# A quantum algorithm for computing the unit group of an arbitrary degree number field*

Kirsten Eisenträger†, Sean Hallgren‡, Alexei Kitaev§, Fang Song¶

**Abstract**

Computing the group of units in a field of algebraic numbers is one of the central tasks of computational algebraic number theory. It is believed to be hard classically, which is of interest for cryptography. In the quantum setting, efficient algorithms were previously known for fields of constant degree. We give a quantum algorithm that is polynomial in the degree of the field and the logarithm of its discriminant. This is achieved by combining three new results. The first is a classical algorithm for computing a basis for certain ideal lattices with doubly exponentially large generators. The second shows that a Gaussian-weighted superposition of lattice points, with an appropriate encoding, can be used to provide a unique representation of a real-valued lattice. The third is an extension of the hidden subgroup problem to continuous groups and a quantum algorithm for solving the HSP over the group $\mathbb{R}^n$.

The problems where quantum algorithms have exponential speedups over the best known classical algorithm have mostly been of number theoretic origin. Shor found quantum algorithms for factoring and discrete log [Sho97] and Hallgren found a quantum algorithm for solving Pell's equation [Hal07]. These algorithms were further generalized to finding the unit group of a number field [Hal05, SV05], solving the principal ideal problem, and computing the class group [Hal05]. These are three of the main problems in computational algebraic number theory [Coh93]. The running time for these problems is measured in terms of the discriminant and the degree of the number field. The degree of a number field is its dimension as a vector space over $\mathbb{Q}$, while the discriminant is related to the volume of the fundamental domain of the ring of integers. The algorithms in [Hal05, SV05] are only efficient for constant degree number fields. In this paper we address the arbitrary degree case and give an algorithm that is efficient in both the discriminant and the degree.

In the context of cryptography, the problem of computing the unit group and solving the principal ideal problem (PIP) are considered to be hard classically, even over degree two number fields. The hardness of the PIP was used as a basis in the Buchmann-Williams key exchange problem in an effort to find a system that is harder to break than factoring-based systems [SBW94]. Given our new algorithm for the unit group, it is conceivable that it will be possible to solve the PIP and also compute the class group in a way similar to the constant degree case, but this is an open question. Solving the PIP could have implications for some of the cryptosystems that have been proposed recently.

*Appeared in *Proceedings of the 46th Annual Symposium on Theory of Computing (STOC)*, 2014.

†Department of Mathematics, The Pennsylvania State University, eisentra@math.psu.edu. Partially supported by National Science Foundation grant DMS-1056703 and by the National Security Agency (NSA) under Army Research Office (ARO) contract number W911NF-12-1-0522. Part of this work was done while visiting Harvard University and MIT.

‡Department Computer Science and Engineering, The Pennsylvania State University, hallgren@cse.psu.edu. Partially supported by National Science Foundation awards CCF-0747274 and CCF-1218721, and by the National Security Agency (NSA) under Army Research Office (ARO) contract number W911NF-12-1-0522. Part of this work was done while visiting MIT.

§California Institute of Technology and Kavli Institute for Theoretical Physics, kitaev@caltech.edu. Funding from NSF grant PHY11-25915, NSA/ARO grant W911NF-09-1-0442, and by the Institute for Quantum Information and Matter, an NSF Physics Frontiers Center with support of the Gordon and Betty Moore Foundation.

¶Department of C&O, and Institute for Quantum Computing, University of Waterloo, fang.song@uwaterloo.ca. Supported in part by grants from NSERC, CIFAR, ORF and Industry Canada.

In the last few years, since the discovery of homomorphic encryption [Gen09] and the ensuing efforts to make the systems more efficient and more secure, constructions using number fields have been given. These systems use hardness assumptions about computational problems in arbitrary degree number fields. In [GH11], a version of the principal ideal problem where a special generator is the secret was used as the hardness assumption. The Ring-LWE problem which forms the basis in [LPR10, BV11] assumes that finding short vectors in ideal lattices of arbitrary degree number fields is hard. It is open whether or not these relatively new assumptions about problems in number fields of arbitrary degree are hard for quantum computers, but it is conceivable that the extra algebraic structure of the fields will make it possible to efficiently solve these problems. Bernstein [Ber14] outlines the beginning of an approach, where the first step would be to use heuristics to (classically) compute the unit group in subexponential time. Our new algorithm given in this paper is the first quantum algorithm for problems of this type in number fields of arbitrary degree. It may move us closer to understanding whether the new homomorphic cryptosystems really are secure against quantum computers.

**The problem.** A number field $K$ can be defined as a subfield of the complex numbers $\mathbb{C}$ which is generated over the rational numbers $\mathbb{Q}$ by an algebraic number, i.e. $K = \mathbb{Q}(\theta)$, where $\theta$ is the root of a polynomial with rational coefficients. If $K$ is a number field, then the subset of $K$ consisting of all elements that are roots of monic polynomials with integer coefficients, forms a ring $\mathcal{O}$, called the ring of integers of $K$. The ring $\mathcal{O} \subseteq K$ can be thought of as a generalization of $\mathbb{Z} \subset \mathbb{Q}$. In particular, we can ask whether $\mathcal{O}$ is a principal ideal domain, whether elements of $\mathcal{O}$ have unique factorization, and what the set of invertible elements is. The unit group $\mathcal{O}^*$ is the set of invertible algebraic integers inside $K$, that is, elements $\alpha \in \mathcal{O}$ such that $\alpha^{-1} \in \mathcal{O}$.

An elementary version of the problem is Pell's equation: given a positive non-square integer $d$, find $x$ and $y$ such that $x^2 - dy^2 = 1$. Solutions to this equation are parametrized by the formula $x_k + y_k\sqrt{d} = \left(x_1 + y_1\sqrt{d}\right)^k$; the numbers $\pm\left(x_k + y_k\sqrt{d}\right)$ are exactly the units of the quadratic ring $\mathbb{Z}\left[\sqrt{d}\right]$ (or a subgroup of index 2 if there is a unit that has norm $-1$). The fundamental solution $(x_1, y_1)$ is difficult to find, or even to write down because it may be exponential in $d$ (i.e., doubly-exponential). Moreover, the computation of the real number $R = \ln\left(x_1 + y_1\sqrt{d}\right)$ with a polynomial number of precision digits is believed to be a hard problem classically.

A polynomial time quantum algorithm for the computation of $R$ was given in [Hal07]. The approach is to reduce the problem to a hidden subgroup problem (HSP) over the real numbers $\mathbb{R}$, and then to give a quantum algorithm for that hidden subgroup problem. In this context, the HSP amounts to having a periodic function on $\mathbb{R}$ which is 1-1 within the period. The goal is to approximate the period. In [Hal07] these issues were addressed by using an intricate notion of "reduced ideals". This method was extended to constant degree number fields [Hal05, SV05], but it is difficult to generalize this method to rings of higher degree. At a minimum, computing the necessary reduced ideals seems to require solving the shortest vector problem in ideal lattices of dimension $n$, and enumerating lattice points also seems necessary. These problems are believed to be computationally difficult. Another problem is running the standard hidden subgroup algorithm for the continuous group $G = \mathbb{R}^m$, where rounding causes errors. Such errors are tolerable when $m$ is fixed, but worsen in higher dimensions.

**The reduction.** We propose a different scheme, leading to a quantum reduction from computing the unit group of a number field of arbitrary degree $n$ to solving an Abelian hidden subgroup problem over $\mathbb{R}^m$, where $m = O(n)$. It involves several important ingredients. First, we represent a lattice by a reduced basis (up to some precision). The HSP function works by performing a doubly-exponential scaling function on a base lattice, which is the ring of integers $\mathcal{O}$ embedded into $\mathbb{R}^m$. The output is a new lattice $L$. This transformation is performed using repeated squaring of lattices and computing LLL-reduced bases after each multiplication to keep the basis size from growing too large. These lattices have the extra property that they can be multiplied because they are also ideals. Having

obtained some basis of the lattice $L$, we construct a canonical *quantum representation* of $L$, namely the Gaussian-weighted superposition of lattice points with a sufficiently large dispersion. To ensure stability against rounding errors, each lattice point is represented by a superposition of nearby points in a fine grid. (For example, in one dimension, such a superposition straddles two adjacent grid points.) In addition to showing how to classically compute approximate bases for the stretched lattices, we prove that the inner product of Gaussian lattice states has a hidden subgroup property.

**Theorem 1.** *There is a reduction from computing the unit group of a number field to a continuous hidden subgroup problem over $\mathbb{R}^m$ running in time polynomial in the degree $m$ and log discriminant.*

**The HSP Algorithm.** One byproduct of this work is a generalization of the HSP to uncountable topological groups such as $\mathbb{R}$. Most exponential speedups by quantum algorithms either use or try to use the HSP [FIM$^+$03, HMR$^+$10]. In the HSP a function $f : G \to S$ is given on a group $G$ to some set $S$. For an unknown subgroup $H \subseteq G$, the function is constant on cosets of $H$ and distinct on different cosets. The goal is to find a set of generators for $H$ in time polynomial in the appropriate input size, e.g. $\log |G|$. When $G$ is finite Abelian or $\mathbb{Z}^m$ there is an efficient quantum algorithm to solve the problem.

Using the usual definition of the HSP for the group $G = \mathbb{R}$ does not work as can be seen by the following illustration. When the group is discrete the function can be evaluated on any group element. For example, it is possible to verify that a given element $h$ is in $H$, by testing if $g(0) = g(h)$. Over the reals, if the period is some transcendental number $x$, then no algorithm could ever even query $g(x)$, and then see that it matches $g(0)$. It is possible to address this by giving an ad-hoc technical definition if we replace $\mathbb{R}$ by a discrete set with rounding, as in the case of constant degree number fields [Hal07, Hal05, SV05]. However, it is not known how to solve the HSP with such a definition. Here we give a cleaner definition using continuous functions:

**Definition (The continuous HSP over $\mathbb{R}^m$).** *The unknown subgroup $L \subseteq \mathbb{R}^m$ is a full-rank lattice satisfying some promise: the norm of the shortest vector is at least $\lambda$ and the unit cell volume is at most $d$. The oracle has parameters $(a, r, \varepsilon)$. Let $f : \mathbb{R}^m \to S$ be a function, where $S$ is the set of unit vectors in some Hilbert space. We assume that $f$ hides $L$ in the following way.*

1. *$f$ is periodic on $L$: for all $v \in L$, $x \in \mathbb{R}^m$, $f(x) = f(x + v)$;*
2. *$\big\||f(x)\rangle - |f(y)\rangle\big\| \leqslant a \cdot \mathrm{dist}(x, y)$ for all $x, y \in \mathbb{R}^m$ (Lipschitz);*
3. *If $\min_{v \in L} \|x - y - v\| \geqslant r$, then $\big|\langle f(x)|f(y)\rangle\big| \leqslant \varepsilon$.*

*Given an efficiently computable function with this property, compute a basis for $L$.*

This definition has several new features. One is that in order to have a continuous function, the range of the HSP function consists of quantum states instead of just classical strings. Property (3) mimics the condition that the function is distinct on different cosets in an approximate way. The Lipschitz condition solves the issue with transcendental numbers described above because $f(x)$ and $f(x + \varepsilon)$ return nearly identical quantum states.

One new feature of the algorithm is that the rounding is done at the very end. Previously the function was rounded in an ad-hoc way which prevented an analysis of how the errors would behave under high-dimensional Fourier transforms. Now the analysis is done in a continuous space (think of continuous quantum states) using generalized functions. With this approach there is a well defined Fourier transform, the Lipschitz property allows the Fourier maximum coefficients to be bounded, and then we can round at the very end for the algorithm.

**Theorem 2.** *There is an efficient quantum algorithm solving the continuous HSP over $\mathbb{R}^m$.*

We also give a quantum reduction from all previous abelian HSP instances to this continuous case. Our algorithm therefore subsumes all previously known abelian HSP cases.

## References


[Ber14] D. J. Bernstein. A subfield-logarithm attack against ideal lattices, 2014. The cr.yp.to blog, http://blog.cr.yp.to/20140213-ideal.html.

[BV11] Zvika Brakerski and Vinod Vaikuntanathan. Fully homomorphic encryption from ring-LWE and security for key dependent messages. In *Advances in cryptology—CRYPTO 2011*, volume 6841 of *LNCS*, pages 505–524. Springer, 2011.

[Coh93] Henri Cohen. *A course in computational algebraic number theory*. Springer-Verlag New York, Inc., New York, NY, USA, 1993.

[FIM+03] Katalin Friedl, Gabor Ivanyos, Frederic Magniez, Miklos Santha, and Pranab Sen. Hidden translation and orbit coset in quantum computing. In *Proceedings of the Thirty-Fifth Annual ACM Symposium on Theory of Computing*, San Diego, CA, 9–11June 2003.

[Gen09] Craig Gentry. Fully homomorphic encryption using ideal lattices. In *STOC '09: Proceedings of the 41st annual ACM symposium on Theory of computing*, pages 169–178, New York, NY, USA, 2009. ACM.

[GH11] C. Gentry and S. Halevi. Implementing gentry's fully-homomorphic encryption scheme. *Eurocrypt 2011*, pages 132–150, 2011.

[Hal05] Sean Hallgren. Fast quantum algorithms for computing the unit group and class group of a number field. In *Proceedings of the 37th Annual ACM Symposium on Theory of Computing*, pages 468–474, 2005.

[Hal07] Sean Hallgren. Polynomial-time quantum algorithms for Pell's equation and the principal ideal problem. *Journal of the ACM*, 54(1):1–19, 2007.

[HMR+10] Sean Hallgren, Cristopher Moore, Martin Rötteler, Alexander Russell, and Pranab Sen. Limitations of quantum coset states for graph isomorphism. *J. ACM*, 57:34:1–34:33, November 2010.

[LPR10] Vadim Lyubashevsky, Chris Peikert, and Oded Regev. On ideal lattices and learning with errors over rings. In *Advances in cryptology—EUROCRYPT 2010*, volume 6110 of *LNCS*, pages 1–23. Springer, 2010.

[SBW94] Renate Scheidler, Johannes A Buchmann, and Hugh C Williams. A key-exchange protocol using real quadratic fields. *Journal of Cryptology*, 7(3):171–199, 1994.

[Sho97] Peter W. Shor. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Journal on Computing*, 26(5):1484–1509, 1997.

[SV05] Arthur Schmidt and Ulrich Vollmer. Polynomial time quantum algorithm for the computation of the unit group of a number field. In *Proceedings of the 37th Annual ACM Symposium on Theory of Computing*, pages 475–480, 2005.