently uniformly from $\mathbb{Z}/(p-1)\mathbb{Z}$. Indeed, the remainder of our analysis does not depend upon the fact that the modulus is one less than a prime, and so we determine the expected number of $k \pmod{N}$ such that $ky \equiv z \pmod{N}$, where y and z are chosen independently uniformly from $\mathbb{Z}/N\mathbb{Z}$.

Given y and z, the congruence $ky \equiv z \pmod{N}$ has no solutions k unless (y,N) divides z, in which case it has (y,N) solutions modulo N. For every divisor d of N, exactly $\phi(d)$ of the N residue classes $y \pmod{N}$ satisfy $(y,N) = d$; given d, the probability that $d \mid z$ is exactly $1/d$.

https://doi.org/10.1112/S1461157014000436 Published online by Cambridge University Press

Therefore the expected number of solutions to the congruence is

$$\sum_{d|N} \frac{\phi(d)}{N} \cdot \frac{1}{d} \cdot d = \frac{1}{N} \sum_{d|N} \phi(d) = 1.$$

Combining this calculation with our heuristic that there is one pair of consecutive nonzero pth powers modulo p^2 on average completes our justification of Conjecture 6.4. □

We conclude by remarking that similar methods can be applied to the problem of estimating how often $D_{\pm}(n, m)$ is squarefree, as both n and m vary. Since $D_{\pm}(n, m)$ is trivially not squarefree when m and n share a common factor, the natural quantity to investigate is the limiting proportion of relatively prime pairs (n, m) for which $D_{\pm}(n, m)$ is squarefree. The third author [**20**] has carried out calculations and heuristics, similar to those presented in this section, suggesting that this proportion is between 92% and 94%. However, the two-dimensional nature of the problem constrained the amount of computation that could be done directly, thereby limiting the precision of the estimates for the proportion.

Acknowledgements. The genesis of this work took place at the 1999 and 2000 Western Number Theory Conferences in Asilomar and San Diego, respectively; we thank the organizers of those conferences and their problem sessions, particularly Gerry Myerson and Jeff Achter for disseminating progress on these problems. We also thank Carlo Beenakker and Cam Stewart for helping us locate elementary examples of *abc* triples in the literature, and Carl Pomerance for his suggestion that improved and simplified Proposition 4.8.

References

1. F. G. Dorais and D. Klyve, 'A Wieferich prime search up to 6.7×10^{15}', *J. Integer Seq.* 14 (2011) no. 9, #11.9.2 (14 pp).
2. J. Esmonde and R. Murty, *Problems in algebraic number theory*, 2nd edn (Springer, New York, 2005).
3. W. Feller, *An introduction to probability theory and its applications*, 3rd edn (John Wiley & Sons, New York, 1968).
4. I. M. Gel'fand, M. M. Kapranov and A. V. Zelevinsky, *Discriminants, resultants, and multidimensional determinants*, Mathematics: Theory & Applications (Birkhäuser, Boston, 1994).
5. D. R. Heath–Brown, 'An estimate for Heilbronn's exponential sum', *Analytic number theory: Proceedings of a conference in honor of Heini Halberstam* (Birkhaüser, Boston, 1996) 451–463.
6. C. Helou, 'Cauchy–Mirimanoff polynomials', *C. R. Math. Rep. Acad. Sci. Canada* 19 (1997) no. 2, 51–57.
7. K. Kedlaya, 'A construction of polynomials with squarefree discriminants', *Proc. Amer. Math. Soc.* 140 (2012) no. 9, 3025–3033.
8. J. Lagarias, Problem 99:10 in 'Western number theory problems, 16 & 19 Dec 1999', Asilomar, CA (ed. G. Myerson), http://www.math.colostate.edu/∼achter/wntc/problems/problems2000.pdf.
9. S. Lang, 'Old and new conjectured Diophantine inequalities', *Bull. Amer. Math. Soc. (N.S.)* 23 (1990) no. 1, 37–75.
10. W. Ljunggren, 'On the irreducibility of certain trinomials and quadrinomials', *Math. Scand.* 8 (1960) 65–70.
11. D. Mirimanoff, 'Sur l'équation $(x + 1^l) - x^l - 1 = 0$', *Nouv. Ann. Math.* 3 (1903) 385–397.
12. D. A. Mit'kin, 'An estimate for the number of roots of some comparisons by the Stepanov method', *Mat. Zametki* 51 (1992) no. 6, 52–58; 157 (Russian); translation in *Math. Notes* **51** (1992), no. 5–6, 565–570.
13. H. Osada, 'The Galois groups of the polynomials $X^n + aX^l + b$', *J. Number Theory* 25 (1987) no. 2, 230–238.
14. P. Ribenboim, 13 *lectures on Fermat's last theorem* (Springer, New York, 1979).
15. P. Ribenboim, *The new book of prime number records* (Springer, New York, 1996).
16. J. H. Silverman, 'Wieferich's criterion and the *abc*-conjecture', *J. Number Theory* 30 (1988) 226–237.
17. R. Slatkevičius, PrimeGrid web site, http://www.primegrid.com; statistics on Wieferich prime search, http://prpnet.mine.nu:13000.
18. C. L. Stewart and R. Tijdeman, 'On the Oesterlé–Masser conjecture', *Monatsh. Math.* 102 (1986) no. 3, 251–257.

19. R. Swan, 'Factorization of polynomials over finite fields', *Pacific J. Math.* 12 (1962) 1099–1106.
20. M. Thom, 'Square-free trinomial discriminants', M.Sc. essay, University of British Columbia, Vancouver, 2011 (26 pp).
21. P. Tzermias, 'On Cauchy–Liouville–Mirimanoff polynomials', *Canad. Math. Bull.* 50 (2007) no. 2, 313–320.

David W. Boyd
Department of Mathematics
University of British Columbia
Room 121, 1984 Mathematics Road
Vancouver, BC
Canada V6T 1Z2
boyd@math.ubc.ca

Greg Martin
Department of Mathematics
University of British Columbia
Room 121, 1984 Mathematics Road
Vancouver, BC
Canada V6T 1Z2
gerg@math.ubc.ca

Mark Thom
Department of Mathematics & Computer Science
University of Lethbridge
C526 University Hall
4401 University Drive
Lethbridge, AB
Canada T1K 3M4
markjordanthom@gmail.com

https://doi.org/10.1112/S1461157014000436 Published online by Cambridge University Press