On Interpolating Between Quantum and Classical Complexity Classes

J. Maurice Rojas*

March 8, 2007

Abstract

We reveal a natural algebraic problem whose complexity appears to interpolate between the well-known complexity classes **BQP** and **NP**:

$\star$ Decide whether a univariate polynomial with exactly m monomial terms has a p-adic rational root.

In particular, we show that while $(\star)$ is doable in quantum randomized polynomial time when $m=2$, $(\star)$ is nearly **NP**-complete for general m. In particular, $(\star)$ is in **NP** for most inputs and, under a plausible hypothesis involving primes in arithmetic progression (implied by the Generalized Riemann Hypothesis for certain cyclotomic fields), a randomized polynomial time algorithm for $(\star)$ would imply the widely disbelieved inclusion $\mathbf{NP}\subseteq\mathbf{BPP}$. This type of quantum/classical interpolation phenomenon appears to be new. As a consequence we can also address recent questions on the complexity of polynomial factorization posed by Cox, and Karpinski and Shparlinski.

1 Introduction and Main Results

Thanks to quantum computation, we now have exponential speed-ups for important practical problems such as Integer Factoring (IF) and Discrete Logarithm (DL) [Sho97]. However, a fundamental open question that remains is whether there are any **NP-complete** problems admitting exponential speed-ups via quantum computation. (We briefly review the complexity classes **NP** and **BQP**, as well as a few more, in Section 2 below.) Succinctly, this is the $\mathbf{NP}\stackrel{?}{\subseteq}\mathbf{BQP}$ question [BV97], and a positive answer would imply that quantum computation can also provide efficient algorithms for a myriad of problems (all at least as hard IF or DL) that have occupied practicioners in optimization and computer science for decades. The truth of the inclusion $\mathbf{NP}\subseteq\mathbf{BQP}$ is currently unknown as of early 2007. However, in light of important derandomization results [IW97], there is reason to believe the opposite (and also unknown) inclusion $\mathbf{BQP}\subseteq\mathbf{NP}$.

We propose an algebraic approach to these questions by illustrating a decision problem, involving sparse polynomials over $\mathbb{Q}_p$ (the p-adic rationals), whose complexity appears to interpolate between the complexity classes **BQP** and **NP**. Roughly speaking, "interpolation" here means that we have a decision problem, with computational complexity an increasing function of a parameter m, such that our problem...

*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.

(a) ...can be solved by a quantum computer in polynomial time, with error probability $< \frac{1}{3}$, for small values of m,
(b) ...can be used to simulate any computation in **BQP**, for small values of m,
(c) ...is **NP**-hard for large values of m, and
(d) ...can be solved in **NP** for large values of m.

Given a problem satisfying properties (a)–(d), one could then obtain the inclusion $\mathbf{BQP} \subseteq \mathbf{NP}$. Furthermore, one could then in principle study the transition from **BQP** to **NP** by analyzing the complexity of our interpolating problem for "mid-range" values of m. Our p-adic problem stated in the Main Theorem below satisfies Properties (a), (d) (for most inputs) and, under a plausible number-theoretic assumption clarified below, Property (c) as well. We will discuss the difficulty behind attaining all 4 properties shortly.

First, let us review some necessary terminology: For any ring R containing the integers $\mathbb{Z}$, let $\mathbf{FEAS}_R$ — the **R-feasibility problem** — denote the problem of deciding whether a given system of polynomials $f_1, \ldots, f_k$ chosen from $\mathbb{Z}[x_1, \ldots, x_n]$ has a root in R^n. Observe then that $\mathbf{FEAS}_{\mathbb{R}}$ and $\mathbf{FEAS}_{\mathbb{Q}}$ are respectively the central problems of algorithmic real algebraic geometry and algorithmic arithmetic geometry (see Section 1.1 below for further details).

To measure the "size" of an input polynomial in our complexity estimates, we will essentially just count the number of bits needed to write down the coefficients and exponents in its monomial term expansion. This is the **sparse** input size, as opposed to the "dense" input size used frequently in computational algebra.

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

$$\mathrm{size}(f) := \sum_{i=1}^{m} \left(1 + \lceil \log_2(2 + |c_i|) \rceil + \lceil \log_2(2 + |a_{1,i}|) \rceil + \cdots + \lceil \log_2(2 + |a_{n,i}|) \rceil\right),$$

and $\mathrm{size}_p(f) := \mathrm{size}(f) + \log(2 + p)$. (We also extend size*, and thereby* size_p*, additively to polynomial systems.) Finally, for any collection $\mathcal{F}$ of polynomial systems with integer coefficients, let $\mathbf{FEAS}_R(\mathcal{F})$ denote the natural restriction of $\mathbf{FEAS}_R$ to inputs in $\mathcal{F}$.* $\diamond$

Observe that $\mathrm{size}(a + bx^{99} + cx^d) = O(\log d)$ if we fix a, b, c. The degree of a polynomial can thus sometimes be exponential in its sparse size. Since it is not hard to show that $\mathbf{FEAS}_{\mathbb{Q}_p}(\mathbb{Z}[x_1]) \in \mathbf{P}$ when p is fixed (cf. Section 3 below), it will be more natural to take the size of an input prime p into account as well, and we do so as follows.

Definition 2 *Let $\mathbf{FEAS}_{\mathbb{Q}_{\mathrm{primes}}}$ (resp. $\mathbf{FEAS}_{\mathbb{Q}_{\mathrm{primes}}}(\mathcal{F})$) denote the union of problems $\bigcup_{p \text{ prime}} \mathbf{FEAS}_{\mathbb{Q}_p}$ (resp. $\bigcup_{p \text{ prime}} \mathbf{FEAS}_{\mathbb{Q}_p}(\mathcal{F})$), so that a prime p is also part of the input, and the underlying input size is* size_p*. Also let Q_n denote the product of the first n primes and define $\mathcal{U}_m := \{f \in \mathbb{Z}[x_1] \mid f \text{ has } \leq m \text{ monomial terms}\}$.* $\diamond$

Observe that $\mathbb{Z}[x_1]$ is thus the union $\bigcup_{m \geq 0} \mathcal{U}_m$. Our results will make use of the following plausible number-theoretic hypothesis.

Flat Primes Hypothesis (FPH) *Following the notation above, there is an absolute constant $C \geq 1$ such that for any $n \in \mathbb{N}$, the set $\{1 + kQ_n \mid k \in \{1, \ldots, 2^{n^C}\}\}$ contains at least $\frac{2^{n^C}}{n}$ primes.*

Assumptions at least as strong as FPH are routinely used, and widely believed, in the cryptology and algorithmic number theory communities (see, e.g., [Mil76, Mih94, Koi97, Roj01a, Hal05]). In particular, we will see in Section 2.1 below how FPH is implied by the Generalized Riemann Hypothesis (GRH) for the number fields $\{\mathbb{Q}(\omega_{Q_n})\}_{n\in\mathbb{N}}$, where ω_M denotes a primitive $M^{\underline{\text{th}}}$ root of unity[1], but can still hold under certain failures of the latter hypotheses.

Main Theorem *Following the notation above,* $\mathbf{FEAS}_{\mathbb{Q}_{\text{primes}}}(\mathcal{U}_2) \in \mathbf{BQP}$. *Also,* $\mathbf{FEAS}_{\mathbb{Q}_{\text{primes}}}(\mathbb{Z}[x_1]) \in \mathbf{NP}$ *for "most" inputs in the following sense: For any* $f \in \mathbb{Z}[x_1]$ *and* $\varepsilon > 0$, *a fraction of at least* $1-\varepsilon$ *of the primes* p *with* $O\left(\log\left(\frac{1}{\varepsilon}\right) + \text{size}(f)\right)$ *digits are such that the solvability of* f *over* $\mathbb{Q}_p$ *admits a succinct certificate. Finally, assuming the truth of FPH, if* $\mathbf{FEAS}_{\mathbb{Q}_{\text{primes}}}(\mathbb{Z}[x_1]) \in \mathcal{C}$ *for some complexity class* $\mathcal{C}$, *then* $\mathbf{NP} \subseteq \mathbf{BPP} \cup \mathcal{C}$. *In particular, assuming the truth of FPH,* $\mathbf{FEAS}_{\mathbb{Q}_{\text{primes}}}(\mathbb{Z}[x_1]) \in \mathbf{BQP} \Longrightarrow \mathbf{NP} \subseteq \mathbf{BQP}$.

Our main result thus suggests that sparse polynomials can provide a tool to shed light on the difference between **BQP** and **NP**. Indeed, one consequence of our results is a new family of problems which admit (or are likely to admit) **BQP** algorithms: even the complexity of $\mathbf{FEAS}_{\mathbb{Q}_{\text{primes}}}(\mathcal{U}_3)$ is currently unknown, so the problems $\{\mathbf{FEAS}_{\mathbb{Q}_{\text{primes}}}(\mathcal{U}_m)\}_{m\geq 3}$ provide a new context — distinct from Integer Factoring or Discrete Logarithm — to study quantum speed-up over classical methods.

Remarks 1 *While it has been known since the late 1990's that* $\mathbf{FEAS}_{\mathbb{Q}_{\text{primes}}} \in \mathbf{EXPTIME}$ *[MW96, MW97] (relative to our notion of input size), we are unaware of any earlier algorithms yielding* $\mathbf{FEAS}_{\mathbb{Q}_{\text{primes}}}(\mathcal{F}) \in \mathbf{BQP}$, *for any non-trivial family of polynomial systems* $\mathcal{F}$. *Also, while it is not hard to show that* $\mathbf{FEAS}_{\mathbb{Q}_{\text{primes}}}$ *is* **NP***-hard from scratch, there appear to be no earlier results indicating the smallest* n *such that* $\mathbf{FEAS}_{\mathbb{Q}_{\text{primes}}}(\mathbb{Z}[x_1, \ldots, x_n])$ *is* **NP***-hard.* $\diamond$

The author is unaware of any other natural algebraic problem that at least partially interpolates between **BQP** and **NP** in the sense above. The only other problem known to interpolate between **BQP** and **some** classical complexity class arises from very recent results on the complexity of approximating a certain braid invariant — the famous **Jones polynomial**, for certain classes of braids, evaluated at an $m^{\underline{\text{th}}}$ root of unity — and involves a complexity class apparently higher than **NP**. In brief: (a') [AJL05] gives a **BQP** algorithm that computes an additive approximation for arbitrary m, (b') seminal work of Freedman, Kitaev, Larsen, and Wang shows that such approximations can simulate any **BQP** computation, already for $m = 5$ [FKW02, FLW02], and (c') [YW06] shows that for arbitrary m, computing the most significant bit of the absolute value of the Jones polynomial is **PP**-hard. In particular, the very notion of **BQP**-completeness is subtle: the Jones polynomial provides the **only** known non-trivial **BQP**-complete problem [AA06] (as opposed to the hundreds of **NP**-complete problems now known [GJ79]), and the definition is technically rather different from that of **NP**-completeness [KL99, AA06].

Thus, while we do not know whether $\mathbf{FEAS}_{\mathbb{Q}_{\text{primes}}}(\mathcal{U}_2)$ is **BQP**-complete in any rigourous sense, our results nevertheless provide a new potential source for quantum/classical complexity interpolation. Note also that the **BQP**-completeness of Integer Factoring and Discrete Logarithm are open questions as well.

[1] i.e., a complex number ω_M with $\omega_M^M = 1$; and $\omega_M^d = 1 \Longrightarrow M|d$

Recall that a univariate polynomial has a root in a field K iff it possesses a degree 1 factor with coefficients in K. Independent of its connection to quantum computing, our Main Theorem also provides a new complexity limit for polynomial factorization over $\mathbb{Q}_p[x_1]$. In particular, the Main Theorem shows that finding even just the low degree factors for **sparse** polynomials (with $\log p$ a summand in the sparse input size) is likely **not** doable in randomized polynomial time. This complements Chistov's earlier deterministic polynomial time algorithm for dense polynomials and fixed p [Chi91]. Our Main Theorem also provides an interesting contrast to earlier work of Lenstra [Len99a], who showed that — over the ring $\mathbb{Q}[x_1]$ instead — one can find all **low** degree factors of a sparse polynomial in polynomial time (thus improving the famous Lenstra-Lenstra-Lovasz algorithm [LLL82]).

One can also naturally ask if detecting a **degenerate** root in $\mathbb{Q}_p$ for f (i.e., a degree 1 factor over $\mathbb{Q}_p$ whose square also divides f) is as hard as detecting arbitary roots in $\mathbb{Q}_p$. Via our techniques, we can easily prove essentially the same complexity lower-bound as above for the latter problem.

Corollary 1 *Using* $\text{size}_p(f)$ *as our notion of input size, suppose we can decide for any input prime* p *and* $f \in \mathbb{Z}[x_1]$ *whether* f *is divisible by the square of a degree* 1 *polynomial in* $\mathbb{Q}_p[x_1]$*, within some complexity class* $\mathcal{C}$*. Then, assuming the truth of FPH,* $\mathbf{NP} \subseteq \mathcal{C} \cup \mathbf{BPP}$*.*

Let $\mathbb{F}_p$ denote the finite field with p elements. Corollary 1 then complements an analogous earlier result of Karpinski and Shparlinski (independent of the truth of FPH) for detecting degenerate roots in $\mathbb{C}$ and the algebraic closure of $\mathbb{F}_p$.

Note also that while the truth of GRH usually implies algorithmic speed-ups (in contexts such as primality testing [Mil76], complex dimension computation [Koi97], detection of rational points [Roj01a], and class group computation [Hal05]), the Main Theorem and Corollary 1 instead reveal complexity **speed-limits** implied by GRH.

1.1 Open Questions and the Relevance of Ultrametric Complexity

Complexity results over one ring sometimes inspire and motivate analogous results over other rings. An important early instance of such a transfer was the work of Paul Cohen on quantifier elimination over $\mathbb{R}$ and $\mathbb{Q}_p$ [Coh69]. To close this introduction, let us briefly review how results over $\mathbb{Q}_p$ can be useful over $\mathbb{Q}$, and then raise some natural questions arising from our main results.

First, recall that the decidability of $\mathbf{FEAS}_{\mathbb{Q}}$ is a major open problem: decidability for the special case of cubic polynomials in two variables would already be enough to yield significant new results in the direction of the 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 $\mathbf{FEAS}_{\mathbb{Z}}$ is undecidable is the famous negative solution of Hilbert's Tenth Problem, due to Matiyasevitch and Davis, Putnam, and Robinson [Mat73, DLPvG00], and is sometimes taken as evidence that $\mathbf{FEAS}_{\mathbb{Q}}$ may be undecidable as well (see also [Poo03]).

From a more positive direction, much work has gone into using p-adic methods to find an algorithm for $\mathbf{FEAS}_{\mathbb{Q}}(\mathbb{Z}[x,y])$ (i.e., deciding the existence of rational points on algebraic curves), via extensions of the **Hasse Principle**[2] (see, e.g., [C-T98, Poo01b, Poo06]).

[2] If $F(x_1,\ldots,x_n)=0$ is any polynomial equation and Z_K is its zero set in K^n, then the Hasse Principle

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], and elliptic curve cryptography [Lau04].

Our results thus provide another step toward understanding the complexity of solving polynomial equations over $\mathbb{Q}_p$, and reveal yet another connection between quantum complexity and number theory. Let us now consider some possible extensions of our results. First, let $\mathbf{FEAS}_{\mathbb{F}_{\text{primes}}}$ denote the obvious finite field analogue of $\mathbf{FEAS}_{\mathbb{Q}_{\text{primes}}}$.

Question 1 *Is* $\mathbf{FEAS}_{\mathbb{F}_{\text{primes}}}(\mathbb{Z}[x_1])$ **NP***-hard?*

Question 2 *Given a prime p and an $f \in \mathbb{F}_p[x_1]$, is it* **NP***-hard to decide whether f is divisible by the square of a degree* 1 *polynomial in $\mathbb{F}_p[x_1]$ (relative to* $\text{size}_p(f)$*)?*

David A. Cox asked the author whether $\mathbf{FEAS}_{\mathbb{F}_{\text{primes}}}(\mathbb{Z}[x_1]) \stackrel{?}{\in} \mathbf{P}$ around August 2004 [Cox04], and Erich Kaltofen posed a variant of Question 1 — $\mathbf{FEAS}_{\mathbb{F}_{\text{primes}}}(\mathcal{U}_3) \stackrel{?}{\in} \mathbf{P}$ — a bit earlier in [Kal03]. Karpinski and Shparlinski raised Question 2 toward the end of [KS99]. Since Hensel's Lemma (cf. Section 2 below) allows one to find roots in $\mathbb{Q}_p$ via computations in the rings $\mathbb{Z}/p^\ell\mathbb{Z}$, the Main Theorem thus provides some evidence toward positive answers for Questions 1 and 2. Note in particular that a positive answer to Question 1 would provide a definitive complexity lower bound for polynomial factorization over $\mathbb{F}_p[x_1]$, since randomized polynomial time algorithms (relative to the **dense** encoding) are already known (e.g., Berlekamp's algorithm [BS96, Sec. 7.4]).

On a more speculative note, one may wonder if quantum computation can produce new speed-ups by circumventing the dependence of certain algorithms on GRH. This is motivated by Hallgren's recent discovery of a **BQP** algorithm for deciding whether the class number of a number field of constant degree is equal to a given integer [Hal05]: The best classical complexity upper bound for the latter problem is $\mathbf{NP} \cap \mathbf{coNP}$, obtainable so far only under the assumption of GRH [BvS89, McC89]. Unfortunately, the precise relation between **BQP** and $\mathbf{NP} \cap \mathbf{coNP}$ is not clear. However, could it be that quantum computation can eliminate the need for GRH in an even more direct way? For instance:

Question 3 *Is there a quantum algorithm which generates, within a number of qubit operations polynomial in n, a prime of the form $kQ_n + 1$ with probability $> \frac{2}{3}$?*

Our main results are proved in Section 3, after the development of some necessary theory in Section 2 below. For the convenience of the reader, we will recall the definitions of all relevant complexity classes and review certain types of Generalized Riemann Hypotheses.

2 Background and Ancillary Results

Recall the containments of complexity classes $\mathbf{P} \subseteq \mathbf{BPP} \subseteq \mathbf{BQP} \subseteq \mathbf{PP} \subseteq \mathbf{PSPACE}$ and $\mathbf{P} \subseteq \mathbf{NP} \cap \mathbf{coNP} \subseteq \mathbf{NP} \cup \mathbf{coNP} \subseteq \mathbf{PP}$, and the fact that the properness of **every** preceding

is the assumption that [$Z_{\mathbb{C}}$ smooth, $Z_{\mathbb{R}} \neq \emptyset$, and $Z_{\mathbb{Q}_p} \neq \emptyset$ for all primes p] $\Longrightarrow Z_{\mathbb{Q}}$ is non-empty as well. The Hasse Principle is a theorem when $Z_{\mathbb{C}}$ is a smooth quadratic hypersurface or a smooth curve of genus zero, but fails in subtle ways already for curves of genus one (see, e.g., [Poo01a]).

containment is a major open problem [Pap95, BV97]. (Indeed, as of early 2007, it is still not known whether even the containment $\mathbf{P} \subseteq \mathbf{PSPACE}$ is proper!) We briefly review the definitions of the aforementioned complexity classes below (see [Pap95, BV97] for a full and rigourous treatment):

P The family of decision problems which can be done within (classical) polynomial-time.

BPP The family of decision problems admitting (classical) randomized polynomial-time algorithms that terminate with an answer that is correct with probability at least[3] $\frac{2}{3}$.

BQP The family of decision problems admitting **quantum** randomized polynomial-time algorithms that terminate with an answer that is correct with probability at least[3] $\frac{2}{3}$ [BV97].

NP The family of decision problems where a ``Yes'' answer can be **certified** within (classical) polynomial-time.

coNP The family of decision problems where a ``No'' answer can be **certified** within (classical) polynomial-time.

PP The family of decision problems admitting (classical) randomized polynomial-time algorithms that terminate with an answer that is correct with probability strictly greater than $\frac{1}{2}$.

PSPACE The family of decision problems solvable within polynomial-time, provided a number of processors exponential in the input size is allowed.

Now recall that **3CNFSAT** is the famous seminal **NP**-complete problem [GJ79] which consists of deciding whether a Boolean sentence of the form $B(X) = C_1(X) \wedge \cdots \wedge C_k(X)$ has a satisfying assignment, where C_i is of one of the following forms:

$$X_i \vee X_j \vee X_k, \;\; \neg X_i \vee X_j \vee X_k, \;\; \neg X_i \vee \neg X_j \vee X_k, \;\; \neg X_i \vee \neg X_j \vee \neg X_k,$$

$i, j, k \in [3n]$, and a satisfying assigment consists of an assigment of values from $\{0, 1\}$ to the variables $X_1, \ldots, X_{3n}$ which makes the equality $B(X) = 1$ true.[4] Each C_i is called a **clause**.

We will need a clever reduction from feasibility testing for univariate polynomial systems over certain fields to **3CNFSAT**. First, note that the nonzero polynomials in $\mathbb{Z}[x_1]$ form a **lattice** [Sta97] with respective to the operations of least common multiple and greatest common divisor.

Definition 3 *Letting Q_n denote the product of the first n primes, let us inductively define a homomorphism $\mathcal{P}_n$ — the* **($n^{\underline{\text{th}}}$) Plaisted morphism** *— from certain Boolean polynomials in the variables $X_1, \ldots, X_n$ to $\mathbb{Z}[x_1]$, as follows: (1) $\mathcal{P}_n(0) := 1$, (2) $\mathcal{P}_n(X_i) := x_1^{Q_n/p_i} - 1$, (3) $\mathcal{P}_n(\neg B) := \frac{x_1^{Q_n} - 1}{\mathcal{P}_n(B)}$, for any Boolean polynomial B for which $\mathcal{P}_n(B)$ has already been defined, (4) $\mathcal{P}_n(B_1 \vee B_2) := \mathrm{lcm}(\mathcal{P}_n(B_1), \mathcal{P}_n(B_2))$, for any Boolean polynomials B_1 and B_2 for which $\mathcal{P}_n(B_1)$ and $\mathcal{P}_n(B_2)$ have already been defined.* $\diamond$

[3] It is easily shown that we can replace $\frac{2}{3}$ by any constant strictly greater than $\frac{1}{2}$ and still obtain the same family of problems [Pap95].

[4] Throughout this paper, for Boolean expressions, we will always identify 0 with ``False'' and 1 with ``True''.

Lemma 1 *For all $n \in \mathbb{N}$ and all clauses $C(X_i, X_j, X_k)$ with $i, j, k \leq n$, we have that $\mathcal{P}_n(C)$ can be computed within time polynomial in n, and $\mathrm{size}(\mathcal{P}_n(C)) = O(n^2)$. Furthermore, if K is any field possessing Q_n distinct Q_n^{th} roots of unity, then a* **3CNFSAT** *instance $B(X) := C_1(X) \wedge \cdots \wedge C_k(X)$ has a satisfying assignment iff the zero set in K of the polynomial system $F_B := (\mathcal{P}_n(C_1), \ldots, \mathcal{P}_n(C_k))$ has a root ζ satisfying $\zeta^{Q_n} - 1$.* ■

David Alan Plaisted proved the special case $K = \mathbb{C}$ of the above lemma in [Pla84]. His proof extends with no difficulty whatsoever to the more general family of fields detailed above. Other than an earlier independent observation of Kaltofen and Koiran [KK05], we are unaware of any other variant of Plaisted's reduction involving a field other than $\mathbb{C}$.

Let us now recall a version of Hensel's Lemma sufficiently general for our proof of our Main Theorem, along with a useful characterization of certain finite rings. Recall that $\mathbb{Z}_p$ denotes the p-adic integers, which can be identified with base-p digit sequences extending infinitely to the left. For any ring R, we also let R^* denote the group of multiplicatively invertible elements of R.

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

Lemma 2 *Given any cyclic group G, $a \in G$, and an integer d, the equation $x^d = a$ has a solution iff the order of a divides $\frac{\#G}{\gcd(d, \#G)}$. In particular, 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 $\ell \geq 3$, $(\mathbb{Z}/2^\ell\mathbb{Z})^* \cong \{-1, 1\} \times \{1, 5, 5^2, 5^3, \ldots, 5^{2^{\ell-2}-1} \bmod 2^\ell\}$.* ■

The last lemma is standard (see, e.g., [BS96, Ch. 5]).

We will also need the following result on an efficient randomized reduction of $\mathbf{FEAS}_K(\mathbb{Z}[x_1]^k)$ to $\mathbf{FEAS}_K(\mathbb{Z}[x_1]^2)$. Recall that $\mathbb{C}_p$ — the p-adic complex numbers — is the metric closure of the algebraic closure of $\mathbb{Q}_p$, and that $\mathbb{C}_p$ is algebraically closed.

Lemma 3 *Suppose $f_1, \ldots, f_k \in \mathbb{Z}[x_1] \setminus \{0\}$ are polynomials of degree $\leq d$, with $k \geq 3$. Also let $Z_K(f_1, \ldots, f_k)$ denote the set of common zeroes of $f_1, \ldots, f_k$ in some field K. Then, if $a = (a_1, \ldots, a_k)$ and $b = (b_1, \ldots, b_k)$ are chosen uniformly randomly from $\{1, \ldots, 18dk^2\}^{2k}$, we have*

$$\mathrm{Prob}\left(Z_K\left(\sum_{i=1}^k a_i f_i, \sum_{i=1}^k b_i f_i\right) = Z_K\left(f_1, \ldots, f_k\right)\right) \geq \tfrac{8}{9}$$

for any $K \in \{\mathbb{C}, \mathbb{C}_p\}$.

While there are certainly earlier results that are more general than Lemma 3 (see, e.g., [GH93, Sec. 3.4.1] or [Koi97, Thm. 5.6]), Lemma 3 is more direct and self-contained for our purposes. For the convenience of the reader, we provide its proof.

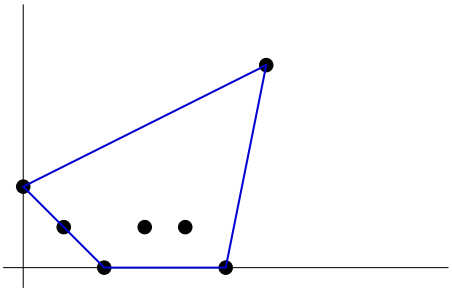
Proof of Lemma 3: Assume $f_i(x) := \sum_{j=0}^d c_{i,j} x^i$ for all $i \in \{1, \ldots, k\}$. Let $W := \left(\bigcup_{i=1}^\ell Z_K(f_i)\right) \setminus Z_K(f_1, \ldots, f_k)$ and $\varphi(u, \zeta) := \sum_{i=1}^k u_i f_i(\zeta)$ for any $\zeta \in W$. Note that $\#W \leq kd$ and that for any fixed $\zeta \in W$, the polynomial $\varphi(u, \zeta)$ is linear in u and not identically zero. By Schwartz's Lemma [Sch80], for any fixed $\zeta \in W$, there are at most kN^{k-1} points $u \in \{1, \ldots, N\}^k$ with $\varphi(u, \zeta) = 0$. So then, there at most dk^2N^{k-1} points $u \in \{1, \ldots, N\}^k$ with $\varphi(u, \zeta) = 0$ for some $\zeta \in W$.

Clearly then, the probability that a uniformly randomly chosen pair $(a,b) \in \{1,\ldots,N\}^{2k}$ satisfies $\varphi(a,\zeta) = \varphi(b,\zeta) = 0$ for some $\zeta \in W$ is bounded above by $\frac{2dk^2}{N}$. So taking $N = 18dk^2$ we are done. ■

Let us also recall the **p-adic Newton polygon**, which allows 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, for any prime p and $x \in \mathbb{Z}_p$, recall that the **p-adic valuation**, $\mathrm{ord}_p x$, is the greatest k such that $p^k | x$. We then extend $\mathrm{ord}_p(\cdot)$ to $\mathbb{Q}_p$ by $\mathrm{ord}_p\left(\frac{a}{b}\right) := \mathrm{ord}_p(a) - \mathrm{ord}_p(b)$ for any $a, b \in \mathbb{Z}_p$, and let $|x|_p := p^{-\mathrm{ord}_p x}$ denote the **p-adic norm**. The norm $|\cdot|_p$ defines a natural metric satisfying the ultrametric inequality and, along with $\mathrm{ord}_p(\cdot)$, extends naturally to the **p-adic complex numbers** $\mathbb{C}_p$ (the metric completion of the algebraic closure of $\mathbb{Q}_p$).

Lemma 4 *(See, e.g., [Rob00].) Given any polynomial $f(x_1) := \sum_{i=1}^m c_i x^{a_i} \in \mathbb{Z}[x_1]$, we define its* **$p$-adic Newton polygon**, $\mathrm{Newt}_p(f)$, *as the convex hull of the points $\{(a_i, \mathrm{ord}_p c_i) \mid i \in \{1,\ldots,m\}\}$. Then the number of roots of f in $\mathbb{C}_p$ with p-adic valuation v is* **exactly** *the horizontal length of the face of $\mathrm{Newt}_p(f)$ with normal $(v,1)$.* ■

Example 1 *For the polynomial $f(x_1) := 243x^6 - 3646x^5 + 18240x^4 - 35310x^3 + 29305x^2 - 8868x + 36$, the polygon $\mathrm{Newt}_3(f)$ can easily be verified to resemble the following illustration:*



Note in particular that there are exactly 3 "lower" edges, and their respective horizontal lengths and inner normals are 2, 3, 1, and $(1,1)$, $(0,1)$, and $(-5,1)$. Lemma 4 then tells us that f has exactly 6 roots in $\mathbb{C}_3$: 2 with 3-adic valuation 1, 3 with 3-adic valuation 0, and 1 with 3-adic valuation -5. Indeed, one can check that the roots of f are exactly 6, 1, and $\frac{1}{243}$, with respective multiplicities 2, 3, and 1. ◇

We now move on to some final background from analytic number theory that we will need.

2.1 Review of Riemann Hypotheses

Primordial versions of the connection between analysis and number theory are not hard to derive from scratch and have been known at least since the 19$^{\underline{\text{th}}}$ century. For example, letting $\zeta(s) := \sum_{n=1}^{\infty} \frac{1}{n^s}$ denote the usual **Riemann zeta function** (for any real number $s > 1$), one can easily derive with a bit of calculus (see, e.g., [TF00, pp. 30–32]) that

$$\zeta(s) = \prod_{p \text{ prime}} \frac{1}{1 - \frac{1}{p^s}}, \text{ and thus } -\frac{\zeta'(s)}{\zeta(s)} = \sum_{n=1}^{\infty} \frac{\Lambda(n)}{n^s},$$

where Λ is the classical Mangoldt function which sends n to $\log p$ or 0, according as $n = p^m$ for some prime p (and some positive integer m) or not. For a deeper connection, recall that $\pi(x)$ denotes the number of primes (in $\mathbb{N}$) $\leq x$ and that the **Prime Number Theorem (PNT)** is the asymptotic formula $\pi(x) \sim \frac{x}{\log x}$ for $x \longrightarrow \infty$. Remarkably then, the first proofs of PNT, by Hadamard and de la Vallée-Poussin (independently, in 1896), were based essentially on the fact that $\zeta(\beta + i\gamma)$ has **no** zeroes on the vertical line $\beta = 1$.[5]

More precisely, writing $\rho = \beta + i\gamma$ for real β and γ, recall that ζ admits an analytic continuation to the complex plane sans the point 1 [TF00, Sec. 2].[6] In particular, the only zeroes of ζ outside the **critical strip** $\{\rho = \beta + i\gamma \mid 0 < \beta < 1\}$ are the so-called **trivial** zeroes $\{-2, -4, -6, \ldots, \}$. Furthermore the zeroes of ζ in the critical strip are symmetric about the **critical line** $\beta = \frac{1}{2}$ and the real axis. The **Riemann Hypothesis (RH)**, from 1859, is then the following assertion:

(RH) All zeroes $\rho = \beta + i\gamma$ of ζ with $\beta > 0$ lie on the critical line $\beta = \frac{1}{2}$.

Among a myriad of hitherto unprovably sharp statements in algorithmic number theory, it is known that RH is true $\iff \left|\pi(x) - \int_2^x \frac{dt}{\log t}\right| = O(\sqrt{x}\log x)$ [TF00]. In particular, RH is widely agreed to be the most important problem in modern mathematics. Since May 24, 2000, RH even enjoys a bounty of one million US dollars thanks to the Clay Mathematics Foundation.

Let us now consider the extension of RH to primes in arithmetic progressions: For any primitive $M^{\underline{\text{th}}}$ root of unity ω_M, define the **(cyclotomic) Dedekind zeta function** via the formula $\zeta_{Q(\omega_M)}(s) := \sum_{\mathfrak{a}} \frac{1}{(\mathcal{N}\mathfrak{a})^s}$, where $\mathfrak{a}$ ranges over all nonzero ideals of $\mathbb{Z}[\omega_M]$ (the ring of algebraic integers in $\mathbb{Q}(\omega_M)$), $\mathcal{N}$ denotes the norm function, and $s > 1$ [BS96]. Then, like ζ, the function $\zeta_{\mathbb{Q}(\omega_M)}$ also admits an analytic continuation to $\mathbb{C}\setminus\{1\}$ (which we'll also call $\zeta_{\mathbb{Q}(\omega_M)}$), $\zeta_{\mathbb{Q}(\omega_M)}$ has trivial zeroes $\{-2, -4, -6, \ldots, \}$, and all other zeroes of $\zeta_{\mathbb{Q}(\omega_M)}$ lie in the critical strip $(0, 1) \times \mathbb{R}$ [LO77]. (The zeroes of $\zeta_{\mathbb{Q}(\omega_M)}$ in the critical strip are also symmetric about the critical line $\frac{1}{2} \times \mathbb{R}$ and the real axis.) We then define the following statement:

($\mathbf{GRH}_{\mathbb{Q}(\omega_M)}$)[7] For any primitive $M^{\underline{\text{th}}}$ root of unity ω_M, all the zeroes $\rho = \beta + i\gamma$ of $\zeta_{\mathbb{Q}(\omega_M)}$ with $\beta > 0$ lie on the critical line $\beta = \frac{1}{2}$.

In particular, letting $\pi(x, M)$ denote the number of primes p congruent to 1 mod M satisfying $p \leq x$, it is known that $\text{GRH}_{\mathbb{Q}(\omega_M)}$ is true $\iff \left|\pi(x, M) - \frac{1}{\varphi(M)} \int_2^x \frac{dt}{\log t}\right| = O\left(\sqrt{x}(\log x + \log M)\right)$, where $\varphi(M)$ is the number of $k \in \{1, \ldots, M-1\}$ relatively prime to M. (This follows routinely from the conditional effective Chebotarev Theorem of [LO77, Thm. 1.1], taking $K = \mathbb{Q}$ and $L = \mathbb{Q}(\omega_M)$ in the notation there. One also needs to recall that the discriminant of $\mathbb{Q}(\omega_M)$ is bounded from above by $M^{\varphi(M)}$ [BS96, Ch. 8, pg. 260].)

From the very last estimate, an elementary calculation shows that FPH is implied by the truth of the hypotheses $\{GRH_{\mathbb{Q}(\omega_{Q_n})}\}_{n\in\mathbb{N}}$. However, we point out that FPH can **still**

[5] Shikau Ikehara later showed in 1931 that PNT is in fact **equivalent** to the fact that ζ has no zeroes on the vertical line $\beta = 1$ (the proof is reproduced in [DMcK72]).

[6] We'll abuse notation henceforth by letting ζ denote the analytic continuation of ζ to $\mathbb{C} \setminus \{1\}$.

[7] There is definitely conflicting notation in the literature as to what the "Extended" Riemann Hypothesis or "Generalized" Riemann Hypothesis are. We thus hope to dissipate any possible confusion via subscripts clearly declaring the field we are working with.

hold even in the presence of infinitely many non-trivial zeta zeroes off the critical line. For instance, if we instead make the weaker assumption that there is an $\varepsilon > 0$ such that all the non-trivial zeroes of $\{\zeta_{\mathbb{Q}(\omega_{Q_n})}\}_{n\in\mathbb{N}}$ have real part $\leq \frac{1}{2} + \varepsilon$, then one can still prove the weaker inequality $\left|\pi(x, M) - \frac{1}{\varphi(M)} \int_2^x \frac{dt}{\log t}\right| = O\left(x^{\frac{1}{2}+\varepsilon}(\log x + \log M)\right)$ (see, e.g., [BGMcI91]). Another elementary calculation then shows that this looser deviation bound **still** suffices to yield FPH. In fact, one can even have non-trivial zeroes of $\zeta_{\mathbb{Q}(\omega_{Q_n})}$ approach the line $\{\beta = 1\}$ arbitrarily closely, provided they do not approach too quickly as a function of n. (See [Roj06] for further details.)

3 The Proofs of Our Main Results

3.1 The Univariate Threshold Over $\mathbb{Q}_p$: Proving the Main Theorem

The first assertion — that $\mathbf{FEAS}_{\mathbb{Q}_{\text{primes}}}(\mathcal{U}_2) \in \mathbf{BQP}$ — rests upon a quantum algorithm for finding the multiplicative order of an element of $(\mathbb{Z}/p^\ell\mathbb{Z})^*$ (see [Sho97, BL95]), once we make a suitable reduction from $\mathbf{FEAS}_{\mathbb{Q}_{\text{primes}}}$. The second assertion — that the larger problem $\mathbf{FEAS}_{\mathbb{Q}_{\text{primes}}}(\mathbb{Z}[x_1])$ lies in $\mathbf{NP}$ — follows from an application of the Newton polygon. The final assertion — that $\mathbf{FEAS}_{\mathbb{Q}_{\text{primes}}}(\mathbb{Z}[x_1])$ is $\mathbf{NP}$-hard under randomized reductions — relies on properties of primes in specially chosen arithmetic progressions, via our generalization (cf. Section 2) of an earlier trick of Plaisted [Pla84].

Before proceeding, we will need a final (elementary) quantitative bound on p-adic roots and Newton polygons, and the computation of sizes/logarithms.

Proposition 1 *For any $f \in \mathbb{Z}[x_1]$ and $\zeta \in \mathbb{Q}_p$, $|\text{ord}_p\zeta| \leq \text{size}(f)$ and $\text{size}(p^{\text{size}(f)}) \leq \text{size}(f)\frac{\log p}{\log 2}$. Also, within time quadratic in $\text{size}(f)$ (resp. $\text{size}_p(f)$), we can compute an integer in the interval $[\text{size}(f), 2\text{size}(f)]$ (resp. $[\text{size}_p(f), 2\text{size}_p(f)]$). Finally, the number of primes for which $\text{ord}_p f'(\zeta) > 0$ for some root $\zeta \in \mathbb{C}_p$ of f is $O(v_f + \deg f \log deg f)$ where v_f is maximum of the base 2 logarithms of the coefficients of f.* ■

In particular, the only non-trivial portion is the final assertion, which follows easily once one applies the classical Hadamard estimates to the product formula for the discriminant of f [GKZ94, Ch. 12].

Proof that $\mathbf{FEAS}_{\mathbb{Q}_{\text{primes}}}(\mathcal{U}_2) \in \mathbf{BQP}$: First note that it clearly suffices to show that we can decide (with error probability $< \frac{1}{3}$, say) whether the polynomial $f(x) := x^d - \alpha$ has a root in $\mathbb{Q}_p$, using a number of qubit operations polynomial in $\text{size}(\alpha) + \log d$. (This is because we can divide by a suitable constant, and arithmetic over $\mathbb{Q}$ is doable in polynomial time.) The case $\alpha = 0$ always results in the root 0, so let us 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 $\mathbf{P}$ [BS96, Ch. 5], we can then clearly assume that $d|\text{ord}_p\alpha$ (for otherwise, there can be no root over $\mathbb{Q}_p$). Moreover, by rescaling x by an appropriate power of p (thanks to Proposition 1) we can assume further that $\text{ord}_p\alpha = 0$.

Now note that $f'(\zeta) = d\zeta^{d-1}$ and thus $\text{ord}_p f'(\zeta) = \text{ord}_p(d)$. 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

$\ell = 1 + 2\mathrm{ord}_p d$. (Note in particular that $\mathrm{size}(p^\ell) = O(\log(p)\log(d))$ which is polynomial in our notion of input size.) By Lemma 2, we can easily decide the latter feasibility problem, given the multiplicative order of α in $(\mathbb{Z}/p^\ell\mathbb{Z})^*$; and we can do the latter in **BQP** by Shor's seminal algorithm for computing order in a cyclic group [Sho97, pp. 1498–1501], provided $p^\ell \notin \{8, 16, 32, \ldots\}$. So the first assertion is proved for $p^\ell \notin \{8, 16, 32, \ldots\}$.

To dispose of the remaining cases $p^\ell \in \{8, 16, 32, \ldots\}$, write $\alpha = (-1)^a 5^b$ and observe that such an expression is unique, by the last part of Lemma 2. The first part of Lemma 2 then easily yields that $x^d - \alpha$ has a root iff

$$(a \text{ odd} \Longrightarrow d \text{ is odd}) \wedge (\text{the order of } 5^b \text{ divides } \tfrac{2^{\ell-2}}{\gcd(d, 2^{\ell-2})}).$$

In particular, we see that $x^d - \alpha$ **always** has a root when d is odd, so we can assume henceforth that d is even.

Letting $\flat$ be the order of 5^b, it is then easy to check that the order of α is either $\flat$ or $2\flat$, according as a is even or odd. Moreover, since d is even, we see that $x^d - \alpha$ can have no roots in $(\mathbb{Z}/2^\ell\mathbb{Z})^*$ when a is odd. So we can now reduce the feasibility of $x^d - \alpha$ to **two** order computations as follows: Compute, now via Boneh and Lipton's quantum algorithm for order computation in Abelian groups [BL95, Thm. 2], the order of α and $-\alpha$. Observe then that a is odd iff the order of α is larger (and then $x^d - \alpha$ has no roots in $(\mathbb{Z}/2^\ell\mathbb{Z})^*$), so we can assume henceforth that α has the smaller order. To conclude, we then declare that $x^d - \alpha$ has a root in $\mathbb{Q}_2$ iff the order of α divides $\frac{2^{\ell-2}}{d}$. This last step is correct, thanks to the first part of Lemma 2, so we at last obtain $\mathbf{FEAS}_{\mathbb{Q}_{\mathrm{primes}}}(\mathcal{U}_2) \in \mathbf{BQP}$. ■

Proof that $\mathbf{FEAS}_{\mathbb{Q}_{\mathrm{primes}}}(\mathbb{Z}[x_1]) \in \mathbf{NP}$ for "most" inputs: First note that detecting the existence of 0 as a root of f is easily done in linear time, simply by checking whether all exponents are positive. Furthermore, by Proposition 1, we can rescale x_1 (inducing at worst quadratic growth in $\mathrm{size}_p(f)$) so that all the roots of f in $\mathbb{Q}_p$ lie in $\mathbb{Z}_p$.

So let us assume without loss of generality that $x_1 \not| f$ and that all the roots of $\mathbb{Q}_p$ lie in $\mathbb{Z}_p$, and proceed to define the following succinct certificate for $\mathbf{FEAS}_{\mathbb{Q}_{\mathrm{primes}}}(\mathbb{Z}[x_1])$: any pair of the form $(v, \zeta) \in \mathbb{Z} \times (\mathbb{Z}/p^k\mathbb{Z})$ with k a fixed positive integer, ζ a root of f over $\mathbb{Z}/p^k\mathbb{Z}$ and $(v, 1)$ an inner edge normal of $\mathrm{Newt}_p(f)$. Since verifying the desired properties for (v, ζ) is clearly doable within time polynomial in $\mathrm{size}_p(f)$, thanks to our earlier algorithmic observations on $\mathbf{FEAS}_{\mathbb{Q}_{\mathrm{primes}}}(\mathcal{U}_2)$, we now need only show that f has a root in $\mathbb{Q}_p$ iff such a certificate exists.

If f indeed has a root $\zeta \in \mathbb{Q}_p$ then $\mathrm{ord}_p\zeta$ is a positive integer and f has a root $\bar{\zeta} \in \mathbb{Z}/p^k\mathbb{Z}$ with $\zeta \equiv \bar{\zeta} (\mathrm{mod} p^k)$ for **all** $k \geq 1$. So our stated certificate exists when f has a root in $\mathbb{Q}_p$.

To see the converse, assume momentarily that $\mathrm{ord}_p f'(\zeta) \leq (k-1)/2$ for all roots $\zeta \in \mathbb{C}_p$ of f. Then, given a certificate as stated above, Hensel's Lemma immediately implies that f has a root in $\mathbb{Q}_p$. The case where $\mathrm{ord}_p f'(\zeta)$ is large for all roots of $\mathbb{Q}_p$ thus presents a difficulty, but Proposition 1 immediately implies that if simply consider primes with $\log O(v_f + \deg f \log(\deg f))$ digits, we can in fact assume that $\mathrm{ord}_p f'(\zeta) = 0$ for all but a vanishingly small fraction of p. Since $\log(v_f + \deg f) = O(\mathrm{size}(f))$, we immediately obtain our desired assertion. ■

Proof that $\mathbf{FEAS}_{\mathbb{Q}_{\mathrm{primes}}}(\mathbb{Z}[x_1])$ is NP-hard Under Randomized Reductions: First note that $\mathrm{size}(Q_n) = O(n \log n)$, via the Prime Number Theorem. Observe then that the truth of FPH implies that we can efficiently find a prime p of the form $kQ_n + 1$, with $k \in \{1, \ldots, 2^{n^C}\}$, via random sampling, as follows: Pick a uniformly randomly integer from

$\{1, \ldots, 2^{n^C}\}$ and using, say, the famous polynomial-time AKS primality testing algorithm [AKS02], verify whether $kQ_n + 1$ is prime. We repeat this until we either find a prime, or fail $9n$ consecutive times.

Via the elementary estimate $(1 - \frac{1}{B})^{Bt} < \frac{1}{t}$, valid for all $B, t > 1$, we then easily obtain that our method results in a prime with probability at least $\frac{8}{9}$. Since $\mathrm{size}(1 + 2^{n^C} Q_n) = O(\log(2^{n^C} Q_n)) = O(n^C + n \log n)$, it is clear that our simple algorithm requires a number of bit operations just polynomial in n. Moreover, the number of random bits needed is clearly $O(n^C)$.

Having now probabilistically generated a prime $p = 1 + kQ_n$, Lemma 1 then immediately yields the implication "$\mathbf{FEAS}_{\mathbb{Q}_{\mathrm{primes}}}(\mathcal{US}) \in \mathcal{C} \implies \mathbf{NP} \in \mathcal{C} \cup \mathbf{BPP}$," where $\mathcal{US} := \{(f_1, \ldots, f_k) \mid f_i \in \mathbb{Z}[x_1] \ , \ k \in \mathbb{N}\}$: Indeed, if $\mathbf{FEAS}_{\mathbb{Q}_{\mathrm{primes}}}(\mathcal{US}) \in \mathcal{C}$ for some complexity class $\mathcal{C}$, then we could combine our hypothetical $\mathcal{C}$ algorithm for $\mathbf{FEAS}_{\mathbb{Q}_{\mathrm{primes}}}(\mathcal{US})$ with our randomized prime generation routine (and the Plaisted morphism for $K = \mathbb{Q}_p$) to obtain an algorithm with complexity in $\mathcal{C} \cup \mathbf{BPP}$ for any **3CNFSAT** instance.

So now we need only show that this hardness persists if we reduce $\mathcal{US}$ to systems consisting of just one univariate sparse polynomial. Clearly, we can at least reduce to pairs of polynomials via Lemma 3, so now we need only reduce from pairs to singletons.

Toward this end, suppose $a \in \mathbb{Z}$ is a non-square mod p and p is odd. Clearly then, the only root in $\mathbb{F}_p$ of (the mod p reduction of) the quadratic form $q(x, y) := x^2 - ay^2$ is $(0, 0)$. Furthermore, by considering the valuations of x and y, it is also easily checked that the only root of q in $\mathbb{Q}_p$ is $(0, 0)$. Thus, given any $(f, g) \in \mathbb{Z}[x_1]^2$, we can form $q(f, g)$ (which has size $O(\mathrm{size}(f) + \mathrm{size}(g) + \mathrm{size}(p))$) to obtain a polynomial time reduction of $\mathbf{FEAS}_{\mathbb{Q}_{\mathrm{primes}}}(\mathbb{Z}[x_1]^2)$ to $\mathbf{FEAS}_{\mathbb{Q}_{\mathrm{primes}}}(\mathbb{Z}[x_1])$, assuming we can find a quadratic non-residue efficiently. (If $p = 2$ then we can simply use $q(x, y) := x^2 + xy + y^2$ and then there is no need at all for a quadratic non-residue.) However, this can easily be done by picking two random $a \in \mathbb{F}_p$: With probability at least $\frac{3}{4}$, at least one of these numbers will be a quadratic non-residue (and this can be checked in $\mathbf{P}$ by computing $a^{(p-1)/2}$ via recursive squaring). So we are done. ■

3.2 Detecting Square-Freeness: Proving Corollary 1

Given any $f \in \mathbb{Z}[x_1]$, observe that f has a root in $\mathbb{Q}_p$ iff f^2 is divisible by the square of a degree 1 polynomial in $\mathbb{Q}_p[x_1]$. Moreover, since $\mathrm{size}(f^2) = O(\mathrm{size}(f)^2)$, we thus obtain a polynomial-time reduction of the problem considered by Corollary 1 to $\mathbf{FEAS}_{\mathbb{Q}_{\mathrm{primes}}}(\mathbb{Z}[x_1])$. So we are done. ■

Acknowledgements

The author thanks Leonid Gurvits, Erich Kaltofen, and David Alan Plaisted for their kind encouragement. In particular, Leonid Gurvits, Sean Hallgren, and Erich Kaltofen respectively pointed out the references [FKW02], [KL99], and [KK05]. I also thank Dan J. Bernstein, Jan Denef, Sidney W. Graham, Sean Hallgren, and Igor Shparlinski for some useful conversations and e-mails during the conception of this work.

Special thanks to Mark Danny Rintoul III, Sean Hallgren, Bernie Shiffman, and Steve

Zelditch for their warm hospitality during visits to Sandia National Laboratories, NEC Laboratories, and Johns Hopkins University, where this work was completed.

Note Added in Proof: *In recent joint work with Sean Hallgren and Bjorn Poonen, the author has extended the Main Theorem to finite fields with a prime number of elements. Also, it appears that the assumption of FPT can be removed over p-adic fields, but not yet over finite fields.* $\diamond$

References

[AKS02] Agrawal, Manindra; Kayal, Neeraj; and Saxena, Nitin, *"PRIMES is in P,"* submitted for publication, downloadable from `http://www.cse.iitk.ac.in/news/primality.html`

[AJL05] Aharonov, Dorit; Jones, Vaughan; and Landau, Zeph, *"A Polynomial Quantum Algorithm for Approximating the Jones Polynomial,"* Math ArXiV preprint `quant-ph/0511096` .

[AA06] Aharonov, Dorit and Arad, Itai, *"The* **BQP***-Hardness of Approximating the Jones Polynomial,"* Math ArXiV preprint `quant-ph/0605181` .

[BS96] Bach, Eric and Shallit, Jeff, *Algorithmic Number Theory, Vol. I: Efficient Algorithms,* MIT Press, Cambridge, MA, 1996.

[BGMcI91] Bach, Eric; Giesbrecht, Mark; and McInnes, *"The complexity of number theoretic problems,"* Technical Report No. 247/91, Dept. Computer Science, Univ. Toronto, January 1991.

[BV97] Bernstein, Ethan and Vazirani, Umesh, *"Quantum Complexity Theory,"* SIAM Journal of Computation **26**, no. 5, pp. 1411–1473, October, 1997.

[BL95] Boneh, Dan and Lipton, Richard J., *"Quantum Cryptanalysis of Hidden Linear Functions,"* Advances in cryptology — CRYPTO '95 (Santa Barbara, CA, 1995), pp. 424–437, Lecture Notes in Comput. Sci., 963, Springer, Berlin, 1995.

[BvS89] Buchmann, J. and Williams, H. C., *"On the existence of a short proof for the value of the class number and regulator of a real quadratic field,"* NATO Advanced Science Institutes Series C, Vol. 256, Kluwer, Dordrecht (1989), pp. 327–345.

[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.

[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 Alan, *personal communication via e-mail*, August 2004.

[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.

[DMcK72] Dym, H. and McKean, H. P., *Fourier Series and Integrals,* Probability and Mathematical Statistics, vol. 14, Academic Press, 1972.

[FKW02] Freedman, Michael; Kitaev, Alexander; and Wang, Z., *"Simulation of Topological Field Theories by Quantum Computers,"* Commun. Math. Phys. **227** (2002), pp. 587–603.

[FLW02] Freedman, Michael; Larsen, Michael; and Wang, Z., *"A Modular Functor which is Universal for Quantum Computation,"* Commun. Math. Phys. **227** (2002), no. 3, pp. 605–622.

[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, x+338 pp.

[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.

[Hal05] Hallgren, Sean, *"Fast quantum algorithms for computing the unit group and class group of a number field,"* STOC'05: Proceedings of the 37th Annual ACM Symposium on Theory of Computing, pp. 468–474, ACM, New York, 2005.

[HS00] Hindry, Marc and Silverman, Joseph H., *Introduction to Diophantine Geometry,* Graduate Texts in Mathematics, vol. 201, Springer-Verlag, 2000.

[IW97] Impagliazzo, Russell and Wigderson, Avi, "**P** = **BPP** if **EXPTIME** Requires Exponential Circuits: Derandomizing the XOR Lemma," STOC '97 (El Paso, TX), pp. 220–229, ACM, New York, 1999.

[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.

[KS99] 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.

[KK05] Kaltofen, Erich and Koiran, Pascal, *"Finding small degree factors of multivariate supersparse (Lacunary) Polynomials over algebraic number fields,"* in ISSAC '06, Proc. 2006 Internat. Symp. Symbolic Algebraic Comput., to appear, ACM Press.

[Koi97] Koiran, Pascal, *"Randomized and Deterministic Algorithms for the Dimension of Algebraic Varieties,"* Proceedings of the $38^{\underline{\text{th}}}$ Annual IEEE Computer Society Conference on Foundations of Computer Science (FOCS), Oct. 20–22, 1997, ACM Press.

[KL99] Knill, Emanuel and Laflamme, Raymond, *"Quantum Computation and Quadratically Signed Weight Enumerators,"* Math ArXiV preprint `quant-ph/9909094` .

[LO77] Lagarias, Jeff and Odlyzko, Andrew, *"Effective Versions of the Chebotarev Density Theorem,"* Algebraic Number Fields: L-functions and Galois Properties (Proc. Sympos. Univ. Durham, Durham, 1975), 409–464, Academic Press, London, 1977.

[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-Kóscielisko, 1997), pp. 267–276, de Gruyter, Berlin, 1999.

[LLL82] Lenstra, Arjen K.; Lenstra, Hendrik W., Jr.; Lovász, L., *"Factoring polynomials with rational coefficients,"* Math. Ann. 261 (1982), no. 4, pp. 515–534.

[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.

[McC89] McCurley, Kevin S., *"Short Cryptographic key distribution and computation in class groups,"* NATO Advanced Science Institutes Series C, Vol. 256, Kluwer, Dordrecht (1989), pp. 459–479.

[Mih94] Mihailescu, Preda, *"Fast generation of provable primes using search in arithmetic progressions,"* Advances in cryptology — CRYPTO '94 (Santa Barbara, CA, 1994), pp. 282–293, Lecture Notes in Comput. Sci., 839, Springer, Berlin, 1994.

[Mil76] Miller, Gary L., *"Riemann's Hypothesis and Tests for Primality,"* J. Comput. System Sci. **13** (1976), no. 3, 300–317.

[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.

[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, to appear. Also available as Math ArXiV preprint `math.NT/0507329` .

[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.

[Roj06] _____, *"Dedekind Zeta Functions and the Complexity of Computing Complex Dimension"*, preprint.

[Sch80] Schwartz, Jacob T., *"Fast Probabilistic Algorithms for Verification of Polynomial Identities,"* J. of the ACM 27, 701–717, 1980.

[Sho97] Shor, Peter W., *"Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer,"* SIAM J. Comput. 26 (1997), no. 5, pp. 1484–1509.

[Sil96] Silverman, Joseph H., *The Arithmetic of Elliptic Curves,* Graduate Texts in Mathematics, vol. 106, Springer-Verlag, 1996.

[Sta97] Stanley, Richard, *Enumerative combinatorics,* Vol. 1. with a foreword by Gian-Carlo Rota, corrected reprint of the 1986 original, Cambridge Studies in Advanced Mathematics, 49, Cambridge University Press, Cambridge, 1997.

[TF00] Tenenbaum, Gérald and Mendès France, Michel, *The Prime Numbers and Their Distribution,* Student Mathematical Library, vol. 6, AMS Press, Rhode Island, 2000.

[YW06] Yard, Jon and Wocjan, Pawel, *"The Jones Polynomial: Quantum Algorithms and Applications in Quantum Complexity Theory,"* Math ArXiV preprint `quant-ph/0603069`.