

Algorithmic Arithmetic Fewnomial Theory I: One Variable (Extended Abstract)

Ashraf Ibrahim*

J. Maurice Rojas[†]

Korben Rusek[‡]

November 26, 2007

Summary

We show that deciding whether a sparse polynomial in one variable has a root in \mathbb{F}_p (for p prime) is **NP**-hard with respect to **BPP** reductions. As a consequence, we answer open questions on the factorization of sparse polynomials posed by Karpinski and Shparlinski, and Cox. We also derive analogous results for detecting p -adic rational roots, thus paralleling a recent complexity phase transition over the real numbers. A related new result is that detecting p -adic rational roots for a sparse polynomial in one variable is in **NP** for most inputs. Along the way, we also develop an efficient method for generating random primes in certain arithmetic progressions

In the sequel to this paper, we extend our complexity results to systems of multivariate polynomials.

*Department of Mathematics, Texas A&M University, TAMU 3368, College Station, Texas 77843-3368, USA. aibrahim@math.tamu.edu, www.math.tamu.edu/~aibrahim.

[†]Department of Mathematics, Texas A&M University, TAMU 3368, College Station, Texas 77843-3368, USA. rojas@math.tamu.edu, www.math.tamu.edu/~rojas. Partially supported by NSF individual grant DMS-0211458, NSF CAREER grant DMS-0349309, and Sandia National Laboratories.

[‡]Department of Mathematics, Texas A&M University, TAMU 3368, College Station, Texas 77843-3368, USA. korben@rusek.org, <http://www.rusek.org/korben>.

1 Introduction and Main Results

In recent work, Bihan, Rojas, and Stella derived a new complexity threshold — from polynomial time to **NP**-hardness — for deciding the existence of real roots for sparse polynomials [BRS07]. Here, we derive even sharper thresholds over the fields \mathbb{F}_p and \mathbb{Q}_p (see Theorems 1.4 and 1.8 in Sections 1.1–1.2 below). As a consequence, we answer questions posed earlier by Karpinski and Shparlinski [KaShp99], and Cox [Cox04], on detecting linear, repeated, and common factors for sparse polynomials over finite fields (see Sections 1.1–1.2 below).

For any commutative ring R with multiplicative identity, we let FEAS_R — the *R*-feasibility problem — denote the problem of deciding whether an input polynomial system $F \in \bigcup_{k,n \in \mathbb{N}} (\mathbb{Z}[x_1, \dots, x_n])^k$ has a root in R^n . (See Definition 1.2 below for a precise statement of the underlying input size.) $\text{FEAS}_{\mathbb{R}}$, $\text{FEAS}_{\mathbb{Q}}$, and $\{\text{FEAS}_{\mathbb{F}_q}\}_{q \text{ a prime power}}$ are central problems respectively in algorithmic real algebraic geometry, algorithmic number theory, and cryptography.

Definition 1.1 *We let $\mathcal{F}_{n,m}$ denote the subset of $\mathbb{Z}[x_1, \dots, x_n]$ consisting of polynomials with exactly m monomial terms, and let \mathbb{P} be the set of all primes in \mathbb{N} . \diamond*

It is then clear, for instance, that $\mathbb{Z}[x_1]$ is the disjoint union $\bigsqcup_{m \geq 0} \mathcal{F}_{1,m}$.

1.1 NP-Hardness in One Variable for Prime Fields

It has long been known, via classical reductions and efficient finite field arithmetic (see, e.g., [BS96, Ch. 5]), that deciding the existence of solutions for polynomial equations over finite fields with a prime number of elements is **NP**-complete. However, the precise threshold for when the number of variables is large enough to make this feasibility question **NP**-hard seems to have remained unknown. Our first main result answers this question, modulo some randomization.

Definition 1.2 *Let $f(x) := \sum_{i=1}^m c_i x^{a_i} \in \mathbb{Z}[x_1, \dots, x_n]$ where $x^{a_i} := x_1^{a_{1,i}} \cdots x_n^{a_{n,i}}$, $c_i \neq 0$ for all i , and the a_i are pair-wise distinct. We call such an f an **n -variate m -nomial**. Also let*

$$\text{size}(f) := \sum_{i=1}^m \log_2 [(2 + |c_i|)(2 + |a_{1,i}|) \cdots (2 + |a_{n,i}|)]$$

and, for any $F := (f_1, \dots, f_k) \in (\mathbb{Z}[x_1, \dots, x_n])^k$, define $\text{size}(F) := \sum_{i=1}^k \text{size}(f_i)$.

For instance, $\text{size}(1 + cx^{99} + x^d) = \Theta(\log(c) + \log(d))$. So the degree, $\deg f$, of a polynomial f can sometimes be exponential in its size.

Definition 1.3 *Let $\text{FEAS}_{\mathbb{F}_{\text{primes}}}$ denote the problem of deciding, for an input polynomial system $F \in \bigcup_{k,n \in \mathbb{N}} (\mathbb{Z}[x_1, \dots, x_n])^k$ and an input prime p , whether F has a root in \mathbb{F}_p^n . Also let $\text{FEAS}_{\mathbb{F}_{\text{primes}}}(\mathcal{I})$ denote the natural restriction of $\text{FEAS}_{\mathbb{F}_{\text{primes}}}$ to inputs in \mathcal{I} . Also, when \mathcal{F} is a family of polynomial systems, we will abuse notation slightly by letting $\text{FEAS}_{\mathbb{F}_{\text{primes}}}(\mathcal{F})$ denote the restriction of $\text{FEAS}_{\mathbb{F}_{\text{primes}}}$ to inputs in $\mathcal{F} \times \mathbb{P}$. The underlying input size for all these problems is $\text{size}_p(F) := \text{size}(F) + \log p$. \diamond*

Since brute force enumeration easily shows that $\text{FEAS}_{\mathbb{F}_p}(\mathbb{Z}[x_1]) \in \mathbf{P}$ when p is fixed, it is natural to consider p as part of the input and work with $\text{FEAS}_{\mathbb{F}_{\text{primes}}}$ and size_p instead of $\text{FEAS}_{\mathbb{F}_p}$ and size . Our notations size and size_p are also sometimes referred to as the **sparse encoding** or **bit-size**. In particular, while it has been known since the late 1960s that one can factor arbitrary polynomials $f \in \mathbb{F}_p[x_1]$ in randomized time polynomial in $\deg f$ and $\log p$ (see, e.g., [BS96, Ch. 7] and [CZ81, Gao05]), the algorithmic complexity in terms of the **sparse encoding** — even for finding just the linear factors — was an open problem until now.

Theorem 1.4 *If $\text{FEAS}_{\mathbb{F}_{\text{primes}}}(\mathbb{Z}[x_1]) \in \mathbf{BPP}$ then $\mathbf{NP} \subseteq \mathbf{BPP}$.*

That $\text{FEAS}_{\mathbb{F}_{\text{primes}}}(\mathbb{Z}[x_1]) \in \mathbf{NP}$ is folkloric. The same can be said for $\text{FEAS}_{\mathbb{F}_{\text{primes}}}(\mathcal{F}_{1,2}) \in \mathbf{P}$ (see, e.g., [BS96, Thm. 5.7.2 & Thm. 5.6.2, pg. 109] or Lemma 5.2 in the Appendix below). However, the complexity of $\text{FEAS}_{\mathbb{F}_{\text{primes}}}(\mathcal{F}_{1,m})$ for larger **fixed** m (even $m=3$ [Kal03]) appears to remain unknown, even though it is known that $\text{FEAS}_{\mathbb{R}}(\mathcal{F}_{1,3}) \in \mathbf{P}$ [BRS07].

Letting $\text{FEAS}_{\mathbb{F}_{\text{prime powers}}}$ denote the natural extension of $\text{FEAS}_{\mathbb{F}_{\text{primes}}}$ to **arbitrary** finite fields, Theorem 1.4 significantly sharpens earlier results stating (in our notation) that $\text{FEAS}_{\mathbb{F}_{\text{prime powers}}}((\mathbb{Z}[x_1])^2)$ and $\text{FEAS}_{\mathbb{F}_{\text{prime powers}}}(\mathbb{Z}[x_1])$ are **NP-hard** under randomized reductions (see [vzGKS96, Sec. 4, Top of Pg. 17], [KK05, Prop. 2], and [KiSha99, Lemma 3.3]). In particular, [KiSha99] proves **NP-completeness** for $\text{FEAS}_{\mathbb{F}_{\text{prime powers}}}(\mathbb{Z}[x_1])$ by a clever construction over the rings $\{\mathbb{F}_{2^k}[x_1]\}_k$, and describes how this enables attacks on certain cryptosystems. Theorem 1.4 also provides strong evidence for a negative answer to an earlier question of David A. Cox [Cox04]: (in our notation) Is $\text{FEAS}_{\mathbb{F}_{\text{primes}}}(\mathbb{Z}[x_1]) \in \mathbf{P}$?

As a consequence of an intermediate reduction in the proof of Theorem 1.4, we obtain the following.

Corollary 1.5 *Using size_p as our notion of input size, suppose we can decide within **BPP**, for any input prime p and polynomials $f, g \in \mathbb{Z}[x_1]$, whether the mod p reduction of $\text{gcd}(f, g)$ has positive degree. Then $\mathbf{NP} \subseteq \mathbf{BPP}$. Similarly, if we can decide within **BPP**, for any input prime p and $f \in \mathbb{Z}[x_1]$, whether the factorization of f over $\mathbb{F}_p[x_1]$ is square-free, then $\mathbf{NP} \subseteq \mathbf{BPP}$.*

Karpinski and Shparlinski proved **NP-hardness** (with respect to randomized reductions) of detecting square-freeness over the rings $\{\mathbb{F}_q[x_1]\}_q$ a prime power [KaShp99, Thm. 2 and Sec. 3], and asked whether the same complexity lower bound held over the subset of rings $\{\mathbb{F}_p[x_1]\}_p$ prime. They also observed the lack of an analogous result for univariate gcd over finite fields. Corollary 1.5 thus answers their questions affirmatively.

We now describe how the preceding complexity lower bounds can be made even sharper, and admit complementary speed-ups, by working over a different family of fields.

1.2 The Ultrametric Side: Relevance and Results

The fields \mathbb{R} and \mathbb{Q}_p (the reals and the p -adic rationals) bear more in common than just completeness with respect to a metric: increasingly, complexity results for one field have inspired and motivated analogous results in the other. Perhaps the first instance of this transfer was the work of Paul Cohen, on quantifier elimination over \mathbb{R} and \mathbb{Q}_p [Coh69]. More recently, following Khovanski's Theorems on Real Fewnomials and Complex Fewnomials [Kho91], Rojas found analogous theorems over \mathbb{Q}_p and \mathbb{C}_p with sharper bounds [Roj04].¹ (Khovanski's results are a vast, higher-dimensional generalization of the fact that a univariate polynomial f , with real coefficients and exactly m monomial terms, can have no more than $2m - 1$ real roots — a bound completely independent of the degree of f .) So let us briefly outline the importance of $\text{FEAS}_{\mathbb{Q}_p}$.

First recall that the decidability of $\text{FEAS}_{\mathbb{Q}}$ is an open problem: solving the special case of cubic polynomials in two variables is already enough to yield new results in the direction of the famous Birch-Swinnerton-Dyer conjecture (see, e.g., [Sil96, Ch. 8]), and the latter conjecture is central in modern number theory (see, e.g., [HS00]). The fact that $\text{FEAS}_{\mathbb{Z}}$ is undecidable is the well-known negative solution of Hilbert's Tenth Problem, due to Matiyasevitch and Davis, Putnam, and Robinson (see, e.g., [Mat73, DLPvG00]), and is sometimes taken as evidence that $\text{FEAS}_{\mathbb{Q}}$ may be undecidable as well (see also [Poo03, Poo07]).

¹This advance also extended earlier seminal results of Denef and van den Dries [DvdD88], Lipshitz [Lip88], and Lenstra [Len99a, Len99b].

From a more positive perspective, much work has gone into using p -adic methods to algorithmically detect rational points on algebraic plane curves via variations of the **Hasse Principle**² (see, e.g., [C-T98, Poo01b, Poo06]). Algorithmic results over the p -adics are also central in many other computational results: polynomial time factoring algorithms over $\mathbb{Q}[x_1]$ [LLL82], computational complexity [Roj02], studying prime ideals in number fields [Coh94, Ch. 4 & 6], elliptic curve cryptography [Lau04], and the computation of zeta functions [CDV06].

So we now present a p -adic analogue of Theorem 1.4 that gives an even sharper complexity threshold between **P** and **NP**. In particular, we also give an algorithmic speed-up that holds for a large set of input polynomials. The exceptions appear to be due to the presence of **ill-conditioned** polynomials: f having a root ζ with the (p -adic) norm of $f'(\zeta)$ very small — a phenomenon of approximation present in complete fields like \mathbb{R} and \mathbb{C} , but **not** present over finite fields.

Definition 1.6 Let $\text{FEAS}_{\mathbb{Q}_{\text{primes}}}$ denote the problem of deciding, for an input polynomial system $F \in \bigcup_{k,n \in \mathbb{N}} (\mathbb{Z}[x_1, \dots, x_n])^k$ and an input prime p , whether F has a root in \mathbb{Q}_p^n . Also let $\text{FEAS}_{\mathbb{Q}_{\text{primes}}}(\mathcal{I})$ denote the natural restriction of $\text{FEAS}_{\mathbb{Q}_{\text{primes}}}$ to inputs in \mathcal{I} . Also, when \mathcal{F} is a family of polynomial systems, we will abuse notation slightly by letting $\text{FEAS}_{\mathbb{Q}_{\text{primes}}}(\mathcal{F})$ denote the restriction of $\text{FEAS}_{\mathbb{Q}_{\text{primes}}}$ to inputs in $\mathcal{F} \times \mathbb{P}$. The underlying input size for all these problems is $\text{size}_p(F)$ (cf. Definition 1.3). Finally, let $(\mathbb{Z} \times (\mathbb{N} \cup \{0\}))^\infty$ denote the set of all infinite sequences of pairs $((c_i, a_i))_{i=1}^\infty$ with $c_i = a_i = 0$ for i sufficiently large. \diamond

Remark 1.7 Note that $\mathbb{Z}[x_1]$ admits a natural embedding into $(\mathbb{Z} \times (\mathbb{N} \cup \{0\}))^\infty$ by considering coefficient-exponent pairs in order of increasing exponents, e.g.,

$$a + bx^{99} + x^{2001} \mapsto ((a, 0), (b, 99), (1, 2001), (0, 0), (0, 0), \dots). \quad \diamond$$

Theorem 1.8

1. $\text{FEAS}_{\mathbb{Q}_{\text{primes}}}(\mathcal{F}_{1,2}) \in \mathbf{P}$.
2. There is a countable union of algebraic hypersurfaces $E \subsetneq \mathbb{Z}[x_1] \times \mathbb{P}$, with natural density 0, such that $\text{FEAS}_{\mathbb{Q}_{\text{primes}}}((\mathbb{Z}[x_1] \times \mathbb{P}) \setminus E) \in \mathbf{NP}$. Furthermore, we can decide in **P** whether an $f \in \mathcal{F}_{1,3}$ also lies in E .
3. If $\text{FEAS}_{\mathbb{Q}_{\text{primes}}}(\mathbb{Z}[x_1]) \in \mathbf{ZPP}$ then $\mathbf{NP} \subseteq \mathbf{ZPP}$.

Remark 1.9 Note that \mathbb{Q}_p is uncountable and thus, unlike $\text{FEAS}_{\mathbb{F}_{\text{primes}}}$, $\text{FEAS}_{\mathbb{Q}_{\text{primes}}}$ does **not** admit an obvious succinct certificate. Also, while it has been known since the late 1990's that $\text{FEAS}_{\mathbb{Q}_{\text{primes}}} \in \mathbf{EXPTIME}$ relative to our notion of input size [MW96, MW97], we are unaware of any earlier algorithms yielding $\text{FEAS}_{\mathbb{Q}_{\text{primes}}}(\mathbb{Z}[x_1, \dots, x_n]) \in \mathbf{NP}$ for some fixed n . In fact, even $\text{FEAS}_{\mathbb{Q}_{\text{primes}}}(\mathcal{F}_{1,3}) \in \mathbf{NP}$ remains unknown. \diamond

Practically speaking, zero density means that under most reasonable input restrictions, the algorithmic speed-up in Assertion 2 is valid over a significantly large fraction of inputs.

Example 1.10 Let T denote the family of pairs $(f, p) \in \mathbb{Z}[x_1] \times \mathbb{P}$ with $f(x_1) = a + bx_1^{11} + cx_1^{17} + x_1^{31}$ and let $T^* := T \setminus E$. Then there is a sparse 61×61 structured matrix \mathcal{S} (cf. Lemma 2.6 in Section 2.3 below), whose entries lie in $\{0, 1, 31, a, b, 11b, c, 17c\}$, such that $(f, p) \in T^* \iff p \nmid \det \mathcal{S}$. So by Theorem 1.8, $\text{FEAS}_{\mathbb{Q}_{\text{primes}}}(T^*) \in \mathbf{NP}$, and Corollary 4.2 in Section 4 below tells us that for large coefficients, T^* occupies almost all of T . In particular, letting $T(H)$ (resp. $T^*(H)$) denote those

²If $F(x_1, \dots, x_n) = 0$ is any polynomial equation and Z_K is its zero set in K^n , then the Hasse Principle is the assumption that $[Z_{\mathbb{C}} \text{ smooth}, Z_{\mathbb{R}} \neq \emptyset, \text{ and } Z_{\mathbb{Q}_p} \neq \emptyset \text{ for all primes } p]$ implies $Z_{\mathbb{Q}} \neq \emptyset$ as well. The Hasse Principle is a theorem when $Z_{\mathbb{C}}$ is a quadric hypersurface or a curve of genus zero, but fails in subtle ways already for curves of genus one (see, e.g., [Poo01a]).

pairs (f, p) in T (resp. T^*) with $|a|, |b|, |c|, p \leq H$, we have $\frac{\#T^*(H)}{\#T(H)} \geq \left(1 - \frac{61}{H}\right) \left(1 - \frac{31 \log_2(124H)}{H}\right)$. For instance, one can check via `Maple` that $(-973 + 21x_1^{11} - 2x_1^{17} + x_1^{31}, p) \in T^*$ for all but 352 primes p . \diamond

While it is not hard to show that the full problem $\text{FEAS}_{\mathbb{Q}_{\text{primes}}}$ is **NP**-hard from scratch, the least n making $\text{FEAS}_{\mathbb{Q}_{\text{primes}}}(\mathbb{Z}[x_1, \dots, x_n])$ **NP**-hard, and the least m making $\text{FEAS}_{\mathbb{Q}_{\text{primes}}}(\mathcal{F}_{1,m})$ **NP**-hard, appear not to have been known. Recalling the standard inclusions $\mathbf{P} \subseteq \mathbf{ZPP} \subseteq \mathbf{NP}$ and $\mathbf{ZPP} \subseteq \mathbf{BPP}$, we also see that Assertion 3 of Theorem 1.8 implies that $\text{FEAS}_{\mathbb{Q}_{\text{primes}}}(\mathbb{Z}[x_1])$ is at least as close to **NP**-hardness as $\text{FEAS}_{\mathbb{F}_{\text{primes}}}(\mathbb{Z}[x_1])$. In fact, the truth of certain well-known number-theoretic conjectures implies an even stronger version of Assertion 3 (see Remark 4.3 in Section 4 below).

Theorem 1.8 also provides a new complexity limit for polynomial factorization over $\mathbb{Q}_p[x_1]$: finding even just the **linear** (p -adic) factors is likely **not** doable in randomized time polynomial in the **sparse** input size. This complements Cantor and Gordon's randomized algorithm for factoring over $\mathbb{Q}_p[x_1]$ in expected time polynomial in the **dense** input size [CG00] (see also [Chi91]). Theorem 1.8 also provides an interesting contrast to earlier work of H. W. Lenstra, Jr. [Len99a], who showed that one can actually find all **low** degree factors of a sparse polynomial (over $\mathbb{Q}[x_1]$) in polynomial time.

We can also derive stronger p -adic analogues of our hardness results for non-trivial gcd detection and repeated factor (a.k.a. non-square-freeness) detection. Recall that $\mathbf{ZPP} \subseteq \mathbf{coRP} \subseteq \mathbf{BPP}$ and $\mathbf{coRP} \subseteq \mathbf{coNP}$.

Corollary 1.11 *Using $\text{size}_p(f)$ as our notion of input size, suppose we can decide within **ZPP**, for any input prime p and $f, g \in \mathbb{Z}[x_1]$, whether $\gcd(f, g) \in \mathbb{Q}_p[x_1]$ has positive degree. Then $\mathbf{NP} \subseteq \mathbf{ZPP}$. Furthermore, for any **fixed** prime p , if we can decide within **coRP**, for any input $f \in \mathbb{Z}[x_1]$, whether the factorization of f over $\mathbb{Q}_p[x_1]$ is square-free, then $\mathbf{NP} \subseteq \mathbf{coRP}$.*

1.3 Random Primes in Arithmetic Progressions

Both our main theorems make use of a technique of possible independent interest: the construction of random primes p such that p is moderately sized and yet $p - 1$ has many prime factors. In particular, efficiently constructing random primes in **arbitrary** arithmetic progressions, as of late 2007, remains a famous open problem. We use the notation $[j] := \{1, \dots, j\}$ for any $j \in \mathbb{N}$.

Theorem 1.12 *For any $\delta > 0$, a success probability $1 - \varepsilon \in (1/2, 1)$, and $n, s \in \mathbb{N}$, we can find — within $O\left(\left(\frac{n}{\varepsilon}\right)^{\frac{3}{2}+\delta} + (n \log(n) + \log\left(\frac{s}{\varepsilon}\right))^{7+\delta}\right)$ randomized bit operations — a sequence $P = (p_i)_{i=1}^n$ of consecutive primes and a positive integer K such that the following hold:*

1. $\log\left(\prod_{i=1}^n p_i\right), \log K = O(n \log(n) + \log(s/\varepsilon))$
2. for any fixed $S_P \subset \mathbb{N}$ of finite cardinality s , a uniformly random $c \in [K]$ yields $p := 1 + c \prod_{i=1}^n p_i$ prime and $p \notin S_P$ with probability $1 - \varepsilon$.

Theorem 1.12 and its proof are inspired in large part by an algorithm of von zur Gathen, Karpinski, and Shparlinski [vzGKS96, Algorithm following Fact 4.9]. In particular, they used an intricate random sampling technique [vzGKS96, Thm. 4.10] to show, in our notation, that the enumerative analogue of $\text{FEAS}_{\mathbb{F}_{\text{prime powers}}}(\mathbb{Z}[x_1, x_2])$ is $\#\mathbf{P}$ -hard [vzGKS96, Thm. 4.11]. Note in particular that neither of Theorem 4.10 of [vzGKS96] or Theorem 1.12 above implies the other. Whether the enumerative analogue of $\text{FEAS}_{\mathbb{F}_{\text{primes}}}(\mathbb{Z}[x_1])$ is $\#\mathbf{P}$ -hard remains an intriguing open question.

Our main results are proved in Sections 3 and 4, after the development of some necessary theory below.

2 Background and Ancillary Results

Our lower bounds will follow from a common chain of reductions, so we will begin by reviewing the fundamental problem from which we reduce. We then show how to efficiently construct random primes p such that $p-1$ has many prime factors in Section 2.2, and conclude with some quantitative results for transferring complexity results over \mathbb{C} to \mathbb{F}_p and \mathbb{Q}_p in Section 2.3.

2.1 Roots of Unity and NP-completeness

Recall that any Boolean expression of one of the following forms:

$$(\heartsuit) \quad y_i \vee y_j \vee y_k, \quad \neg y_i \vee y_j \vee y_k, \quad \neg y_i \vee \neg y_j \vee y_k, \quad \neg y_i \vee \neg y_j \vee \neg y_k, \quad \text{with } i, j, k \in [3n],$$

is a **3CNFSAT clause**. Let us first refine slightly Plaisted’s elegant reduction from 3CNFSAT to feasibility testing for univariate polynomial systems over the complex numbers [Pla84, Sec. 3, pp. 127–129].

Definition 2.1 *Letting $P := (p_1, \dots, p_n)$ denote any strictly increasing sequence of primes, let us inductively define a semigroup homomorphism \mathcal{P}_P — the **Plaisted morphism with respect to P** — from certain Boolean expressions in the variables y_1, \dots, y_n to $\mathbb{Z}[x_1]$, as follows:³ (0) $D_P := \prod_{i=1}^n p_i$, (1) $\mathcal{P}_P(0) := 1$, (2) $\mathcal{P}_P(y_i) := x_1^{D_P/p_i} - 1$, (3) $\mathcal{P}_P(\neg B) := (x_1^{D_P} - 1)/\mathcal{P}_P(B)$, for any Boolean expression B for which $\mathcal{P}_P(B)$ has already been defined, (4) $\mathcal{P}_P(B_1 \vee B_2) := \text{lcm}(\mathcal{P}_P(B_1), \mathcal{P}_P(B_2))$, for any Boolean expressions B_1 and B_2 for which $\mathcal{P}_P(B_1)$ and $\mathcal{P}_P(B_2)$ have already been defined. \diamond*

Lemma 2.2 [Pla84, Sec. 3, pp. 127–129] *Suppose $P = (p_i)_{i=1}^n$ is an increasing sequence of primes with $\log(p_k) = O(k^\gamma)$ for some constant γ . Then, for all $n \in \mathbb{N}$ and any clause C of the form (\heartsuit) , we have $\text{size}(\mathcal{P}_P(C))$ polynomial in n . In particular, \mathcal{P}_P can be evaluated at any such C in time polynomial in n . Furthermore, if K is any field possessing D_P distinct D_P^{th} roots of unity, then a 3CNFSAT instance $B(y) := C_1(y) \wedge \dots \wedge C_k(y)$ has a satisfying assignment iff the univariate polynomial system $F_B := (\mathcal{P}_P(C_1), \dots, \mathcal{P}_P(C_k))$ has a root $\zeta \in K$ satisfying $\zeta^{D_P} - 1 = 0$. \blacksquare*

Plaisted actually proved the special case $K = \mathbb{C}$ of the above lemma, in slightly different language, in [Pla84]. However, his proof extends with no difficulty whatsoever to the more general family of fields detailed above.

2.2 Randomization to Avoid Riemann Hypotheses

Specializing $(A, \varepsilon, \delta, y, a) = (49/20, 1/2, 2/245, x, 1)$ in [AGP94, Thm. 2.1, pg. 712] we can obtain the result below which allows us to prove Theorem 1.12 and further tailor Plaisted’s clever reduction to our purposes. We let $\varphi(j)$ denote the number of integers in $[j]$ relatively prime to j , $\pi(x)$ the number of primes $\leq x$, and let $\pi(x; M, 1)$ denote the number of primes $\leq x$ that are congruent to 1 mod M .

AGP Theorem (very special case of [AGP94, Thm. 2.1, pg. 712]) *There exist $x_0 > 0$ and an $\ell \in \mathbb{N}$ such that for each $x \geq x_0$, there is a subset $\mathcal{E}(x) \subset \mathbb{N}$ of finite cardinality ℓ with the following property: If $M \in \mathbb{N}$ satisfies $M \leq x^{2/5}$ and $a \not\equiv 1 \pmod{M}$ for all $a \in \mathcal{E}(x)$ then $\pi(x; M, 1) \geq \frac{\pi(x)}{2\varphi(M)}$. \blacksquare*

The AGP Theorem enables us to construct random primes from certain arithmetic progressions while also avoiding a “moving target” (depending on P) with high probability. In particular, consider the following algorithm.

³Throughout this paper, for Boolean expressions, we will always identify 0 with ‘‘False’’ and 1 with ‘‘True’’.

Algorithm 2.3

Input: A success probability $1 - \varepsilon \in (1/2, 1)$, positive integers n and s , and the constants x_0 and ℓ from the AGP Theorem.

Output: A sequence $P = (p_j)_{j=1}^n$ of consecutive primes and a positive integer c such that for any $S_P \subset \mathbb{N}$ of finite cardinality s , $p := 1 + c \prod_{i=1}^n p_i$ satisfies the following properties:

1. $\log p = O(n \log(n) + \log(s/\varepsilon))$
2. with probability $1 - \varepsilon$, p is prime and $p \notin S_P$.

In particular, we also know (with no additional work) whether p is prime.

Description:

0. Let $L := \lceil 3/\varepsilon \rceil \ell$, $s' := \max\{1, s\}$, and compute the first nL primes p_1, \dots, p_{nL} in increasing order.

1. Define (but do not compute) $M_j := \prod_{k=(j-1)n+1}^{jn} p_k$ for any $j \in \mathbb{N}$. Then compute M_L, M_i for a

uniformly random $i \in [L]$, and $x := \max \left\{ x_0, 17, 1 + M_L \left[\max \left\{ M_L^{3/2}, 1 + 3s'/\varepsilon \right\} \right] \right\}$.

2. Compute $K := \lfloor (x-1)/M_i \rfloor$ and $J := \lceil 2 \log(3/\varepsilon) \log x \rceil$.

3. Pick uniformly random $c \in [K]$ until one either has $p := 1 + cM_i$ prime, or one has J such numbers that are each composite.

4. If a prime p was found then output the corresponding c and $P := (p_j)_{j=(i-1)n+1}^{in}$, and say

“... p is a prime that probably avoids your set.”,

or

“... p is a prime that works!”

(according as s is positive or zero) and stop. Otherwise, stop and output

“I have failed to find a suitable prime. Please forgive me.” \diamond

Remark 2.4 In our algorithm above, it suffices to find integer approximations to the underlying logarithms and square-roots. In particular, we restrict to algorithms that can compute the $\log_2 \mathcal{L}$ most significant bits of $\log \mathcal{L}$, and the $\frac{1}{2} \log_2 \mathcal{L}$ most significant bits of $\sqrt{\mathcal{L}}$, using

$$O((\log \mathcal{L})(\log \log \mathcal{L}) \log \log \log \mathcal{L})$$

bit operations. Arithmetic-Geometric Mean Iteration and (suitably tailored) Newton Iteration are algorithms that respectively satisfy our requirements (see [Ber03] and [Ber04] for a detailed description). \diamond

Proof of Theorem 1.12: It clearly suffices to prove that Algorithm 2.3 is correct, has a success probability that is at least $1 - \varepsilon$, and works within $O\left(\left(\frac{n}{\varepsilon}\right)^{\frac{3}{2}+\delta} + (n \log(n) + \log(s/\varepsilon))^{7+\delta}\right)$ randomized bit operations, for any $\delta > 0$. This we do in the Appendix. \blacksquare

2.3 Transferring from \mathbb{C} to Arithmetic Fields

As one might suspect from the formal connection between \mathbb{F}_p and \mathbb{Q}_p , the proofs of Theorems 1.4 and 1.8 bear some similarities: Both complexity lower bound proofs reduce feasibility testing for systems of univariate polynomials to feasibility testing for a single univariate polynomial. We now state some final tricks to complete our line of reasoning.

Proposition 2.5 Given any $f_1, \dots, f_k \in \mathbb{Z}[x_1]$ of maximum degree d and maximum coefficient absolute value H , let

$$\tilde{f}(x_1) = x^d(f_1(x_1)f_1(1/x_1) + \dots + f_k(x_1)f_k(1/x_1)).$$

Then $f_1 = \dots = f_k = 0$ has a root on the complex unit circle iff \tilde{f} has a root on the complex unit circle. In particular, if $f_i \in \mathcal{F}_{1, \mu_i}$ and $\mu_i \leq m$ for all i , then $\tilde{f} \in \mathcal{F}_{1, \mu}$ for some μ with $\mu \leq ((m-1)m+1)k$ and \tilde{f} has maximum coefficient bit-size $O(\log(kmH))$. ■

Proposition 2.5 follows easily upon observing that $f_i(x_1)f_i(1/x_1) = |f_i(x_1)|^2$ for all $i \in [k]$ and any $x_1 \in \mathbb{C}$ with $|x_1| = 1$.

Lemma 2.6 (See, e.g., [GKZ94, Ch. 12, Sec. 1, pp. 397–402].) Suppose $f(x_1) = a_0 + \dots + a_d x_1^d$ and $g(x_1) = b_0 + \dots + b_{d'} x_1^{d'}$ are polynomials with indeterminate coefficients. Define their **Sylvester matrix** to be the $(d+d') \times (d+d')$ matrix

$$\mathcal{S}_{(d,d')}(f,g) := \begin{bmatrix} a_0 & \dots & a_d & 0 & \dots & 0 \\ & \ddots & & & \ddots & \\ 0 & \dots & 0 & a_0 & \dots & a_d \\ b_0 & \dots & b_{d'} & 0 & \dots & 0 \\ & \ddots & & & \ddots & \\ 0 & \dots & 0 & b_0 & \dots & b_{d'} \end{bmatrix} \left. \begin{array}{l} \vphantom{\begin{bmatrix} a_0 \\ \vdots \\ 0 \\ b_0 \\ \vdots \\ 0 \end{bmatrix}} \right\} d' \text{ rows} \\ \left. \vphantom{\begin{bmatrix} 0 \\ \vdots \\ 0 \\ b_0 \\ \vdots \\ 0 \end{bmatrix}} \right\} d \text{ rows}$$

and their **Sylvester resultant** to be $\mathcal{R}_{(d,d')}(f,g) := \det \mathcal{S}_{(d,d')}(f,g)$. Then, assuming $f, g \in K[x_1]$ for some field K and $a_d b_{d'} \neq 0$, we have that $f = g = 0$ has a root in the algebraic closure of K iff $\mathcal{R}_{(d,d')}(f,g) = 0$. Finally, if we assume further that f and g have complex coefficients of absolute value $\leq H$, and f (resp. g) has exactly m (resp. m') monomial terms, then $|\mathcal{R}_{(d,d')}(f,g)| \leq m^{d'/2} m'^{d/2} H^{d+d'}$. ■

The last part of Lemma 2.6 follows easily from Hadamard's Inequality (see, e.g., [Mig82, Thm. 1, pg. 259]). The following lemma is proved in the Appendix.

Lemma 2.7 Suppose $D \in \mathbb{N}$ and $f \in \mathbb{Z}[x_1] \setminus \{0\}$ has degree d , exactly m monomial terms, and maximum coefficient absolute value H . Also let p be any prime congruent to 1 mod D . Then

1. f vanishes at a complex D^{th} root of unity \iff f vanishes at a D^{th} root of unity in \mathbb{Q}_p .
2. f vanishes at a complex D^{th} root of unity \implies the mod p reduction of f vanishes at a D^{th} root of unity in \mathbb{F}_p .
3. With the exception of $O(d + D \log(mH))$ primes p , f vanishes at **no** complex D^{th} root of unity \implies f vanishes at **no** D^{th} root of unity in \mathbb{F}_p .

We call the primes for which the implication in Assertion 3 fails **exceptional (for (f, D))**. ■

Remark 2.8 Note that $x_1^2 + x_1 + 1$ vanishes at a 3^{rd} root of unity in \mathbb{C} , but has **no** roots at all in \mathbb{F}_5 or \mathbb{Q}_5 . Hence our congruence assumption on p in Lemma 2.7. \diamond

3 The Univariate Threshold Over \mathbb{F}_p : Proof of Theorem 1.4

Suppose $B(y) := C_1(y) \wedge \dots \wedge C_k(y)$ is any 3CNFSAT instance. The polynomial system $(\mathcal{P}_P(C_1), \dots, \mathcal{P}_P(C_k))$, for P the first n primes (employing Lemma 2.2), then clearly yields the implication $\text{FEAS}_{\mathbb{C}}(\{\mathbb{Z}[x_1]^k \mid k \in \mathbb{N}\}) \in \mathbf{P} \implies \mathbf{P} = \mathbf{NP}$. Composing this reduction with Proposition 2.5, we then immediately obtain the implication $\text{FEAS}_{\mathbb{C}}(\mathbb{Z}[x_1] \times \{x_1^D - 1 \mid D \in \mathbb{N}\}) \in \mathbf{P} \implies \mathbf{P} = \mathbf{NP}$.

At this point, we need only find a means of transferring from \mathbb{C} to \mathbb{F}_p . This we do by preceding our reductions above by a judicious (possibly new) choice of P . In particular, by applying Theorem 1.12 with $\varepsilon = 1/3$ and S_P equal to the set of primes exceptional for (\tilde{f}, D_P) (cf. Lemma 2.7), we immediately obtain the implication $\text{FEAS}_{\mathbb{F}_{\text{primes}}}(\mathbb{Z}[x_1] \times \{x_1^D - 1 \mid D \in \mathbb{N}\}) \in \mathbf{BPP} \implies \mathbf{NP} \subseteq \mathbf{BPP}$. So far, we thus know how to convert 3CNFSAT instances into triples of the form $(f, x^{D_P} - 1, p)$ with p a **random** prime in the arithmetic progression $\{1 + D_P, 1 + 2D_P, 1 + 3D_P, \dots\}$ and D_P a product of n consecutive primes.

To conclude, observe that when χ is a quadratic non-residue mod p , the only root in \mathbb{F}_p^2 of the quadratic form $x^2 - \chi y^2$ is $(0, 0)$. Since such a χ can be found in **ZPP** (via random sampling and polynomial-time Jacobi symbol calculation [BS96, Cor. 5.7.5 & Thm. 5.9.3, pg. 110 & 113]), we thus easily obtain a **ZPP**-reduction from $\text{FEAS}_{\mathbb{F}_{\text{primes}}}(\mathbb{Z}[x_1] \times \{x_1^D - 1 \mid D \in \mathbb{N}\})$ to $\text{FEAS}_{\mathbb{F}_{\text{primes}}}(\mathbb{Z}[x_1])$: simply map any instance $(f(x_1), x_1^D - 1, p)$ of the former problem to $(f(x_1)^2 - (x_1^D - 1)^2 \chi, p)$. So we are done. ■

Proposition 2.5, Lemma 2.7, and Theorem 1.12 are the key to our improvements over the earlier results [vzGKS96, Sec. 4, Top of Pg. 17] and [KiSha99, Lemma 3.3] of von zur Gathen, Karpinski, and Shparlinski, and Kipnis and Shamir. In particular, our results over \mathbb{F}_p and \mathbb{Q}_p would not have been possible had we instead used the classic trick of random linear combinations (e.g., [GH93, Sec. 3.4.1] or [vzGKS96, Lemma 4.7]) to reduce the number of equations in a polynomial system.

4 The Univariate Threshold Over \mathbb{Q}_p : Proving Theorem 1.8

Let us first clarify how often our p -adic speed-ups hold for inputs with bounded coefficients.

Definition 4.1 Write any $f \in \mathbb{C}[x_1]$ as $f(x_1) = \sum_{i=1}^m c_i x_1^{a_i}$ with $0 \leq a_1 < \dots < a_m$. Letting $\mathcal{A} = \{a_1, \dots, a_m\}$, and following the notation of Lemma 2.7, we then define

$$\mathcal{D}_{\mathcal{A}}(f) := \mathcal{R}_{(a_m - a_1, a_m - a_2)} \left(\frac{f(x_1)}{x_1^{a_1}}, \frac{\partial \left(\frac{f(x_1)}{x_1^{a_1}} \right)}{\partial x_1} \Big/ x^{a_2 - 1} \right) \Big/ c_m$$

to be the **A-discriminant** of f (see also [GKZ94, Ch. 12, pp. 403–408]). Finally, if $c_i \neq 0$ for all i , then we call $\text{Supp}(f) := \{a_1, \dots, a_m\}$ the **support** of f . ◊

Corollary 4.2 For any subset $\mathcal{A} \subset \mathbb{N} \cup \{0\}$ of cardinality m , let $\mathcal{I}_{\mathcal{A}}$ denote the family of pairs $(f, p) \in \mathbb{Z}[x_1] \times \mathbb{P}$ with $f(x) = \sum_{i=1}^m c_i x_1^{a_i}$ and let $\mathcal{I}_{\mathcal{A}}^*$ denote the subset of $\mathcal{I}_{\mathcal{A}}$ consisting of those pairs (f, p) with $p \nmid \mathcal{D}_{\mathcal{A}}(f)$. Also let $\mathcal{I}_{\mathcal{A}}(H)$ (resp. $\mathcal{I}_{\mathcal{A}}^*(H)$) denote those pairs (f, p) in $\mathcal{I}_{\mathcal{A}}$ (resp. $\mathcal{I}_{\mathcal{A}}^*$) where $|c_i| \leq H$ for all $i \in [m]$ and $p \leq H$. Then $\frac{\#\mathcal{I}_{\mathcal{A}}^*(H)}{\#\mathcal{I}_{\mathcal{A}}(H)} \geq \left(1 - \frac{(2d-1)m}{H}\right) \left(1 - \frac{d \log_2(dmH)}{H}\right)$. ■

Our corollary above follows easily from our proof of Assertion 2 of Theorem 1.8 via an application of Lemma 2.6.

Proof of Theorem 1.8

(FEAS $_{\mathbb{Q}_{\text{primes}}}$ ($\mathcal{F}_{1,2}$) \in \mathbf{P}): First note that we can easily reduce to the special case $f(x) := x^d - \alpha$ with $\alpha \in \mathbb{Q}$, since we can divide any input by a suitable monomial term, and arithmetic over \mathbb{Q} is doable in polynomial time. The case $\alpha = 0$ always results in the root 0, so let us also assume $\alpha \neq 0$. Clearly then, any p -adic root ζ of $x^d - \alpha$ satisfies $d \text{ord}_p \zeta = \text{ord}_p \alpha$. Since we can compute $\text{ord}_p \alpha$ and reductions of integers mod d in polynomial-time [BS96, Ch. 5], we can then assume that $d \mid \text{ord}_p \alpha$ (for otherwise, f would have no roots over \mathbb{Q}_p). Replacing $f(x_1)$ by $p^{-\text{ord}_p \alpha} f(p^{\text{ord}_p \alpha / d} x_1)$, we can assume further that $\text{ord}_p \alpha = \text{ord}_p \zeta = 0$. In particular, if $\text{ord}_p \alpha$ was initially a nonzero multiple of d , then $\log \alpha \geq d \log_2 p$. So $\text{size}(f) \geq d$ and our rescaling at worst doubles $\text{size}(f)$.

Letting $k := \text{ord}_p d$, note that $f'(x) = dx^{d-1}$ and thus $\text{ord}_p f'(\zeta) = \text{ord}_p(d) + (d-1)\text{ord}_p \zeta = k$. So by Hensel's Lemma, it suffices to decide whether the mod p^ℓ reduction of f has a root in $(\mathbb{Z}/p^\ell \mathbb{Z})^*$, for $\ell = 1 + 2k$. Note in particular that $\text{size}(p^\ell) = O(\log(p)\text{ord}_p d) = O(\log(p)\log(d)/\log p) = O(\log d)$ which is linear in our notion of input size. By Lemma 5.2 of the Appendix, we can then clearly decide whether $x^d - \alpha$ has a root in $(\mathbb{Z}/p^\ell \mathbb{Z})^*$ within \mathbf{P} (via a single fast exponentiation), provided $p^\ell \notin \{8, 16, 32, \dots\}$.

To dispose of the remaining cases $p^\ell \in \{8, 16, 32, \dots\}$, first note that we can replace d by its reduction mod $2^{\ell-2}$ since every element of $(\mathbb{Z}/2^\ell \mathbb{Z})^*$ has order dividing $2^{\ell-2}$, and this reduction can certainly be computed in polynomial-time. Let us then write $d = 2^h d'$ where $2 \nmid d'$ and $h \in \{0, \dots, \ell-3\}$, and compute $d'' := 1/d' \pmod{2^{\ell-2}}$. Clearly then, $x^d - \alpha$ has a root in $(\mathbb{Z}/2^\ell \mathbb{Z})^*$ iff $x^{2^h} - \alpha'$ has a root in $(\mathbb{Z}/2^\ell \mathbb{Z})^*$, where $\alpha' := \alpha^{d''}$ (since exponentiation by any odd power is an automorphism of $(\mathbb{Z}/2^\ell \mathbb{Z})^*$). Note also that α' , d' , and d'' can clearly be computed in polynomial time.

Since $x^{2^h} - \alpha'$ always has a root in $(\mathbb{Z}/2^\ell \mathbb{Z})^*$ when $h=0$, we can then restrict our root search to the cyclic subgroup $\{1, 5^2, 5^4, 5^6, \dots, 5^{2^{\ell-2}-2}\}$ when $h \geq 1$ and α' is a square (since there can be no roots when $h \geq 1$ and α' is not a square). Furthermore, we see that $x^{2^h} - \alpha'$ can have no roots in $(\mathbb{Z}/2^\ell \mathbb{Z})^*$ if $\text{ord}_2 \alpha'$ is odd. So, by rescaling x , we can assume further that $\text{ord}_2 \alpha' = 0$, and thus that α' is odd. Now an odd α' is a square in $(\mathbb{Z}/2^\ell \mathbb{Z})^*$ iff $\alpha' \equiv 1 \pmod{8}$ [BS96, Ex. 38, pg. 192], and this can clearly be checked in \mathbf{P} . So we can at last decide the existence of a root in \mathbb{Q}_2 for $x^d - \alpha$ in \mathbf{P} : Simply combine fast exponentiation with Assertion 3 of Lemma 5.2 again, applied to $x^{2^h} - \alpha'$ over the cyclic group $\{1, 5^2, 5^4, 5^6, \dots, 5^{2^{\ell-2}-2}\}$.

(FEAS $_{\mathbb{Q}\text{-primes}}(\mathbb{Z}[x_1]) \in \mathbf{NP}$ for most inputs): First note that $x \in \mathbb{Q}_p \setminus \mathbb{Z}_p \iff \frac{1}{x} \in p\mathbb{Z}_p$. Letting $f^*(x) := x^{\deg f} f(1/x)$ denote the reciprocal polynomial of f , note that the set of p -adic rational roots of f is simply the union of the p -adic integer roots of f and the reciprocals of the p -adic integer roots of f^* . So it suffices to derive succinct certificates for the roots of f in \mathbb{Z}_p , and do so for the stated fraction of inputs (f, p) . Let $\text{Newt}_p(f)$ denote the **p -adic Newton polygon** of f (cf. the Appendix).

Observe that the p -adic valuations of all the roots of f in \mathbb{C}_p can be computed in polynomial-time. This is easily seen via two facts: (1) convex hulls of subsets of \mathbb{Z}^2 can be computed in polynomial-time (see, e.g., [Ede87]), and (2) the valuation of any root of $f(x) = \sum_{i=1}^m c_i x^{a_i}$ is a ratio of the form $\frac{\text{ord}_p(c_i) - \text{ord}_p(c_j)}{a_j - a_i}$, where $(a_i, \text{ord}_p(c_i))$ and $(a_j, \text{ord}_p(c_j))$ are respectively the left and right vertices of a lower edge of $\text{Newt}_p(f)$ (cf. Lemma 5.1 of the Appendix). Since $\text{ord}_p(c_i) \leq \log_p(c_i) \leq \text{size}(c_i)$, note in particular that every root $\zeta \in \mathbb{C}_p$ of f satisfies $|\text{ord}_p \zeta| \leq 2 \max_i \text{size}(c_i) \leq 2\text{size}(f) < 2\text{size}_p(f)$.

Since $\text{ord}_p(\mathbb{Z}_p) = \mathbb{N} \cup \{0\}$, we can clearly assume that $\text{Newt}_p(f)$ has an edge with nonnegative integral slope, for otherwise f would have no roots in \mathbb{Z}_p . Letting a denote the smallest nonzero exponent in f , $g(x) := f'(x)/x^{a-1}$, and $\zeta \in \mathbb{Z}_p$ any p -adic integer root of f , note then that $\text{ord}_p f'(\zeta) = (a-1)\text{ord}_p(\zeta) + \text{ord}_p g(\zeta)$. Note also that $\mathcal{D}_{\mathcal{A}}(f) = \text{Res}_{a_m, a_m - a_1}(f, g)$ so if $p \nmid \mathcal{D}_{\mathcal{A}}(f)$ then f and g have no common roots in the algebraic closure of \mathbb{F}_p by Lemma 2.6. In particular, $p \nmid \mathcal{D}_{\mathcal{A}}(f) \implies g(\zeta) \not\equiv 0 \pmod{p}$; and thus $p \nmid \mathcal{D}_{\mathcal{A}}(f, g) \implies \text{ord}_p f'(\zeta) = (a-1)\text{ord}_p(\zeta)$. Furthermore, by the convexity of the lower hull of $\text{Newt}_p(f)$, it is clear that $\text{ord}_p(\zeta) \leq \frac{\text{ord}_p c_i - \text{ord}_p c_0}{i} \leq \frac{2 \max_i \log_p |c_i|}{a_1}$. So $p \nmid \mathcal{D}_{\mathcal{A}}(f) \implies \text{ord}_p f'(\zeta) < 2\text{size}(f)$.

Our fraction of inputs admitting a succinct certificate will then correspond precisely to those (f, p) such that $p \nmid \mathcal{D}_{\mathcal{A}}(f)$. In particular, let us define E to be the union of all pairs (f, p) such that $p \nmid \mathcal{D}_{\mathcal{A}}(f)$, as \mathcal{A} ranges over all finite subsets of $\mathbb{N} \cup \{0\}$. It is then easily checked that E is a countable union of hypersurfaces.

Fix $\ell = 4\text{size}(f)$. Clearly then, by Hensel's Lemma, for any $(f, p) \in (\mathbb{Z}[x_1] \times \mathbb{P}) \setminus E$, f has a root $\zeta \in \mathbb{Z}_p \iff f$ has a root $\zeta_0 \in \mathbb{Z}/p^\ell\mathbb{Z}$. Since $\log(p^\ell) = O(\text{size}(f) \log p) = O(\text{size}_p(f)^2)$, and since arithmetic in $\mathbb{Z}/p^\ell\mathbb{Z}$ can be done in time polynomial in $\log(p^\ell)$ [BS96, Ch. 5], we have thus at last found our desired certificate: a root $\zeta_0 \in (\mathbb{Z}/p^\ell\mathbb{Z})^*$ of f with $\ell = 4\text{size}(f)$.

(Efficiently Checking whether an $f \in \mathcal{F}_{1,3}$ also lies in E): Similar to our last argument, we can clearly reduce to the special case $f(x_1) = a + bx_1^d + x_1^D$ with $0 < d < D$ and $ab \neq 0$. Letting $\mathcal{A} := \{0, d, D\}$ we then obtain $\mathcal{D}_{\mathcal{A}}(f) = (D-d)^{D-d} d^d b^D - (-D)^D a^{D-d}$ (see, e.g., [GKZ94, Prop. 1.8, pg. 274]). In particular, while one can certainly evaluate $\mathcal{D}_{\mathcal{A}}(f)$ with a small number of arithmetic operations, the bit-size of $\mathcal{D}_{\mathcal{A}}(f)$ can be quite large. However, we can nevertheless decide $\mathcal{D}_{\mathcal{A}}(f) \stackrel{?}{=} 0 \pmod p$ in \mathbf{P} by simply using recursive squaring and efficient finite-field arithmetic.

(FEAS $_{\mathbb{Q}_{\text{primes}}}(\mathbb{Z}[x_1])$ is NP-hard under ZPP-reductions): We will prove a (ZPP) randomized polynomial-time reduction from 3CNFSAT to FEAS $_{\mathbb{Q}_{\text{primes}}}(\mathbb{Z}[x_1])$, making use of the intermediate input families $\{(\mathbb{Z}[x_1])^k \mid k \in \mathbb{N}\}$ and $\mathbb{Z}[x_1] \times \{x_1^D - 1 \mid D \in \mathbb{N}\}$ along the way.

Toward this end, suppose $B(y) := C_1(y) \wedge \dots \wedge C_k(y)$ is any 3CNFSAT instance. The polynomial system $(\mathcal{P}_P(C_1), \dots, \mathcal{P}_P(C_k))$, for P the first n primes (employing Lemma 2.2), then clearly yields the implication FEAS $_{\mathbb{C}}(\{(\mathbb{Z}[x_1])^k \mid k \in \mathbb{N}\}) \in \mathbf{P} \implies \mathbf{P} = \mathbf{NP}$. Composing this reduction with Proposition 2.5, we then immediately obtain the implication FEAS $_{\mathbb{C}}(\mathbb{Z}[x_1] \times \{x_1^D - 1 \mid D \in \mathbb{N}\}) \in \mathbf{P} \implies \mathbf{P} = \mathbf{NP}$.

At this point, we need only find a means of transferring from \mathbb{C} to \mathbb{Q}_p . This we do by preceding our reductions above by a judicious (possibly new) choice of P . In particular, by applying Theorem 1.12 with $\varepsilon = 1/3$ and $S_P = \emptyset$ (cf. Lemma 2.7) we immediately obtain the implication FEAS $_{\mathbb{Q}_{\text{primes}}}(\mathbb{Z}[x_1] \times \{x_1^D - 1 \mid D \in \mathbb{N}\}) \in \mathbf{ZPP} \implies \mathbf{NP} \subseteq \mathbf{ZPP}$.

To conclude, observe that if $\chi \in \{1, \dots, p-1\}$ is a quadratic non-residue mod p then $\text{ord}_p \chi = 0$ and thus any root (x, y) of the quadratic form $x^2 - \chi y^2$ must satisfy $\text{ord}_p x = \text{ord}_p y$. By homogeneity we can then assume $\text{ord}_p x = \text{ord}_p y = 0$ (if $xy \neq 0$), and by reduction mod p we thus obtain that the first base- p digits of x and y must both be 0: a contradiction unless $x = y = 0$. Therefore, the only p -adic rational root of $x^2 - \chi y^2$ is $(0, 0)$. Since such a χ can be found in ZPP (via random sampling and polynomial-time Jacobi symbol calculation [BS96, Cor. 5.7.5 & Thm. 5.9.3, pg. 110 & 113]), we thus easily obtain a ZPP-reduction from FEAS $_{\mathbb{Q}_{\text{primes}}}(\mathbb{Z}[x_1] \times \{x_1^D - 1 \mid D \in \mathbb{N}\})$ to FEAS $_{\mathbb{Q}_{\text{primes}}}(\mathbb{Z}[x_1])$: simply map any instance $(f(x_1), x_1^D - 1, p)$ of the former problem to $(f(x_1)^2 - (x_1^D - 1)^2 \chi, p)$. So we are done. ■

Remark 4.3 *If the Generalized Riemann Hypothesis holds for all cyclotomic fields, then one can in fact find quadratic non-residues mod p in deterministic polynomial-time [BS96, thm. 7.8.2, pg. 178]. If we also have the truth of the Wagstaff Conjecture [BS96, Conj. 8.5.10, pg. 224] then we immediately obtain the stronger implication FEAS $_{\mathbb{Q}_{\text{primes}}}(\mathbb{Z}[x_1]) \in \mathbf{P} \implies \mathbf{P} = \mathbf{NP}$. ◊*

Acknowledgements

The authors would like to thank David Alan Plaisted for his kind encouragement, and Eric Bach, Sidney W. Graham, and Igor Shparlinski for many helpful comments on primes in arithmetic progression. We also thank Matt Papanikolas for valuable p -adic discussions.

References

[AKS02] Agrawal, Manindra; Kayal, Neeraj; and Saxena, Nitin, “PRIMES is in P,” Ann. of Math. (2) 160 (2004), no. 2, pp. 781–793.

- [AGP94] Alford, W. R.; Granville, Andrew; and Pomerance, Carl, “*There are Infinitely Many Carmichael Numbers*,” *Ann. of Math. (2)* **139** (1994), no. 3, pp. 703–722.
- [BS96] Bach, Eric and Shallit, Jeff, *Algorithmic Number Theory, Vol. I: Efficient Algorithms*, MIT Press, Cambridge, MA, 1996.
- [Ber03] Bernstein, Daniel J., “*Computing Logarithm Intervals with the Arithmetic-Geometric Mean Iterations*,” available from <http://cr.yp.to/papers.html> .
- [Ber04] Bernstein, Daniel J., “*Removing Redundancy in High-Precision Newton Iteration*,” available from <http://cr.yp.to/papers.html> .
- [BRS07] Bihan, Frederic; Rojas, J. Maurice; and Stella, Casey, “*First Steps in Algorithmic Fewnomial Theory*,” submitted for publication. Also available as Math ArXiv preprint [math.AG/0411107](https://arxiv.org/abs/math/0411107) .
- [CG00] Cantor, David G. and Gordon, Daniel M., “*Factoring polynomials over p -adic fields*,” *Algorithmic number theory (Leiden, 2000)*, pp. 185–208, *Lecture Notes in Comput. Sci.*, 1838, Springer, Berlin, 2000.
- [CZ81] Cantor, David G. and Zassenhaus, Hans, “*A new algorithm for factoring polynomials over finite fields*,” *Math. Comp.* **36** (1981), no. 154, pp. 587–592.
- [CDV06] Castrick, Wouter; Denef, Jan; and Vercauteren, Frederik, “*Computing Zeta Functions of Nondegenerate Curves*,” *International Mathematics Research Papers*, vol. 2006, article ID 72017, 2006.
- [Chi91] Chistov, Alexander L., “*Efficient Factoring [of] Polynomials over Local Fields and its Applications*,” in I. Satake, editor, *Proc. 1990 International Congress of Mathematicians*, pp. 1509–1519, Springer-Verlag, 1991.
- [Coh94] Cohen, Henri, *A course in computational algebraic number theory*, *Graduate Texts in Mathematics*, 138, Springer-Verlag, Berlin, 1993.
- [Coh69] Cohen, Paul J., “*Decision procedures for real and p -adic fields*,” *Comm. Pure Appl. Math.* **22** (1969), pp. 131–151.
- [C-T98] Colliot-Thelene, Jean-Louis, “*The Hasse principle in a pencil of algebraic varieties*,” *Number theory (Tiruchirapalli, 1996)*, pp. 19–39, *Contemp. Math.*, 210, Amer. Math. Soc., Providence, RI, 1998.
- [Cox04] Cox, David Archibald, *personal communication via e-mail*, August 2004.
- [DvdD88] Denef, Jan and van den Dries, Lou, “ *p -adic and Real Subanalytic Sets*,” *Annals of Mathematics (2)* **128** (1988), no. 1, pp. 79–138.
- [DLPvG00] *Hilbert’s Tenth Problem: Relations with Arithmetic and Algebraic Geometry*, Papers from a workshop held at Ghent University, Ghent, November 2–5, 1999. Edited by Jan Denef, Leonard Lipshitz, Thanases Pheidas and Jan Van Geel. *Contemporary Mathematics*, 270, American Mathematical Society, Providence, RI, 2000.
- [Ede87] Edelsbrunner, Herbert, *Algorithms in combinatorial geometry*, *EATCS Monographs on Theoretical Computer Science*, 10, Springer-Verlag, Berlin, 1987.

- [Gao05] Gao, Shuhong, “*On the Deterministic Complexity of Factoring Polynomials*,” *Journal of Symbolic Computation* (2001) **31**, pp. 19–36.
- [GJ79] Garey, Michael R. and Johnson, David S. *Computers and Intractability: A Guide to the Theory of NP-Completeness*, A Series of Books in the Mathematical Sciences, W. H. Freeman and Co., San Francisco, Calif., 1979.
- [vzGKS96] von zur Gathen, Joachim; Karpinski, Marek; and Shparlinski, Igor, “*Counting curves and their projections*,” *Computational Complexity* 6, no. 1 (1996/1997), pp. 64–99.
- [GKZ94] Gel’fand, Israel Moseyevitch; Kapranov, Misha M.; and Zelevinsky, Andrei V.; *Discriminants, Resultants and Multidimensional Determinants*, Birkhäuser, Boston, 1994.
- [GH93] Giusti, Marc and Heintz, Joos, “*La détermination des points isolés et la dimension d’une variété algébrique peut se faire en temps polynomial*,” *Computational Algebraic Geometry and Commutative Algebra (Cortona, 1991)*, Sympos. Math. XXXIV, pp. 216–256, Cambridge University Press, 1993.
- [HS00] Hindry, Marc and Silverman, Joseph H., *Introduction to Diophantine Geometry*, Graduate Texts in Mathematics, vol. 201, Springer-Verlag, 2000.
- [Kal03] Kaltofen, Erich, “*Polynomial factorization: a success story*,” In ISSAC 2003 Proc. 2003 Internat. Symp. Symbolic Algebraic Comput. (New York, N.Y., 2003), J. R. Sendra, Ed., ACM Press, pp. 3–4.
- [KK05] Kaltofen, Erich and Koiran, Pascal, “*Finding small degree factors of multivariate super-sparse (Lacunary) Polynomials over algebraic number fields*,” in ISSAC ’06, Proc. 2006 Internat. Symp. Symbolic Algebraic Comput., to appear, ACM Press.
- [KaShp99] Karpinski, Marek and Shparlinski, Igor, “*On the computational hardness of testing square-freeness of sparse polynomials*,” *Applied algebra, algebraic algorithms and error-correcting codes (Honolulu, HI, 1999)*, pp. 492–497, Lecture Notes in Comput. Sci., 1719, Springer, Berlin, 1999.
- [Kho91] Khovanski, Askold, *Fewnomials*, AMS Press, Providence, Rhode Island, 1991.
- [KiSha99] Kipnis, Aviad and Shamir, Adi, “*Cryptanalysis of the HFE public key cryptosystem by relinearization*,” *Advances in cryptology — CRYPTO ’99 (Santa Barbara, CA)*, pp. 19–30, Lecture Notes in Comput. Sci., 1666, Springer, Berlin, 1999.
- [Lau04] Lauder, Alan G. B., “*Counting solutions to equations in many variables over finite fields*,” *Found. Comput. Math.* 4 (2004), no. 3, pp. 221–267.
- [Len99a] Lenstra (Jr.), Hendrik W., “*Finding Small Degree Factors of Lacunary Polynomials*,” *Number Theory in Progress, Vol. 1 (Zakopane-Kościelisko, 1997)*, pp. 267–276, de Gruyter, Berlin, 1999.
- [Len99b] _____, “*On the Factorization of Lacunary Polynomials*,” *Number Theory in Progress, Vol. 1 (Zakopane-Kościelisko, 1997)*, pp. 277–291, de Gruyter, Berlin, 1999.
- [LLL82] Lenstra, Arjen K.; Lenstra (Jr.), Hendrik W.; Lovász, L., “*Factoring polynomials with rational coefficients*,” *Math. Ann.* 261 (1982), no. 4, pp. 515–534.

- [LP05] Lenstra (Jr.), Hendrik W., and Pomerance, Carl, “*Primality Testing with Gaussian Periods*,” manuscript, downloadable from <http://www.math.dartmouth.edu/~carlp/PDF/complexity12.pdf> .
- [Lip88] Lipshitz, Leonard, “*p-adic Zeros of Polynomials*,” J. Reine Angew. Math. **390** (1988), pp. 208–214.
- [MW96] Maller, Michael and Whitehead, Jennifer, “*Computational complexity over the 2-adic numbers*,” The mathematics of numerical analysis (Park City, UT, 1995), pp. 513–521, Lectures in Appl. Math., 32, Amer. Math. Soc., Providence, RI, 1996.
- [MW97] Maller, Michael and Whitehead, Jennifer, “*Computational complexity over the p-adic numbers*,” J. Complexity 13 (1997), no. 2, pp. 195–207.
- [Mat73] Matiyasevich, Yuri V., “*On Recursive Unsolvability of Hilbert’s Tenth Problem*,” Logic, Methodology and Philosophy of Science, IV (Proc. Fourth Internat. Congr., Bucharest, 1971), pp. 89–110, Studies in Logic and Foundations of Math., Vol. 74, North-Holland, Amsterdam, 1973.
- [Mig82] Mignotte, Maurice, “*Some Useful Bounds*,” in Computer Algebra: Symbolic and Algebraic Computation, 2nd ed., (edited by B. Buchberger, G. E. Collins, and R. Loos, in cooperation with R. Albrecht), Springer-Verlag 1982.
- [Pap95] Papadimitriou, Christos H., *Computational Complexity*, Addison-Wesley, 1995.
- [Pla84] Plaisted, David A., “*New NP-Hard and NP-Complete Polynomial and Integer Divisibility Problems*,” Theoret. Comput. Sci. 31 (1984), no. 1–2, 125–138.
- [Pla06] Plaisted, David A., *e-mail communication*, March 28, 2006.
- [Poo01a] Poonen, Bjorn, “*An explicit algebraic family of genus-one curves violating the Hasse principle*,” 21st Journées Arithmétiques (Rome, 2001), J. Théor. Nombres Bordeaux 13 (2001), no. 1, pp. 263–274.
- [Poo01b] _____, “*The Hasse principle for complete intersections in projective space*,” Rational points on algebraic varieties, pp. 307–311, Progr. Math., 199, Birkhuser, Basel, 2001.
- [Poo03] _____, “*Hilbert’s tenth problem and Mazur’s conjecture for large subrings of \mathbb{Q}* ,” J. Amer. Math. Soc. 16 (2003), no. 4, pp. 981–990.
- [Poo06] _____, “*Heuristics for the Brauer-Manin Obstruction for Curves*,” Experimental Mathematics, Volume 15, Issue 4 (2006), pp. 415–420.
- [Poo07] _____, “*Characterizing Integers Among Rational Numbers with a Universal-Existential Formula*,” Math ArXiv preprint [math.NT/0703907](https://arxiv.org/abs/math.NT/0703907) .
- [Rob00] Robert, Alain M., *A course in p-adic analysis*, Graduate Texts in Mathematics, 198, Springer-Verlag, New York, 2000.
- [Roj01a] Rojas, J. Maurice, “*Computational Arithmetic Geometry I: Sentences Nearly in the Polynomial Hierarchy*,” J. Comput. System Sci., STOC ’99 special issue, vol. 62, no. 2, march 2001, pp. 216–235.

- [Roj02] _____, “*Additive Complexity and the Roots of Polynomials Over Number Fields and p -adic Fields*,” Proceedings of ANTS-V (5th Annual Algorithmic Number Theory Symposium, University of Sydney, July 7–12, 2002), Lecture Notes in Computer Science #2369, Springer-Verlag (2002), pp. 506–515.
- [Roj04] _____, “*Arithmetic Multivariate Descartes’ Rule*,” American Journal of Mathematics, vol. 126, no. 1, February 2004, pp. 1–30.
- [Roj07b] _____, “*Efficiently Detecting Torsion Points and Subtori*,” proceedings of MAGIC 2005 (Midwest Algebra, Geometry, and their Interactions Conference, Oct. 7–11, 2005, Notre Dame University, Indiana), edited by A. Corso, J. Migliore, and C. Polini), pp. 213–233, Contemporary Mathematics, AMS Press, to appear.
- [Sil96] Silverman, Joseph H., *The Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics, vol. 106, Springer-Verlag, 1996.

5 Appendix: Proofs of Secondary Results

(Correctness and Success Probability of Algorithm 2.3): First observe that M_1, \dots, M_L are relatively prime. So at most ℓ of the M_i will be divisible by elements of $\mathcal{E}(x)$. Note also that $K \geq 1$ and $1 + cM_i \leq 1 + KM_i \leq 1 + ((x-1)/M_i)M_i = x$ for all $i \in [L]$ and $c \in [K]$.

Since $x \geq x_0$ and $x^{2/5} \geq (x-1)^{2/5} \geq \left(M_i^{5/2}\right)^{2/5} = M_i$ for all $i \in [L]$, the AGP Theorem implies that with probability $\geq 1 - \frac{\varepsilon}{3}$ (since $i \in [\lceil 3/\varepsilon \rceil \ell]$ is uniformly random), the arithmetic progression $\{1 + M_i, \dots, 1 + KM_i\}$ contains at least $\frac{\pi(x)}{2\varphi(M_i)} \geq \frac{\pi(x)}{2M_i}$ primes. In which case, the proportion of numbers in $\{1 + M_i, \dots, 1 + KM_i\}$ that are prime is $\frac{\pi(x)}{2KM_i} > \frac{\pi(x)}{2+2KM_i} > \frac{x/\log x}{2x} = \frac{1}{2\log x}$, since $\pi(x) > x/\log x$ for all $x \geq 17$ [BS96, Thm. 8.8.1, pg. 233]. So let us now assume that i is fixed and M_i is not divisible by any element of $\mathcal{E}(x)$.

Recalling the inequality $(1 - \frac{1}{i})^{ct} \leq e^{-c}$ (valid for all $c \geq 0$ and $t \geq 1$), we then see that the AGP Theorem implies that the probability of **not** finding a prime of the form $p = 1 + cM_i$ after picking J uniformly random $c \in [K]$ is $\left(1 - \frac{1}{2\log x}\right)^J \leq \left(1 - \frac{1}{2\log x}\right)^{2\log(3/\varepsilon)\log x} \leq e^{-\log(3/\varepsilon)} = \frac{\varepsilon}{3}$.

Now, by the structure of the maximum in the definition of x , we have

$K = \lfloor (x-1)/M_i \rfloor \geq \lfloor M_L \lceil 1 + 3s'/\varepsilon \rceil / M_i \rfloor \geq \lfloor (1 + 3s'/\varepsilon)M_L/M_i \rfloor \geq (3s'/\varepsilon)M_L/M_L = 3s'/\varepsilon$, and thus x is large enough so that, with probability $\geq 1 - \frac{\varepsilon}{3}$, our random $1 + cM_i$ avoids S_P .

In summary, with probability $\geq 1 - \frac{\varepsilon}{3} - \frac{\varepsilon}{3} - \frac{\varepsilon}{3} = 1 - \varepsilon$, Algorithm 2.3 picks an i with M_i not divisible by any element of $\mathcal{E}(x)$ and a c such that $p := 1 + cM_i$ is prime and avoids S_P . In particular, we clearly have that $\log p = O(\log(1 + KM_i)) = O(n \log(n) + \log(s/\varepsilon))$. ■

(Complexity Analysis of Algorithm 2.3): Let $L' := nL$ and, for the remainder of our proof, let p_i denote the i^{th} prime. Since $L' \geq 6$, $p_{L'} \leq L'(\log(L') + \log \log L')$ by [BS96, Thm. 8.8.4, pg. 233]. Recall that the primes in $[\mathcal{L}]$ can be listed simply by deleting all multiples of 2 in $[\mathcal{L}]$, then deleting all multiples of 3 in $[\mathcal{L}]$, and so on until one reaches multiples of $\lfloor \sqrt{\mathcal{L}} \rfloor$. (This is the classic sieve of Eratosthenes.) Recall also that one can multiply an integer in $[\mu]$ and an integer $[\nu]$ within $O((\log \mu)(\log \log \nu)(\log \log \log \nu) + (\log \nu)(\log \log \mu) \log \log \log \mu)$ bit operations (see, e.g., [BS96, Table 3.1, pg. 43]). So let us define the function $\lambda(a) := (\log \log a) \log \log \log a$.

Step 0: By our preceding observations, it is easily checked that Step 0 takes $O(L'^{3/2} \log^3 L')$ bit operations.

Step 1: This step consists of $n - 1$ multiplications of primes with $O(\log L')$ bits (resulting in M_L , which has $O(n \log L')$ bits), multiplication of a small power of M_L by a square root of M_L , multiplication of powers of M_L by an integer with $O(\log(s/\varepsilon))$ bits, division by an integer with $O(n \log L')$ bits, a constant number of additions of integers of comparable size, and the generation of $O(\log L)$ random bits. Employing Remark 2.4 along the way, we thus arrive routinely at an estimate of

$$O(n^2(\log L')\lambda(L') + \log(s/\varepsilon)\lambda(s/\varepsilon))$$

for the total number of bit operations needed for Step 1.

Step 2: Similar to our analysis of Step 1, we see that Step 2 has bit complexity

$$O((n \log(L') + \log(s/\varepsilon))\lambda(n \log L')).$$

Step 3: This is our most costly step: Here, we require

$$O(\log K) = O(n \log(L') + \log(s/\varepsilon))$$

random bits and $J = O(\log x) = O(n \log(L') + \log(s/\varepsilon))$ primality tests on integers with $O(\log(1 + cM_i)) = O(n \log(L') + \log(s/\varepsilon))$ bits. By an improved version of the AKS primality testing algorithm [AKS02, LP05] (which takes $O(N^{6+\delta})$ bit operations to test an N bit integer for primality), Step 3 can then clearly be done within

$$O((n \log(L') + \log(s/\varepsilon))^{7+\delta})$$

bit operations, and the generation of $O(n \log(L') + \log(s/\varepsilon))$ random bits.

Step 4: This step clearly takes time on the order of the number of output bits, which is just $O(n \log(n) + \log(s/\varepsilon))$ as already observed earlier.

Conclusion: We thus see that Step 0 and Step 3 dominate the complexity of our algorithm, and we are left with an overall randomized complexity bound of

$$\begin{aligned} & O\left(L'^{3/2} \log^3(L') + (n \log(L') + \log(s/\varepsilon))^{7+\delta}\right) \\ &= O\left(\left(\frac{n}{\varepsilon}\right)^{3/2} \log^3(n/\varepsilon) + (n \log(n) + \log(s/\varepsilon))^{7+\delta}\right) \\ &= O\left(\left(\frac{n}{\varepsilon}\right)^{\frac{3}{2}+\delta} + (n \log(n) + \log(s/\varepsilon))^{7+\delta}\right) \end{aligned}$$

randomized bit operations. ■

(Proof of Lemma 2.7): First note that by our assumption on p , the fields \mathbb{F}_p and \mathbb{Q}_p each have D distinct D^{th} roots of unity: The first containment is immediate since the unit group \mathbb{F}_p^* is cyclic of order divisible by D , and the second follows easily from Hensel's Lemma (cf. Section 4 below) and \mathbb{F}_p having D distinct D^{th} roots of unity.

Assertion 1: Since $\mathbb{Z} \hookrightarrow \mathbb{Q}_p$ and \mathbb{Q}_p contains all D^{th} roots of unity by construction, the equivalence follows directly from Lemma 2.6.

Assertion 2: Note that $f(x_1) = x_1^D - 1 = 0$ has a root in $\mathbb{C} \implies \text{Res}_{d,D}(f(x_1), x_1^D - 1) = 0$. The latter condition in turn implies that $\text{Res}_{d,D}(f(x_1), x_1^D - 1)$ is divisible by p and thus, by Lemma 2.6 once more, $f(x_1) = x_1^D - 1 = 0$ has a root in \mathbb{F}_p .

Assertion 3: Lemma 2.6 implies that if $f(x_1) = x_1^D - 1 = 0$ has **no** complex root then the Sylvester matrix $\mathcal{S} := \mathcal{S}_{(d,D)}(f, x_1^D - 1)$ has full rank, and the corresponding resultant \mathcal{R} is a nonzero integer with $\log |\mathcal{R}| = O(d + D \log(mH))$. Therefore, there must be a row-vector

$$w := [u_0, \dots, u_{D-1}, v_0, \dots, v_{d-1}] \in \mathbb{Q}^{D+d}$$

such that $w\mathcal{S} = [1, 0, \dots, 0]$. Defining $g_1(x_1) := u_0 + \dots + u_{D-1}x_1^{D-1}$ and $g_2(x_1) := v_0 + \dots + v_{d-1}x_1^{d-1}$, it is then easily checked that $g_1(x_1)f(x_1) + (x_1^D - 1)g_2(x_1) = 1$ identically. By Cramer's Rule, we then see that the u_i and v_j have common denominator dividing \mathcal{R} . So $\bar{g}_1(x_1)f(x_1) + (x_1^D - 1)\bar{g}_2(x_1) = \mathcal{R}$ identically, where $\bar{g}_i = \mathcal{R}g_i \in \mathbb{Z}[x_1]$ for all $i \in [2]$.

Thus, if p is a prime **not** dividing \mathcal{R} , the last identity persists modulo p and clearly implies the impossibility of a root in \mathbb{F}_p for $(f(x_1), x_1^D - 1)$. (Evaluating the last polynomial linear combination at a putative root would result in the false identity $0 = \mathcal{R}$.) Since the number of prime divisors of \mathcal{R} is bounded above by $1 + \log |\mathcal{R}|$, we are done. ■

5.1 Some Additional Algebraic Basics

Hensel's Lemma (See, e.g., [Rob00, Pg. 48].) Suppose $f \in \mathbb{Z}_p[x_1]$ and $\zeta_0 \in \mathbb{Z}_p$ satisfies $f(\zeta_0) \equiv 0 \pmod{p^\ell}$ and $\text{ord}_p f'(\zeta_0) < \frac{\ell}{2}$. Then there is a root $\zeta \in \mathbb{Z}_p$ of f with $\zeta \equiv \zeta_0 \pmod{p^{\ell - \text{ord}_p f'(\zeta_0)}}$ and $\text{ord}_p f'(\zeta) = \text{ord}_p f'(\zeta_0)$. ■

The **p -adic Newton polygon**, defined below, will allow us to easily read off the norms of p -adic roots of polynomials. In particular, recall that the convex hull of any subset $S \subseteq \mathbb{R}^2$ is the smallest convex set containing S . Also, an edge of a polygon $P \subset \mathbb{R}^2$ is called **lower** iff it has an inner normal with positive last coordinate, and the **lower hull** of P is simply the union of all lower edges. Finally, for any prime p and $x \in \mathbb{Z}_p$, recall that the **p -adic valuation**, $\text{ord}_p x$, is the greatest k such that $p^k | x$. We then extend $\text{ord}_p(\cdot)$ to \mathbb{Q}_p by $\text{ord}_p\left(\frac{a}{b}\right) := \text{ord}_p(a) - \text{ord}_p(b)$ for any $a, b \in \mathbb{Z}_p$; and we let $|x|_p := p^{-\text{ord}_p x}$ denote the **p -adic norm**. The norm $|\cdot|_p$ defines a natural

metric satisfying the ultrametric inequality and, along with $\text{ord}_p(\cdot)$, extends naturally to the **p -adic complex numbers** \mathbb{C}_p (the metric completion of the algebraic closure of \mathbb{Q}_p) [Rob00, Ch. 3].

Lemma 5.1 (See, e.g., [Rob00, Ch. 6, sec. 1.6].) *Given any polynomial $f(x_1) := \sum_{i=1}^m c_i x_1^{a_i} \in \mathbb{Z}[x_1]$, we define its **p -adic Newton polygon**, $\text{Newt}_p(f)$, to be the convex hull of the points $\{(a_i, \text{ord}_p c_i) \mid i \in \{1, \dots, m\}\}$. Then the number of roots of f in \mathbb{C}_p with valuation v , counting multiplicities, is **exactly** the horizontal length of the lower face of $\text{Newt}_p(f)$ with inner normal $(v, 1)$. ■*

The final tool we will need is a standard lemma on binomial equations over certain finite groups. Recall that for any ring R , we denote its unit group by R^* .

Lemma 5.2 (See, e.g., [BS96, Thm. 5.7.2 & Thm. 5.6.2, pg. 109]) *Given any cyclic group G , $a \in G$, and an integer d , the following 3 conditions are equivalent:*

1. *the equation $x^d = a$ has a solution $x \in G$.*
2. *the order of a divides $\frac{\#G}{\gcd(d, \#G)}$.*
3. *$a^{\#G/\gcd(d, \#G)} = 1$.*

Also, \mathbb{F}_q^ is cyclic for any prime power q , and $(\mathbb{Z}/p^\ell\mathbb{Z})^*$ is cyclic for any (p, ℓ) with p an odd prime or $\ell \leq 2$. Finally, for $\ell \geq 3$, $(\mathbb{Z}/2^\ell\mathbb{Z})^* = \{\pm 1, \pm 5, \pm 5^2, \pm 5^3, \dots, \pm 5^{2^{\ell-2}-1} \pmod{2^\ell}\}$. ■*

5.2 The Proofs of Corollaries 1.5 and 1.11

The latter halves of our corollaries require one last modular reduction result, analogous to Lemma 2.7.

Lemma 5.3 *Suppose $f \in \mathbb{Z}[x_1] \setminus \{0\}$ has degree d , exactly m monomial terms, and maximum coefficient absolute value H . Then*

1. *For any prime p , f has a repeated factor over $\mathbb{Z}[x_1] \iff f$ has a repeated factor over $\mathbb{Q}_p[x_1]$.*
2. *With the exception of $O(d^2 + d \log H)$ primes p , f has a repeated factor over $\mathbb{Z}[x_1] \implies f$ has a repeated factor over $\mathbb{F}_p[x_1]$.*
3. *With the exception of $O(d \log(dmH))$ primes p , f has **no** repeated factors over $\mathbb{Z}[x_1] \implies f$ has **no** repeated factors over $\mathbb{F}_p[x_1]$.*

*We call the primes for which the implications in Assertions 2 or 3 fail **exceptional (for f)**.*

Proof of Lemma 5.3: Assertion 1 follows immediately upon observing that $\mathbb{Z} \hookrightarrow \mathbb{Q}_p$ and applying Lemma 2.6 to (f, f') .

For Assertion 2, one simply observes that the coefficients of any factor of f have bit-size $O(d + \log H)$ [Mig82, Thm. 4, pg. 261]. Thus, as long as $p > d + 1$, p does not divide all the coefficients of f , and p does not divide all the coefficients of some factor of f , any factor of f over $\mathbb{Z}[x_1]$ retains its degree after mod p reduction and our implication holds. Counting the number of primes for which these conditions fail, we obtain no more than $d + 1 + (d + 1)O(d + \log H)$ such primes and we are done.

For Assertion 3, we proceed as in the proof of Assertion 3 of Lemma 2.7, except that we employ the resultant of (f, f') instead of the resultant of (f, g) . ■

Proof of Corollary 1.5

(Deciding $\text{deggcd}(f, g) > 0$ over the rings $\{\mathbb{F}_p[x_1]\}_p$ prime in BPP $\implies \text{NP} \subseteq \text{BPP}$): At an intermediate step of our proof of Theorem 1.4, we saw that deciding whether $f(x_1) = x_1^D - 1 = 0$ has a root in \mathbb{F}_p (with $p \equiv 1 \pmod{D}$) is **NP-hard** under **BPP** reductions. Clearly, the latter feasibility

question has an affirmative answer iff $f(x_1)$ and $x_1^D - 1$ have gcd of positive degree in $\mathbb{F}_p[x_1]$. So we are done.

(Detecting repeated factors over the rings $\{\mathbb{F}_p[x_1]\}_{p \text{ prime}}$ in $\mathbf{BPP} \implies \mathbf{NP} \subseteq \mathbf{BPP}$): From the proof of [KaShp99, Cor. 1], we know that deciding whether $f \in \mathbb{Z}[x_1]$ has repeated factors over $\mathbb{Z}[x_1]$ is \mathbf{NP} -hard with respect to \mathbf{coRP} reductions. So it suffices to find a \mathbf{BPP} -reduction from this problem to its finite-field analogue. This immediately follows upon using Algorithm 2.3 — with $i = n = 1$, $x_0 = 17$, $\ell = 0$, and S_P equal to the set of primes exceptional for f (cf. Lemma 5.3) — to generate a suitable prime p . In particular, we can work with the arithmetic progression $\{1 + 2, 1 + 2 \cdot 2, 1 + 3 \cdot 2, \dots\}$ and simply use the classical Prime Number Theorem instead of the AGP Theorem. So we are done. ■

Proof of Corollary 1.11

(Deciding $\text{deggcd}(f, g) > 0$ over the rings $\{\mathbb{Q}_p[x_1]\}_{p \text{ prime}}$ in $\mathbf{ZPP} \implies \mathbf{NP} \subseteq \mathbf{ZPP}$): At an intermediate step of our proof of Theorem 1.8, we saw that deciding whether $f(x_1) = x_1^D - 1 = 0$ has a root in \mathbb{Q}_p (with $p \equiv 1 \pmod{D}$) is \mathbf{NP} -hard with respect to \mathbf{ZPP} reductions. Clearly, the latter feasibility question has an affirmative answer iff $f(x_1)$ and $x_1^D - 1$ have gcd of positive degree in $\mathbb{Q}_p[x_1]$. So we are done.

(Detecting repeated factors over $\mathbb{Q}_p[x_1]$ in $\mathbf{coRP} \implies \mathbf{NP} \subseteq \mathbf{coRP}$): From the proof of [KaShp99, Cor. 1], we know that deciding whether $f \in \mathbb{Z}[x_1]$ has repeated factors over $\mathbb{Z}[x_1]$ is \mathbf{NP} -hard with respect to \mathbf{coRP} reductions. So it suffices to find a \mathbf{coRP} -reduction from this problem to its $\mathbb{Q}_p[x_1]$ analogue. Thanks to Assertion 1 of Lemma 5.3, our reduction can simply be the replacement of f by the pair (f, p) , for **any** fixed prime p . So we are done. ■