Abstract

The discriminant of a polynomial of the form $\pm x^n \pm x^m \pm 1$ has the form $n^n \pm m^m(n - m)^{n-m}$ when $n, m$ are relatively prime. We investigate when these discriminants have prime power divisors. We explain several symmetries that appear in the classification of these values of $n, m$. We prove that there are infinitely many pairs of integers $n, m$ for which this discriminant has no prime cube divisors. This result is extended to show that for infinitely many fixed $m$, there are infinitely many $n$ for which the discriminant has no prime cube divisor.

1 Introduction

The prime factorization of the discriminant of a polynomial is of vital importance in understanding its factorization in finite fields. In particular, it is known that if the discriminant of a polynomial $p(x)$ is squarefree and $\theta$ is an algebraic root of $p(x)$, then the full ring of integers of $\mathbb{Q}(\theta)$ is $\mathbb{Z}[\theta]$ and it is generated by the powers of the single element $\theta$ [2, p. 210, Exercise 4.2.8]. These types of results motivate research surrounding the prime factorization of the discriminant of polynomials.

Boyd et al. [1] examined discriminants of polynomials of the form $x^n \pm x^m \pm 1$, which take the form $n^n \pm m^m(n - m)^{n-m}$ when $n, m$ are relatively prime integers. In their paper, they proved a great deal of interesting number theoretical results about the squarefree values of these discriminants through analyzing the function

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

which is closely related to the discriminant in question if $\varepsilon \in \{-1, 1\}$. Boyd et al. studied the values of $D_\varepsilon(n, m) \pmod{p^2}$ for odd primes $p$ as a means of finding discriminants that are not squarefree, and using this number theoretical approach they showed that the values of $n, m$ can be treated as congruence classes modulo $p(p - 1)$ without altering the value
of $D_\varepsilon(n, m) \mod p^2$ [1, Lemma 3.1]. This result enables heuristic approximations of the relative frequency of squarefree values of $D_\varepsilon(n, m)$ and related functions, and this is carried out for the polynomial $x^n - n - 1$ [1, Conjecture 1.1]. In particular, it is conjectured that discriminants of these kinds of trinomials are squarefree infinitely often. In their treatment of $D_\varepsilon(n, m)$, Boyd et al. treated $p$ as a fixed odd prime, $m$ as fixed and relatively prime to $p$, and $\varepsilon \in \{-1, 1\}$ fixed and focused their number theoretical analysis primarily on $n$ with a secondary focus on situations where $m$ varies. Among many other interesting results, Boyd et al. prove a very useful relationship between the pairs of integers $n, m$ that satisfy $p^2 | D_\varepsilon(n, m)$ with the roots of the equation $(x + 1)^p \equiv x^p + 1 \pmod{p^2}$ [1, Theorem 3.6], which makes the primes $p$ for which non-trivial solutions arise a sort of generalization of the Wieferich primes, a well develop heuristic analysis of the asymptotic behavior of solutions to $D_\varepsilon(n, m)$ [1, Theorem 1.2, Theorem 4.6, Conjecture 5.4], and a new method of generating $abc$ triples [1, Proposition 4.8]. Shparlinski [4] has done further work on the special case of the polynomial $x^n - x - 1$, which has discriminant $n^n + (-1)^n(n - 1)^{n-1} = D_{-1}^{\varepsilon}(n, 1)$, and proves a lower bound on the number of squarefree parts of these discriminants, making partial progress towards the conjecture that these values are squarefree infinitely often.

The aim of this paper is to generalize the problem and ask when the discriminants $D_\varepsilon(n, m)$ have prime power divisors $p^k$, when $k$ is an integer greater than 1. We retain the convention that $\varepsilon \in \{-1, 1\}$ is a constant, and we assume that $p$ is an odd prime. Note that if $p^k | D_\varepsilon(n, m)$ then $n, m$ and $n-m$ are either all multiples of $p$ or all relatively prime to $p$. Since the case where all are divisible by $p$ is trivial, focus is placed on the case where $n, m, n-m$ are relatively prime to $p$, and this is taken to be a standard assumption throughout unless otherwise stated.

Since we seek to solve the equation $D_\varepsilon(n, m) \equiv 0 \pmod{p^k}$, a generalization of the equation $D_\varepsilon(n, m) \equiv 0 \pmod{p^2}$, it is reasonable to expect that many structural results about the latter equation will carry to the general case. This turns out to be correct, most importantly that when solving the equivalence $D_\varepsilon(n, m) \equiv 0 \pmod{p^k}$, the values of $n, m$ can be treated modulo $\phi(p^k) = p^{k-1}(p - 1)$. Once methods for evaluating the same equation in various prime power moduli are established, it is then very natural to ask whether there exists some test similar to Hensel’s lifting lemma, which shows precisely how to relate the roots of a polynomial modulo $p$ to roots of the same polynomial modulo powers of $p$. Since $D_\varepsilon(n, m)$ is not itself a polynomial, Hensel’s lifting lemma does not directly apply, but we show in Section 4 that there is a way to “lift” the modulus of the equation from $p^k$ to $p^{k+1}$ and keep track of the effects on solutions modulo $p^{k+1}$. Once these results are formulated and their consequences worked out, we can prove a weaker version of the conjectured infinitude of squarefree values of $D_\varepsilon(n, m)$.

**Theorem 1.** Let $\varepsilon \in \{-1, 1\}$ be given. Then the set $E = \{(n, m) \in \mathbb{N}^2 : D_\varepsilon(n, m) \text{ is cubefree}\}$ has nonzero density in $\mathbb{N}^2$. In particular, there are infinitely many such pairs.

The methods used to prove Theorem 1 can be extended to prove that $D_\varepsilon(n, m)$ is cubefree infinitely often for some fixed values of $m$, but not all fixed values of $m$. 

2
Section 2 of the paper is dedicated to proving key structural lemmas and helper lemmas. Section 3 gives more detailed exposition of the results of Boyd et al. most relevant to the problem of the higher power divisibilities, and uses the ideas developed, along with elementary number theoretical methods, to derive symmetries between different solutions to \( D_\varepsilon(n, m) \equiv 0 \pmod{p^k} \). Section 4 details how to take solutions to \( D_\varepsilon(n, m) \equiv 0 \pmod{p^k} \) and find all “corresponding solutions” to the equation \( D_\varepsilon(n, m) \equiv 0 \pmod{p^{k+1}} \), and some of the consequences of the “lifting lemmas” are expounded. The main results of the paper are then expounded and proven in Section 5, and some discussion about further work that could be done on the problem is provided in Section 6.

2 Preliminary Results

In this section, we prove a variety of basic facts that are useful for later results. We begin by analyzing expressions of the form \((A + Bp^a)^{A + p^a} \pmod{p^k}\), and in particular reducing these expressions to more manageable ones.

**Lemma 2.** Let \( p \) be an odd prime, \( A, B \) arbitrary integers, and \( a, k \) positive integers such that \( a < k \leq 2a \). Then we have

\[
(A + p^a B)^{A + p^a B} \equiv (1 + p^a B)^{A + p^a B} \pmod{p^k}.
\]

*Proof.* By the binomial theorem, we have that

\[
(A + p^a B)^{A + p^a B} \equiv \sum_{j=0}^{A + p^a B} \binom{A + p^a B}{j} A^{A + p^a B - j} B^j p^{aj} \pmod{p^k}. \tag{2.1}
\]

Now, since \( a < k \leq 2a \), we have \( p^a \not\equiv 0 \pmod{p^k} \) and \( p^{2a} \equiv 0 \pmod{p^k} \). Therefore, noting that the summation in 2.1 has a term \( p^{aj} \), the only terms which are potentially different from zero modulo \( p^k \) are the terms associated with \( j = 0 \) and \( j = 1 \). Therefore, we can further simplify equation 2.1:

\[
(A + p^a B)^{A + p^a B} \equiv A^{A + p^a B} + \binom{A + p^a B}{1} A^{A + p^a B - 1} (p^a B) \pmod{p^k} \\
\equiv A^{A + p^a B} + p^a B (A + p^a B) A^{A + p^a B - 1} \pmod{p^k} \\
\equiv (1 + p^a B) A^{A + p^a B} \pmod{p^k}.
\]

\[\square\]

**Lemma 3.** Let \( p \) be an odd prime, and let \( A, B \) be positive integers relatively prime to \( p \). Then we may construct from \( A, B, p \) the values \( d_0, d_1, d_2 \) such that

\[
(A + Bp(p - 1))^{A + Bp(p - 1)} \equiv d_0 + d_1 p + d_2 p^2 \pmod{p^3}.
\]

3
Note that this lemma, on its surface, only states that the number \((A + Bp(p-1))^{A+Bp(p-1)}\) can be written in base \(p\), which is trivial. The content of the lemma, then, is to determine precisely the values of \(d_0, d_1,\) and \(d_2\) given the constants \(A, B\). The proof of the lemma provides the mechanism for doing this, and at its end provides explicit formulas for \(d_0, d_1,\) and \(d_2\).

**Proof.** Since the term \(Bp(p-1)\) is a multiple of \(p\) and \(A\) is not (since \(A\) is relatively prime to \(p\)), any term \(Bp(p-1)\) to a power of three or higher is equivalent to zero modulo \(p^3\). Therefore, we have

\[
(A + Bp(p-1))^{A+Bp(p-1)} \equiv \sum_{j=0}^{A+Bp(p-1)} \binom{A+Bp(p-1)}{j} A^{A+Bp(p-1)-j} (Bp(p-1))^j \pmod{p^3}
\]

\[
\equiv \sum_{j=0}^{2} \binom{A+Bp(p-1)}{j} A^{A+Bp(p-1)-j} (Bp(p-1))^j \pmod{p^3}
\]

\[
\equiv 2^{-1}(A + Bp(p-1)-1)(A + Bp(p-1))A^{A+Bp(p-1)-2}B^2p^2(p-1)^2
\]

\[
+ (A + Bp(p-1))A^{A+Bp(p-1)-1}Bp(p-1) + A^{A+Bp(p-1)} \pmod{p^3},
\]

where the computation of the binomial coefficient \(\binom{A+Bp(p-1)}{2}\) modulo any odd number, and \(p\) is an odd prime. By Euler’s theorem, \(A^{p(p-1)} = \theta p^2 + 1\) for some positive integer \(\theta\), and therefore \(A^{Bp(p-1)} \equiv (1 + p^2\theta)^B \equiv 1 + p^2B\theta \pmod{p^3}\). Note further that \(p^2(p-1)^2 \equiv p^2 \pmod{p^3}\). Using these simplifications, in addition to distributing
terms and canceling multiples of $p^3$, we can continue the previous chain of simplifications:

$$(A + Bp(p - 1))^{A + Bp(p - 1)} \equiv 2^{-1}(A + Bp(p - 1) - 1)(A + Bp(p - 1))A^{A + Bp(p - 1) - 2}B^2p^2(p - 1)^2$$

$$+ (A + Bp(p - 1))A^{A + Bp(p - 1) - 1}Bp(p - 1) + A^{A + Bp(p - 1)} \pmod{p^3}$$

$$\equiv 2^{-1}(A + Bp(p - 1) - 1)(A + Bp(p - 1))A^{A - 2}(1 + p^2B\theta)B^2p^2$$

$$+ (A + Bp(p - 1))A^{A - 1}(1 + p^2B\theta)Bp(p - 1) + A^A(1 + p^2B\theta) \pmod{p^3}$$

$$\equiv 2^{-1}(A^A - A^A - 1)B^2p^2 + (A + Bp(p - 1))A^{A - 1}Bp(p - 1)$$

$$+ A^A(1 + p^2B\theta) \pmod{p^3}$$

$$\equiv (2^{-1}A^AB^2p^2 - 2^{-1}A^{-1}B^2p^2) + (A^ABp(p - 1) + A^{-1}B^2p^2)$$

$$+ (A^A + A^AB\theta p^2) \pmod{p^3}$$

$$\equiv (2^{-1}A^AB^2 - 2^{-1}A^{-1}B^2 + A^AB + A^{-1}B^2 + A^AB\theta)p^2$$

$$+ (-A^A)p + A^A \pmod{p^3}$$

$$\equiv (2^{-1}A^AB^2 + 2^{-1}A^{-1}B^2 + A^AB + A^AB\theta)p^2 + (-A^A)p + A^A \pmod{p^3}.$$ 

From the last line, we conclude that $d_0 \equiv A^A \pmod{p^3}$, $d_1 \equiv -A^AB \pmod{p^3}$, and $d_2 \equiv 2^{-1}A^AB^2 + 2^{-1}A^{-1}B^2 + A^AB + A^AB\theta \pmod{p^3}$. 

**Lemma 4.** Let $p, \varepsilon, k, n, m$ be defined as usual, and let $m', n'$ be integers so that $m' \equiv m \pmod{p^{k-1}(p - 1)}$ and $n' \equiv n \pmod{p^{k-1}(p - 1)}$. Then $p^k|D_\varepsilon(n, m)$ if and only if $p^k|D_\varepsilon(n', m')$.

**Proof.** Suppose that $p^k|D_\varepsilon(n, m)$. By the definition of modular equivalence, we can write $n' = n + tp^{k-1}(p - 1)$ for some integer $t$ and $m' = m + sp^{k-1}(p - 1)$ for some integer $s$. Now, we seek to show that $p^k|D_\varepsilon(n', m')$, or equivalently that $D_\varepsilon(n', m') \equiv 0 \pmod{p^k}$. Using the previously derived equations for $n', m'$ as substitutions, we have

$$D_\varepsilon(n', m') \equiv (n + tp^{k-1}(p - 1))^{n + tp^{k-1}(p - 1)}$$

$$+ \varepsilon(m + sp^{k-1}(p - 1))^{m + sp^{k-1}(p - 1)}(n - m + (t - s)p^{k-1}(p - 1))^{n - m + (t - s)p^{k-1}(p - 1)} \pmod{p^k}.$$ 

Now, the prior equation contains three components which fit the requirements of Lemma 2. In all three of these, we set $a = k - 1$. The first one sets $A = n$ and $B = t(p - 1)$, the second sets $A = m$ and $B = s(p - 1)$, and the third sets $A = n - m$ and $B = (t - s)(p - 1)$. Furthermore, note that if $\phi$ is the Euler phi function, then $p^{k-1}(p - 1) = \phi(p^k)$, and use this as a substitution. By applying Lemma 2 in each of these settings, we may write

$$D_\varepsilon(n', m') \equiv (1 + t\phi(p^k))^{n + t\phi(p^k)}$$

$$+ \varepsilon(1 + s\phi(p^k))(1 + (t - s)\phi(p^k))^{m + s\phi(p^k)}(n - m)^{n - m + (t - s)\phi(p^k)} \pmod{p^k}.$$
Furthermore, since we assume that $n, m$, and $n - m$ are each relatively prime to $p$, they are each invertible modulo $p^k$ and it follows from Euler’s theorem that

$$n^{t\phi(p^k)} \equiv m^{s\phi(p^k)} \equiv (n - m)^{(t-s)\phi(p^k)} \equiv 1 \pmod {p^k}. \quad (2.2)$$

Furthermore, since $k > 2$, we have $\phi(p^k)^2 \equiv 0 \pmod {p^k}$, and therefore

$$(1 + s\phi(p^k))(1 + (t-s)\phi(p)) \equiv 1 + (t-s)\phi(p) + s\phi(p^k) \equiv 1 + t\phi(p^k) \pmod {p^k}. \quad (2.3)$$

Therefore, from equations $2.2$ and $2.3$ it follows that

$$D_\varepsilon(n', m') \equiv (1 + t\phi(p^k))\left(n^n + \varepsilon m^m(n - m)^{n-m}\right) \pmod {p^k}$$

$$\equiv (1 + t\phi(p^k))D_\varepsilon(n, m) \pmod {p^k}.$$

Now since $p|\phi(p^k)$, it follows that $1 + t\phi(p^k)$ is relatively prime to $p$. Therefore, it follows that $D_\varepsilon(n', m') \equiv 0 \pmod {p^k}$ if and only if $D_\varepsilon(n, m) \equiv 0 \pmod {p^k}$. \hfill $\square$

**Lemma 5.** Let $D_\varepsilon(n, m) \equiv 0 \pmod {p^2}$ non-trivially, so that $n, m, n - m$ are all relatively prime to $p$. Then $n^{n-1} + \varepsilon m^m(n - m)^{n-m-1}$ is invertible modulo $p$.

**Proof.** Assume for the sake of argument that $n^{n-1} + \varepsilon m^m(n - m)^{n-m-1}$ is not invertible modulo $p$. Then since $p$ is prime, we can write $n^{n-1} + \varepsilon m^m(n - m)^{n-m-1} \equiv 0 \pmod {p}$. Now since $D_\varepsilon(n, m) \equiv 0 \pmod {p^2}$, we also have $D_\varepsilon(n, m) \equiv 0 \pmod {p}$, and by the transitive property of equivalence modulo $p$ we have

$$D_\varepsilon(n, m) \equiv n^{n-1} + \varepsilon m^m(n - m)^{n-m-1} \pmod {p}.$$  

Writing $D_\varepsilon(n, m) = n^n + \varepsilon m^m(n - m)^{n-m}$ and rearranging the above equation to put the isolated powers of $n$ on the left hand side, the equation becomes

$$n^{n-1}(n - 1) \equiv \varepsilon m^m(n - m)^{n-m-1}(m + 1 - n) \pmod {p}. \quad (2.4)$$

Based on the initial assumption, we may write $n^{n-1} \equiv -\varepsilon m^m(n - m)^{n-m-1} \pmod {p}$. Using this as a substitution for $n^{n-1}$ in equation $2.4$ and canceling the invertible terms $\varepsilon, m^m$, and $(n - m)^{n-m-1}$ from both sides, we obtain $-(n - 1) \equiv (m + 1 - n) \pmod {p}$. This reduces to $m \equiv 0 \pmod {p}$, a contradiction to the assumption that $m$ is relatively prime to $p$. Therefore, $n^{n-1} + \varepsilon m^m(n - m)^{n-m-1} \equiv 0 \pmod {p^2}$.

\hfill $\square$

### 3 Symmetries in $D_\varepsilon(n, m)$

The main goal of this section is to elaborate on the work of Boyd et al. in [1] about the values of $D_\varepsilon(n, m)$ and to use these properties to uncover several symmetries in the solutions to the equation $D_\varepsilon(n, m) \equiv 0 \pmod {p^k}$. To begin, we provide a statement of a crucial result of [1] that provides a sensible way to find all solutions to $D_\varepsilon(n, m) \equiv 0 \pmod {p^2}$.  

6
Theorem 6 (Theorem 3.6, [1]). Let \( m, \varepsilon, p \) be fixed, \( p \) an odd prime, and suppose \( p \nmid m \). Then there is a bijective correspondence between the values of \( n \) modulo \( p(p-1) \) which satisfy \( p^2 | D_\varepsilon(n, m) \) and pairs \((x \mod p^2), k \mod (p-1)\) such that \( x \) is a nonzero \( p \)th power modulo \( p^2 \) and \( x^k \equiv -\varepsilon(1-x)^m \mod (p^2) \). This bijection is given by the two functions

\[
\alpha_{p,m,\varepsilon}(n \mod p(p-1)) = (\text{the } p \text{th power modulo } p^2 \text{ such that } x \equiv 1 - mn^{-1} \mod (p), m - n \mod (p-1))
\]

and

\[
\beta_{p,m,\varepsilon}(x \mod p^2, k \mod p-1) = (m - k)p - m(1 - x)^{-1}(p-1) \mod (p(p-1)).
\]

where the inverse of \( 1 - x \) is taken modulo \( p^2 \).

It is shown in Corollary 3.4 of [1] that the conditions of \( x \) being a nonzero \( p \)th power modulo \( p^2 \) and \( x^k \equiv -\varepsilon(1-x)^m \mod (p^2) \) suffice to show that \( x-1 \) is also a \( p \)th power modulo \( p^2 \), and from Lemma 2.4 of [1] we conclude that the consecutive \( p \)th powers \( x, x-1 \) are \( p \)th powers of consecutive residue classes. Therefore, these \( p \)th powers modulo \( p^2 \) correspond to solutions to the equation

\[
(x + 1)^p \equiv x^p + 1 \mod (p^2).
\]

This equation is interesting in its own right, as it is a generalization of the notorious freshman’s dream identity, which states that for all primes \( p \) and all integers \( a, b \), the equivalence \((a+b)^p \equiv a^p + b^p \mod (p)\) holds. The equation of interest here, \((x+1)^p \equiv x^p + 1 \mod (p^2)\), is the same type of equation with the modulus a prime power rather than a prime. Currently, very little is known about the number of roots to this identity for any prime \( p \), the most notable result is that of Mit’kin, who shows that this equation has at most \( 2p^{2/3} \) solutions apart from \( x = -1, 0 \) [3, Theorem 1]. This theorem turns out to be useful in the context of the proof of Theorem 1, and so this upper bound will resurface in Section 5.

A further noteworthy observation is that since \( x-1 \) is a \( p \)th power modulo \( p^2 \), the validity of the equation \( x^k \equiv -\varepsilon(1-x)^m \mod (p^2) \) depends only on the residue class of \( m \) modulo \( p - 1 \). Therefore, any solution \((n, m)\) will generate a set of \( p - 1 \) solutions with the same \( n \) value and \( m \) ranging over the \( p - 1 \) possible values it might take modulo \( p \) while remaining fixed modulo \( p - 1 \) and relatively prime to \( p \). It also follows from this that when determining the set of all solutions to \( p^2 | D_\varepsilon(n, m) \), we need only perform tests for the values of \( m \) from 1 to \( p - 1 \), and solutions for values of \( m \) larger than this can be extrapolated from those test values.

Despite knowing very little about solutions to \((x+1)^p \equiv x^p + 1 \mod (p^2)\), there is a significant amount known about its structure. In order to talk about this equation more clearly, we define the polynomial

\[
f_p(x) = \frac{(x+1)^p - x^p - 1}{p}
\]
and look at this polynomial modulo \( p \), which by use of the freshman’s dream identity is logically equivalent to analyzing the equation \((x+1)^p \equiv x^p + 1 \pmod{p^2}\). It has been known for a long time that this polynomial satisfies the identities

\[
f_p(x) \equiv f_p(-x - 1) \equiv f_p(x^{-1}) \pmod{p}.
\]

The proof is given in [1] and is in fact mostly trivial. These identities induce orbits of the values of \( x \) modulo \( p \) for which \( f_p \) is constant. These orbits take the form

\[
\left\{ x, \frac{1}{x} - \frac{1}{x+1}, -\frac{x}{x+1}, -\frac{x+1}{x}, -x-1 \right\} \subset \mathbb{Z}/p\mathbb{Z}
\]

where, in this case, we are neglecting the orbit containing \( x = 0, -1 \). In most cases, these orbits exhibit six distinct elements. The exceptions are the case \( \zeta, \zeta^{-1} \) where \( \zeta \) is a primitive cube root of unity modulo \( p \), which exist for primes \( p \) equivalent to 1 modulo 6. These orbits are important because the image of \( f_p \) is constant under these orbits, and in fact if \((x, k)\) satisfies \( f_p(x) \equiv 0 \pmod{p} \) and \((x^p)^k \equiv -\varepsilon(1-x^p)^m \pmod{p^2}\), equivalent to the conditions in Theorem 6, then for each element \( y \) of the orbit of \( x \), we can construct some \( k' \) so that \((y, k')\) also satisfies the conditions of Theorem 6. Using this concept, we can start with a pair \((n, m)\) satisfying \( p^2|D_\varepsilon(n, m) \) and reconstruct other pairs \((n', m')\) that satisfy \( p^2|D_\varepsilon(n', m') \) that are closely related to \((n, m)\). The first of these resembles the correspondence between \( x \) and \(-x-1\).

**Proposition 7.** The pair of integers \( n, m \) satisfies \( D_\varepsilon(n, m) \equiv 0 \pmod{p^k} \) if and only if they also satisfy \( D_\varepsilon(-1)^m(m - n, m) \equiv 0 \pmod{p^k} \).

This proposition, as well as Proposition 8, can be proven in the case \( k = 2 \) by using the properties of \( f_p \) modulo \( p \) and Theorem 6. However, both of these can be proven using an elementary method that works for general \( k \). Since this method is both easier to use and more general in its scope, we present only this proof here.

**Proof.** The proof equivalence begins with a combination of a few simple factorization tricks:

\[
D_\varepsilon(-1)^m(m - n, m) \equiv (m - n)^{m-n} + \varepsilon(-1)^mm^m(-n)^{-n} \pmod{p^k}
\]

\[
\equiv (-1)^{m-n}(n - m)^{m-n} + \varepsilon(-1)^m-m^m n^{-n} \pmod{p^k}
\]

\[
\equiv n^{-n}(n - m)^{m-n}(-1)^{m-n} \left( n^n + \varepsilon m^m(n - m)^{n-m} \right) \pmod{p^k}
\]

\[
\equiv n^{-n}(n - m)^{m-n}(-1)^{m-n} D_\varepsilon(n, m) \pmod{p^k}.
\]

Since \( n^{-n}(n - m)^{m-n}(-1)^{m-n} \) is invertible modulo \( p^k \), we can also write \( D_\varepsilon(n, m) \equiv n^n(n - m)^{n-m}(-1)^{n-m} D_\varepsilon(-1)^m(m - n, n) \pmod{p^k} \). If either one of \( D_\varepsilon(n, m), D_\varepsilon(-1)^m(m - n, n) \) is equivalent to zero modulo \( p^k \), it follows that the other must be as well. 

**Proposition 8.** Assume \( n, m \) are integers which are invertible modulo \( p^{k-1}(p - 1) \). Then \( D_\varepsilon(n, m) \equiv 0 \pmod{p^k} \) if and only if \( D_\varepsilon(n^{-1}, m^{-1}) \equiv 0 \pmod{p^k} \).
Proof. Assume that \( D_\varepsilon(n^{-1}, m^{-1}) \equiv n^{-n-1} + \varepsilon m^{-m-1}(n^{-1} - m^{-1})n^{-1-m^{-1}} \equiv 0 \pmod{p^k} \). Multiplying that equivalence by \( n^{n-1}m^{-m-1} \), we obtain

\[
0 \equiv n^{-n-1}m^{n-1} + \varepsilon n^{-1-m^{-1}}m^{n-1-m^{-1}}(n^{-1} - m^{-1})n^{-1-m^{-1}} \pmod{p^k}
\]

\[
\equiv n^{-n-1}m^{n-1} + \varepsilon(m-n)^{n-1-m^{-1}} \pmod{p^k}.
\]

Now, rewrite this as \( n^{-m^{-1}}m^{n-1} \equiv -\varepsilon(m-n)^{n-1-m^{-1}} \pmod{p^k} \). Take both sides of this equation to the power \( nm \), and we then obtain \( n^{-n}m^m \equiv (1)^{nm} \varepsilon^{nm}(m-n)^{m-n} \pmod{p^k} \). We remark that since \( n,m \) are invertible modulo \( p^{k-1}(p-1) \), both \( n \) and \( m \) must be odd, so \( nm \) is odd, and \( (1)^{nm} = 1 \) and \( \varepsilon^{nm} = \varepsilon \). Therefore, we again rewrite the previous equation by \( n^{-n}m^m \equiv -\varepsilon(m-n)^{m-n} \pmod{p^k} \), or \( n^{-n}m^m + \varepsilon(m-n)^{m-n} \equiv 0 \pmod{p^k} \). Finally, we note that \( n - m \) is even and therefore \( (m-n)^{m-n} \equiv (1)^{m-n}(m-n)^{m-n} \equiv (n-m)^{m-n} \pmod{p^k} \), and we multiply this equation through by \( \varepsilon n^m(m-n)^{m-n} \), every term of which is invertible, and we obtain

\[
0 \equiv \varepsilon n^m(n-m)^{m-n} \equiv \varepsilon n^m(n-m)^{m-n} \equiv D_\varepsilon(n, m) \pmod{p^k}.
\]

If we let \( n,m \) take the roles of \( n^{-1},m^{-1} \), the proof is completely symmetric, and so the result follows. \qed

4 Lifting Equations for \( D_\varepsilon(n, m) \)

The purpose of this section is to demonstrate the relationship between solutions to the divisibility \( p^k|D_\varepsilon(n, m) \) and \( p^{k+1}|D_\varepsilon(n, m) \). In particular, the objective is to show how to construct all solutions to the \( k+1 \) case from the solutions to the \( k \) case. This process is referred to as lifting solutions from the modulus \( p^k \) to \( p^{k+1} \), a term which intentionally mirrors Hensel’s lifting lemma, which derives solutions to polynomial equivalences modulo a prime power from the solutions modulo a lower prime power.

Lemma 9. Suppose that \( p \) is an odd prime, \( k \geq 2 \) an integer, and residue classes \( n,m \) modulo \( p^{k}(p-1) \) which are relatively prime to \( p \). Then the divisibility \( p^{k+1}|D_\varepsilon(n, m) \) is true only if the residue classes \( n',m' \) modulo \( p^{k-1}(p-1) \) which satisfy \( n' \equiv n \pmod{p^{k-1}(p-1)} \) and \( m' \equiv m \pmod{p^{k-1}(p-1)} \) also satisfy \( p^{k}|D_\varepsilon(n', m') \).

Proof. Now \( n, m \) satisfy \( p^{k+1}|D_\varepsilon(n, m) \), and therefore they also satisfy \( p^{k}|D_\varepsilon(n, m) \). By Lemma 4, determining whether \( p^{k}|D_\varepsilon(n, m) \) requires only computing \( n, m \) modulo \( p^{k-1}(p-1) \). Therefore, any values \( n', m' \) equivalent to \( n, m \) modulo \( p^{k-1}(p-1) \) will satisfy \( p^{k}|D_\varepsilon(n', m') \). In particular, since \( 0 \leq n, m < p^{k}(p-1) \), we may uniquely positive integers \( n', m' \) less than \( p^{k-1}(p-1) \) and positive integers \( s, t \) less than \( p \) such that \( n = n' + tp^{k-1}(p-1) \) and \( m = m' + sp^{k-1}(p-1) \). Since \( n, m \) are equivalent to \( n', m' \) modulo \( p^{k-1}(p-1) \), this choice of \( n', m', s, t \) satisfies all requirements of the lemma. \qed
In less technical terms, this lemma asserts that any solution to the equivalence in question modulo $p^{k+1}$ corresponds in a unique way to a solution to the same equivalence modulo $p^k$. By taking the contrapositive, we find from the lemma that any values of $n, m$ which do not satisfy $p^k | D_\varepsilon(n, m)$ cannot be used to derive any solution to $p^{k+1} | D_\varepsilon(n, m)$.

It is the goal of the remainder of this section to provide an explicit method for lifting the solutions to the equivalence $D_\varepsilon(n, m) \equiv 0 \pmod{p^k}$ to the solutions to the equivalence $D_\varepsilon(n, m) \equiv 0 \pmod{p^{k+1}}$. Using $n', n$ in the same context as previously, the definition of modular equivalence tells us that $n = n' + tp^{k-1}(p-1)$ for some integer $t$, and since $n$ can be treated as a residue class modulo $p^k(p-1)$, it is evident that it suffices to restrict $t$ by $0 \leq t < p$. We can similarly write $m = m' + sp^{k-1}(p-1)$ with the restriction $0 \leq s < p$, and these equations are precisely the means by which values of $n', m'$ are transformed into values of $n, m$. The remainder of this section focuses on simplifying the expressions that result by writing $D_\varepsilon(n, m)$ by $D_\varepsilon(n' + tp^{k-1}(p-1), m' + sp^{k-1}(p-1))$ and exploring the consequences of doing this.

To begin this project, we state two important propositions that make the equation $D_\varepsilon(n + tp^{k-1}(p-1), m + sp^{k-1}(p-1)) \equiv 0 \pmod{p^{k+1}}$ more manageable.

**Proposition 10.** Suppose that $D_\varepsilon(n, m) \equiv 0 \pmod{p^2}$ under the standard assumptions about $n, m, \varepsilon, p$. Then the solutions to $D_\varepsilon(n + tp(p-1), m + sp(p-1)) \equiv 0 \pmod{p^3}$ are the solutions to a bivariate quadratic polynomial modulo $p$ with nontrivial $t^2$ coefficient, that is, an equation of the form

$$At^2 + Bs^2 + Cst + Dt + Es + F \equiv 0 \pmod{p}$$

with $A$ invertible modulo $p$.

**Proposition 11.** Suppose that $D_\varepsilon(n, m) \equiv 0 \pmod{p^k}$ for $k > 2$ under the standard assumptions about $n, m, \varepsilon, p$. Then the solutions to the equation

$$D_\varepsilon(n + tp^{k-1}(p-1), m + sp^{k-1}(p-1)) \equiv 0 \pmod{p^{k+1}}$$

are in bijective correspondence with the solutions to a bivariate linear polynomial of the form

$$\alpha t + \beta s + \gamma \equiv 0 \pmod{p}.$$ 

These two lemmas reduce the problem of lifting solutions to solving a bivariate quadratic and linear polynomials modulo $p$, which is a fairly straightforward task. Furthermore, as will be shown later, these polynomials can be used to put upper bounds on the total number of ways a given solution can lift to other solutions, which is vital in the proof of the main theorems in Section 5.

We prove the propositions in the opposite order in which they were presented, because the proof of Proposition 11 is simpler, and an understanding of this proof will help make the proof of Proposition 10 more clear.
Proof of Proposition 11. Define \( f(s, t) = D_\varepsilon(n + tp^{k-1}(p-1), m + sp^{k-1}(p-1)) \), and consider the equation
\[
f(s, t) \equiv 0 \pmod{p^{k+1}}. \tag{4.1}
\]
The proof begins with modifications to the left-hand side of equation 4.1. Now, applying the definition of \( D_\varepsilon(n, m) \) and observing that Lemma 2 and equation 2.3 both apply in this case (since for \( k > 2 \) we have \((k + 1)/2 \leq k - 1 < k + 1\)), we may perform the following simplifications to the left-hand side of 4.1:
\[
f(s, t) \equiv (n + t\varphi(p^k))^{n + t\varphi(p^k)} + \varepsilon(m + s\varphi(p^k)(m + s\varphi(p^k))^{n - m + (t - s)\varphi(p^k)})^{n - m + (t - s)\varphi(p^k)} \pmod{p^{k+1}}
\]
\[
\equiv (1 + t\varphi(p^k))(n^{n + t\varphi(p^k)} + \varepsilon m^{n + s\varphi(p^k)}(n - m)^{n - m + (t - s)\varphi(p^k)}) \pmod{p^{k+1}}. \tag{4.2}
\]
Now consider the quantity \( n^{t\varphi(p^k)} \). Treated as an integer, Euler’s theorem guarantees the existence of an integer \( \theta_n \) such that \( n^{\varphi(p^k)} = \theta_np^k + 1 \). Using this fact, it is clear that we must have
\[
n^{t\varphi(p^k)} \equiv (\theta_np^k + 1)^t \equiv t\theta_np^k + 1 \pmod{p^{k+1}}.
\]
This can be applied to \( m \) and \( n - m \), defining \( \theta_m, \theta_{n-m} \) in a similar way, and we obtain the following three equivalences:
\[
n^{t\varphi(p^k)} \equiv t\theta_np^k + 1 \pmod{p^{k+1}},
\]
\[
m^{s\varphi(p^k)} \equiv s\theta_mp^k + 1 \pmod{p^{k+1}},
\]
\[
(n - m)^{(t-s)\varphi(p^k)} \equiv (t - s)\theta_{n-m}p^k + 1 \pmod{p^{k+1}}.
\]
Applying these to equation 4.2 and further reducing modulo \( p^{k+1} \) via grouping terms by powers of \( p \) and distributions, we obtain
\[
f(s, t) \equiv (1 + t\varphi(p^k))\left(n^n(1 + t\theta_np^k) + \varepsilon m^n(n - m)^{n - m}(1 + s\theta_mp^k)(1 + (t - s)\theta_{n-m}p^k)\right) \pmod{p^{k+1}}
\]
\[
\equiv (1 + t\varphi(p^k))\left(n^n(1 + t\theta_np^k) + \varepsilon m^n(n - m)^{n - m}(1 + (s\theta_m + (t - s)(n-m)p^k))\right) \pmod{p^{k+1}}
\]
\[
\equiv (1 + t\varphi(p^k))\left(D_\varepsilon(n, m) + p^k\left(t\theta_n n^n + \varepsilon m^n(n - m)^{n - m}(s\theta_m + (t - s)\theta_{n-m})\right)\right) \pmod{p^{k+1}}
\]
\[
\equiv D_\varepsilon(n, m) + p^k\left(t\theta_n n^n + \varepsilon m^n(n - m)^{n - m}(s\theta_m + (t - s)\theta_{n-m})\right) \pmod{p^{k+1}}, \tag{4.3}
\]
where equation 4.3 follows since every term within the brackets multiplied by \( \varphi(p^k) \) is equivalent to 0 modulo \( p^{k+1} \). Now, we know that \( D_\varepsilon(n, m) \equiv 0 \pmod{p^k} \), and since every term of equation 4.3 is a multiple of \( p^k \) we can see that the roots of equation 4.1 must correspond to the roots of the equation
\[
t\theta_n n^n + \varepsilon m^n(n - m)^{n - m}(s\theta_m + (t - s)\theta_{n-m}) + \frac{D_\varepsilon(n, m)}{p^k} \equiv 0 \pmod{p}. \tag{4.4}
\]
Call the linear equation on the left-hand side of equation 4.4 $g(s,t)$. Now, noting that $\varepsilon m^n (n-m)^{n-m} = D_\varepsilon(n,m) - n^n$ by definition, we may write

$$g(s,t) \equiv t\theta_n n^n + (D_\varepsilon(n,m) - n^n)(s\theta_m + (t-s)\theta_{n-m}) + \frac{D_\varepsilon(n,m)}{p^k} \pmod p$$

$$\equiv n^n((\theta_n - \theta_{n-m})t + (\theta_{n-m} - \theta_m)s) + \frac{D_\varepsilon(n,m)}{p^k} \pmod p.$$  

Setting $\alpha = n^n(\theta_n - \theta_{n-m})$, $\beta = n^n(\theta_{n-m} - \theta_m)$, and $\gamma = \frac{D_\varepsilon(n,m)}{p^k}$ completes the proof. \(\Box\)

The proof of Proposition 10 uses the same approach as the proof of Proposition 11, and so an understanding of the approach is useful. The difficulty arises from the fact that when $k=2$, the inequality $(k+1)/2 \leq k-1 < k+1$ fails, and so Lemma 2 no longer applies. This increases the technical burden of simplifying the expression, but the approach used will be largely the same.

**Proof of Proposition 10.** Define $f(s,t) = D_\varepsilon(n+tp(p-1), m+sp(p-1))$, and consider the equation

$$f(s,t) \equiv 0 \pmod {p^3}. \quad (4.5)$$

The objective of the proof is to reduce $f(s,t)$ modulo $p^3$ in such a way that demonstrates that the roots of equation 4.5 correspond to the roots of a bivariate quadratic equation modulo $p$. Now, note that Lemma 3 provides a method of reducing modulo $p^3$ the three quantities that take the form $(A+Bp(p-1))^{A+Bp(p-1)}$ to the form $d_0 + d_1p + d_2p^2$, where $A^{p(p-1)} = \theta_A p^2 + 1$ defines the constant $\theta_A$, and

$$d_0 \equiv A^A \pmod {p^3},$$

$$d_1 \equiv -BA^A \pmod {p^3},$$

and

$$d_2 \equiv BA^A + 2^{-1} A^2 B + BA^A \theta_A + 2^{-1} A^{A-1} B^2 \pmod {p^3}.$$  

Let the three triples $(a_0, a_1, a_2), (b_0, b_1, b_2)$, and $(c_0, c_1, c_2)$ correspond to $(d_0, d_1, d_2)$ when $(n,t), (m,s)$, and $(n-m, t-s)$ correspond to $(A, B)$. So, for example, $a_1 = -tn^n, b_1 = -sm^m$, and $c_1 = -(t-s)(n-m)^{n-m}$. Using these three applications of Lemma 3, we can write

$$f(s,t) \equiv (a_0 + a_1p + a_2p^2) + \varepsilon(b_0 + b_1p + b_2p^2)(c_0 + c_1p + c_2p^2) \pmod {p^3}. \quad (4.6)$$

Now, equation 4.6 can be reduced by grouping terms based on powers of $p$. First, we consider all of the terms which have no explicit multiple of $p$:

$$a_0 + \varepsilon b_0 c_0 \equiv n^n + \varepsilon m^m (n-m)^{n-m} \equiv D_\varepsilon(n,m) \pmod {p^3}. \quad (4.7)$$
Secondly, we consider the collection of all terms in equation 4.6 that have exactly one explicit multiple of $p$:

\[
(a_1 + \varepsilon(b_0c_1 + b_1c_0))p \equiv (-tn^n + \varepsilon(m^m(n - m)^{n-m}(s - t) - sm^m(n - m)^{n-m}))p \pmod{p^3} \\
\equiv -t(n^n + \varepsilon m^m(n - m)^{n-m})p \pmod{p^3} \\
\equiv -tD_\varepsilon(n, m)p \pmod{p^3} \\
\equiv 0 \pmod{p^3}
\]  

since $D_\varepsilon(n, m) \equiv 0 \pmod{p^2}$. We now apply Lemma 3 to $f(s, t)$ and use equations 4.7 and 4.8 to simplify equation 4.6:

\[
f(s, t) \equiv (a_0 + a_1p + a_2p^2) + \varepsilon(b_0 + b_1p + b_2p^2)(c_0 + c_1p + c_2p^2) \pmod{p^3} \\
\equiv (a_0 + \varepsilon b_0c_0) + (a_1 + \varepsilon(b_0c_1 + b_1c_0))p + (a_2 + \varepsilon(b_0c_2 + b_1c_1 + b_2c_0))p^2 \pmod{p^3} \\
\equiv D_\varepsilon(n, m) + (a_2 + (b_0c_2 + b_1c_1 + b_2c_0))p^2 \pmod{p^3}. \tag{4.9}
\]

Now $p^2|D_\varepsilon(n, m)$ by hypothesis, so that $\frac{D_\varepsilon(n, m)}{p^2}$ is an integer. Now since every term in equation 4.9 is a multiple of $p^2$, this expression will be equivalent to 0 modulo $p^3$ if and only if

\[
a_2 + \varepsilon(b_0c_2 + b_1c_1 + b_2c_0) + \frac{D_\varepsilon(n, m)}{p^2} \equiv 0 \pmod{p}. \tag{4.10}
\]

Now by inspection, one find that the term $a_2$ is a quadratic polynomial in $t$, that $b_0c_2$ is a quadratic both in $t$ and $s$, $b_1c_1$ is a constant multiple of $st$, and $b_2c_0$ is a quadratic in $s$. It follows from this that there are no terms of degree three in this expression, therefore this is a bivariate quadratic in the two variables $s, t$, as claimed. In fact, the definitions of $a_i, b_i, c_i$ provided do allow the computation of every coefficient. However, having shown that this expression is in fact a bivariate quadratic is sufficient, and it remains only to show that the quadratic is nontrivial, and we show this by demonstrating that the coefficient on $t^2$ is invertible modulo $p$.

In the previous paragraph, it is noted that the only sources of $t^2$ terms derive from the terms $a_2$ and $\varepsilon b_0c_2$. Therefore, to find the total exponent of $t^2$ it suffices to determine the total coefficient of $t^2$ in these two expressions. Note that since no $t^2$ term will have a nonzero power of $s$, we may set $s = 0$ for this portion of the analysis. Setting $s = 0$, we can calculate

\[
a_2 \equiv tn^n + 2^{-1}n^nt^2 + tn^n\theta_n + 2^{-1}n^{n-1}t^2 \pmod{p^3}
\]

and

\[
\varepsilon b_0c_2 \equiv \varepsilon m^m\left(t(n-m)^{n-m}+2^{-1}(n-m)^{n-m}t^2+t(n-m)^{n-m}\theta_{n-m}+2^{-1}(n-m)^{n-m-1}t^2\right) \pmod{p^3}.
\]

From these, we can isolate all of the $t^2$ terms without any trouble, and we find that the $t^2$ coefficient, denoted here by $T$, is

\[
T \equiv 2^{-1}\left(n^n + n^{n-1} + \varepsilon m^m(n - m)^{n-m} + \varepsilon m^m(n - m)^{n-m-1}\right) \pmod{p}.
\]

13
Now this expression contains $n^n + \varepsilon m^m(n - m)^{n-m}$, which is identical to $D_\varepsilon(n, m)$, and so equivalent to 0 modulo $p$. Therefore, we may write

$$T \equiv 2^{-1}(n^{n-1} + \varepsilon m^m(n - m)^{n-m-1}) \pmod{p}. \quad (4.11)$$

Since $T$ is invertible modulo $p$ if and only if $T \not\equiv 0 \pmod{p}$, it will suffice to assume that $T \equiv 0 \pmod{p}$ and derive a contradiction, which will complete the proof.

Assume that $n^{n-1} + \varepsilon m^m(n - m)^{n-m-1} \equiv 0 \pmod{p}$. Multiplying both sides of this equation by $(n - m)$, which is valid since by hypothesis $n - m$ is relatively prime to $p$, yields

$$n^n - mn^{n-1} + \varepsilon m^m(n - m)^{n-m} \equiv 0 \pmod{p}. \quad \text{Since } n^n + \varepsilon m^m(n - m)^{n-m} = D_\varepsilon(n, m) \text{ by definition, which is equivalent to 0 modulo } p, \text{ we now have that } mn^{n-1} \equiv 0 \pmod{p}. \quad \text{But then it is the case that either } p|m \text{ or } p|n, \text{ a contradiction since } n, m \text{ are assumed to be relatively prime to } p. \quad \text{Therefore, it must be the case that } T \text{ is invertible modulo } p, \text{ and the proof of the proposition is complete.} \quad \square$$

Now, since solving polynomials modulo $p$ is a relatively simple exercise, these propositions provide a sufficiently easy way to lift the solutions to $D_\varepsilon(n, m) \equiv 0 \pmod{p^k}$ to the corresponding solutions modulo $p^{k+1}$. The only pitfall of these equations is that they do rely on knowledge of solutions modulo $p^k$ in order to compute the solutions modulo $p^{k+1}$. Attempts were made to generalize Theorem 6 to provide a more direct way of finding these solutions in higher moduli, but with no success. Were any generalization of this sort discovered, it would very likely lead to a lot of new insights into the problem, as well as probably strengthening all of the major results of this paper. However, even in the absence of such a result, these lifting equations do provide enough information to derive a result which will be of great importance.

**Corollary 12.** Suppose that $D_\varepsilon(n, m) \equiv 0 \pmod{p^2}$ with standard assumptions about $p, n, m, \varepsilon$. Then the pair of residue classes $(n, m)$ modulo $p(p-1)$ lifts to at most 2$p$ pairs of residue classes $(n', m')$ modulo $p^2(p-1)$ which satisfy $D_\varepsilon(n', m') \equiv 0 \pmod{p^3}$.

**Proof.** From Proposition 10, we have that the number of ways that $(n, m)$ lifts is in correspondence with the roots of a nontrivial bivariate quadratic polynomial in the variables $s, t$ taken modulo $p$. Now for every fixed value of $s$, since the coefficient of $t^2$ is invertible modulo $p$, it follows from the weaker form of the Fundamental Theorem of Algebra that the equation has at most 2 solutions for $t$. Since there are $p$ possible values of $s$ over which this process occurs, there are at most $2p$ solutions for the combination of variables $s, t$. \quad \square

## 5 Asymptotic Analysis of $D_\varepsilon(n, m)$

The upper bound on the number of ways a solution to $D_\varepsilon(n, m) \equiv 0 \pmod{p^2}$ can lift to solutions to $D_\varepsilon(n, m) \equiv 0 \pmod{p^3}$ turns out to be the final step needed to prove Theorem 1. Now that all the tools are in place, we begin the proof of the major result.
Proof of Theorem 1. First, we frame the question in the language of probability theory. Let $A_p$ represent the event $p^3|D_\varepsilon(n, m)$, and define $\delta$ to be the true probability that $D_\varepsilon(n, m)$ is not cubefree, which is identical to the density of the complement of $E$ in $\mathbb{N}^2$. With these definitions, the theorem is therefore proven if we can show that $\delta < 1$. Now, it follows from the inclusion-exclusion principle that

$$\delta \leq \sum_p P(A_p). \quad (5.1)$$

First, we remark that computing $P(A_p)$ can be simplified by introducing $B_p$, the event that $p|(n, m)$. Since whenever $A_p$ happens, either $B_p$ happens or it fails to happen, we may then write $P(A_p) = P(A_p \cap B_p) + P(A_p \cap B_p^C)$, where $X^C$ denotes the complement of event $X$. Therefore from equation (5.1) we conclude that

$$\delta \leq \sum_p P(A_p \cap B_p) + \sum_p P(A_p \cap B_p^C). \quad (5.2)$$

Now if $B_p$ is true, that is if $p|(n, m)$, then $p^3|n^2$ if $n > 2$ and $p^3|m^2$ if $m > 2$, there can only be finitely many cases where $B_p$ is true and $p^3|D_\varepsilon(n, m)$ fails, and these cases can be ignored in probability calculations. Therefore, $P(A_p \cap B_p) = P(B_p)$. If we let $\zeta_p(s) = \sum_{p} \frac{1}{p^s}$ denote the prime zeta function, it follows that

$$\sum_p P(A_p \cap B_p) = \sum_p P(B_p) = \zeta_p(2).$$

To complete the calculation of $\delta$ in equation (5.2), it remains only to calculate $P(A_p \cap B_p^C)$. Now, in order for $A_p \cap B_p^C$ to be true, it becomes clear that $p \not| nm(n - m)$, and under these assumptions we can use results from Section 4. In particular, Corollary 12 shows that if there are $N$ total pairs $(n, m) \pmod{p(p - 1)}$ that satisfy $p^3|D_\varepsilon(n, m)$, then there are at most $2pN$ such residue classes modulo $p^3(p - 1)$. Since by Lemma 4 this residue classification suffices to classify all of the solutions in $\mathbb{N}^2$, we may write $P(A_p \cap B_p^C) \leq \frac{2pN}{(p^3(p - 1))^2} = \frac{2pN}{p^4(p - 1)^2}$. To place a bound on $N$, note that in Theorem 6 and the comments that follow, the value of $N$ can be calculated by summing, for each $m$, the number of pairs $x \pmod{p^2}$, $k \pmod{(p - 1)}$ such that $x$ is not 0 or 1 and both of the equations $(x + 1)^p \equiv x^p + 1 \pmod{p^2}$ and $x^k \equiv -\varepsilon(1 - x)^m \pmod{p^2}$ are solved. From Mit’kin [3, Theorem 1], the first of these equations admits at most $2p^{2/3}$ solutions apart from 0, 1, and since the order of both $x$ and $1 - x \pmod{p^2}$ must be at least 2, at most half of possible values of $k, m$ can be solutions to this equation if the other is fixed. Therefore, $k$ has at most $\frac{p - 1}{2}$ possible values and $m$ has at most $\frac{p(p - 1)}{2}$ possible values. Therefore, taking all possibilities of $x, k, m$, we have

$$N \leq \left(2p^{2/3}\right)\left(\frac{p - 1}{2}\right)\left(\frac{p(p - 1)}{2}\right) = \frac{p^{5/3}(p - 1)^2}{2}.$$
Therefore, we have

\[ P(A_p \cap B_p^C) \leq \frac{(2p)^{5/3}(p-1)^2}{p^4(p-1)^2} = \frac{p^{8/3}}{p^4} = \frac{1}{p^{4/3}}. \]

As a final remark, it is straightforward to check, as has been done in [1], that the smallest value of \( p \) such that \( A_p \cap B_p^C \) can occur is \( p = 7 \), so the sum over primes for \( P(A_p \cap B_p^C) \) can be taken as a sum over primes \( p \geq 7 \). Therefore,

\[ \sum_p P(A_p \cap B_p^C) \leq \sum_{p \geq 7} \frac{1}{p^{4/3}} = \zeta_p(4/3) - \frac{1}{2^{4/3}} - \frac{1}{3^{4/3}} - \frac{1}{5^{4/3}}. \]

Therefore, applying the results of \( P(A_p \cap B_p) \) and \( P(A_p \cap B_p^C) \) to equation 5.2, we obtain

\[ \delta \leq \sum_p P(A_p \cap B_p) + \sum_p P(A_p \cap B_p^C) \leq \zeta_p(2) + \zeta_p(4/3) - \frac{1}{2^{4/3}} - \frac{1}{3^{4/3}} - \frac{1}{5^{4/3}} \approx 0.835418... < 1. \]

Therefore, since \( \delta < 1 \), the probability \( 1 - \delta \) of \( D_{\epsilon}(n, m) \) being cubefree is greater than 1, and therefore \( D_{\epsilon}(n, m) \) is cubefree infinitely often.

This then proves that there are infinitely many pairs \( (n, m) \) such that \( D_{\epsilon}(n, m) \) is cubefree. However, the related question of whether this is true for any fixed value of \( m \) remains open. In agreement with others who have worked on the problem, I would conjecture that every value of \( m \) has infinitely many values of \( n \) that make \( D_{\epsilon}(n, m) \) squarefree, and therefore infinitely many that make it cubefree as well. Unfortunately, the mechanics provided here are not sufficient to prove this conjecture for all fixed \( m \), but it does have sufficient power to prove the conjecture for large numbers of fixed values of \( m \). The remaining two theorems provide a classification of many values of \( m \) for which we can prove that \( D_{\epsilon}(n, m) \) is cubefree for infinitely many \( n \).

**Theorem 13.** Let \( \epsilon \in \{-1, 1\} \) be given, and let \( m = 2^a 3^b 5^c r \) be fixed such that \( (30, r) = 1 \). Then \( D_{\epsilon}(n, m) \) is cubefree infinitely often if we have

\[ \frac{\phi(m)}{m} + 2 \sum_{p | r} \frac{1}{p^{4/3}} > \Theta, \]

where \( \Theta = 2 \left( \zeta_p(4/3) - \frac{1}{2^{4/3}} - \frac{1}{3^{4/3}} - \frac{1}{5^{4/3}} \right) \).

**Proof.** Define \( \delta, A_p, B_p \) as in the previous proof. Then using the same logic as in the previous proof, we conclude that

\[ \delta \leq \sum_p P(A_p \cap B_p) + \sum_{p \geq 7} P(A_p \cap B_p^C). \]

With \( m \) fixed, we have

\[ \sum_p P(A_p \cap B_p) = \sum_p P(B_p) = P((n, m) > 1) = 1 - P((n, m) = 1) = 1 - \frac{\phi(m)}{m}, \]
where $\phi(m)$ is the Euler phi function of $m$. Also, remark that in the proof of Corollary 12, it is noted that for any fixed $m$, a value of $n$ modulo $p(p - 1)$ lift in at most two ways to a value modulo $p^2(p - 1)$. Therefore, if $N$ is the number of different values of $n$ modulo $p(p - 1)$ so that $p^2|D_\varepsilon(n, m)$, then there are at most $2N$ residue classes $n'$ modulo $p^2(p - 1)$ such that $p^3|D_\varepsilon(n', m)$. Furthermore, using the same analysis of Theorem 6 as in the proof of Theorem 1, ignoring the factor induced by the varying of $m$, we can write $N \leq \frac{(2p^{2/3})^{p - 1}}{2} = p^{2/3}(p - 1)$. Therefore, $P(A_p \cap B_p^C) \leq \frac{2p^{2/3}(p - 1)}{p^2(p - 1)} = \frac{2}{p^{4/3}}$. Additional constraints may be added, in particular, $B_p^C$ is impossible for any $m$ such that $p|m$, so these $p$ can be removed from the sum in addition to the primes 2, 3, and 5 (having been removed by the restraint $p \geq 7$). If we let $m = 2^a3^b5^cr$, where $(30, r) = 1$, we can write

$$\sum_p P(A_p \cap B_p^C) \leq \sum_{p \geq 7} \frac{2}{p^{4/3}} = 2\zeta_p(4/3) - 2\sum_{p|30} \frac{1}{p^{4/3}} - 2\sum_{p|r} \frac{1}{p^{4/3}}.$$  

For simplicity, write $\Theta = 2\zeta_p(4/3) - 2\sum_{p|30} \frac{1}{p^{4/3}} \approx 0.76634\ldots$. Applying these results to equation 5.3, we have

$$\delta \leq 1 - \frac{\phi(m)}{m} + \Theta - 2\sum_{p|r} \frac{1}{p^{4/3}}. \quad (5.4)$$

Now, we desire $\delta < 1$. This happens whenever $\delta - 1 < 0$. But from equation 5.4, we can see that

$$\delta - 1 \leq \Theta - \left(\frac{\phi(m)}{m} + 2\sum_{p|r} \frac{1}{p^{4/3}}\right).$$

Therefore, we can guarantee the result if the right hand side of the above inequality is itself less than zero, which implies that

$$\frac{\phi(m)}{m} + 2\sum_{p|r} \frac{1}{p^{4/3}} > \Theta. \quad (5.5)$$

Using the sufficient condition from Theorem 13, we can prove for infinitely many values of $m$ that $D_\varepsilon(n, m)$ is cubefree infinitely often.

**Theorem 14.** Let $\varepsilon \in \{-1, 1\}$ be given, and let $m = p_1^{a_1}p_2^{a_2}\ldots p_k^{a_k}$ be the prime factorization of $m$, with $p_1 < p_2 < \cdots < p_k$. Then $D_\varepsilon(n, m)$ is cubefree infinitely often if for any constant $1 \leq \ell \leq k$ and $m_\ell = \prod_{i=1}^{\ell-1} \left(1 - \frac{1}{p_i}\right)$ determined by $\ell$ and $m$, we have $m_\ell > \Theta$ and

$$p_\ell > \frac{1}{1 - \left(\Theta/m_\ell\right)^{1/(1-\varepsilon)}}.$$
Proof. Let $m, k, \ell$ be as defined, and assume that $m_\ell > \Theta$. Then we have

$$\frac{\phi(m)}{m} = \prod_{p | m} \left(1 - \frac{1}{p}\right) = \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \ldots \left(1 - \frac{1}{p_k}\right) \geq m_\ell \left(1 - \frac{1}{p_\ell}\right)^{k-\ell+1}.$$  

Now, if we can show that $m_\ell \left(1 - \frac{1}{p_\ell}\right)^{k-\ell+1} > \Theta$, then by Theorem ?? the proof is done, since then $\frac{\phi(m)}{m} > \Theta$. But, by the hypothesis, $p_\ell > \frac{1}{1 - (\Theta/m_\ell)^{k-\ell+1}}$. Isolating $\Theta$ in this inequality yields $m_\ell \left(1 - \frac{1}{p_\ell}\right)^{k-\ell+1} > \Theta$, which is precisely what is desired.  

Corollary 15. For all integers $k$, there are infinitely many values of $m$ having $k$ distinct prime factors and where $D_\epsilon(n, m)$ is cubefree infinitely often.

Proof. If $m$ is the product of $k$ distinct primes, with the smallest of these equal to $p$. Then by setting $\ell = 1$ in Theorem 14, $D_\epsilon(n, m)$ is cubefree infinitely often if $m_1 = 1 > \Theta$, which is trivially true, and

$$p > \frac{1}{1 - \Theta^1/k}.$$  

If $k$ is known, then $\frac{1}{1 - \Theta^1/k}$ is finite, and there are infinitely many primes $p$ that satisfy this inequality. There are infinitely many ways to choose a value of $m$ having $k$ distinct prime divisors with smallest prime divisor $p$, and therefore there are infinitely many values of $m$ such that $D_\epsilon(n, m)$ is cubefree infinitely often.  

6 Further Work

The question about whether there are infinitely many squarefree $D_\epsilon(n, m)$ remains very much open. As other authors have noted, this is a very difficult problem and it isn’t clear how to address the issue. If the methods of Section 5 are applied to this case, the result is an inequality of the form

$$\delta \leq \sum_p \frac{N}{p^2(p-1)^2},$$  

where $N$ the number of solutions $x, m, k$ given by Theorem 6. The upper bound that was used in this paper for this value is $N \leq \frac{p^{5/3}(p-1)^2}{2}$, which leads to the inequality

$$\delta \leq \sum_p \frac{p^{5/3}(p-1)^2}{2p^2(p-1)^2} = \frac{1}{2} \sum_p \frac{1}{p^{1/3}} \to \infty,$$  

18
so the method fails to obtain a finite sum, which is necessary to show that $\delta < 1$. The problem is that $O(N) = O(p^{11/3})$ and $O(p^2(p-1)^2) = O(p^4)$, and $O(p^{11/3}) / O(p^4) = O(p^{-1/3})$.

The series will only converge if the ratio involved is $O(p^{-1-\alpha})$ for some positive constant $\alpha$. So, in order for this method to work, the bound on $N$ must be reduced to $O(p^{3-\alpha})$, which could be accomplished by placing stronger bounds on either of the equations involved in Theorem 6. However, it is unclear how to obtain such bounds, and even if this new bound is obtained, extensive computation would still be necessary. In order to obtain a proof that would work without the need for extensive computations, we require $\sum_{p} N = O(p^{-1/3})$.

do this, we require $N \approx p^{13/5}$, and to reach this requires an improvement on the bound of $N$ by $O(p^{14/15})$. So, while this approach would suffice, it is very much unclear that such drastic reductions in the bounds are possible.

Another interesting problem that arises in this context is the question of which primes have any $(n, m)$ that satisfy $p^k | D_\varepsilon(n, m)$. For the case $k = 2$, this is equivalent to determining which primes $p$ have nontrivial roots for $(x+1)^p \equiv x^p + 1 \pmod{p^2}$. If $x = 1$ is a root of this equation, then $p$ is a Wieferich primes, and the form of the equation itself is a generalization of the freshman’s dream, which makes its solutions doubly interesting and worthy of study. Some heuristic results are known about the case $k = 2$, and there is nothing known when $k > 2$. Providing a mechanism similar to Theorem 6 for the cases $k > 2$ would probably provide a lot of information about these primes, but even for the case $k = 2$ very little is known.

### 7 Acknowledgements

I would like to thank the editors and referees for their work and their input to this paper. I would also like to thank Dr. Ezra Brown, whose number theory class led directly to my interest in this topic.

### References

[1] D. W. Boyd, G. Martin, and M. Thom, Squarefree values of trinomial discriminants, LMS J. Comput. Math. 18 (1) (2015) 148169.

[2] J. Esmonde and R. Murty, Problems in algebraic number theory, 2nd edn (Springer, New York, 2005).

[3] D. A. Mitkin, An estimate for the number of roots of some comparisons by the Stepanov method, Mat. Zametki 51 (1992) no. 6, 5258; 157 (Russian); translation in Math. Notes 51 (1992), no. 56, 565570.
[4] I. E. Shparlinski, Squarefree parts of discriminants of trinomials, Arch. Math. 102 (2014), 545 - 554.

2010 Mathematics Subject Classification: Primary 11R29; Secondary 11Z05.
Keywords: Discriminant, trinomial, cubefree.