Polynomial Time Reduction from Approximate Shortest Vector Problem to Principal Ideal Problem for Lattices in Some Cyclotomic Rings

Hao Chen *

November 16, 2015

Abstract

Many cryptographic schemes have been established based on the hardness of lattice problems. For the asymptotic efficiency, ideal lattices in the ring of cyclotomic integers are suggested to be used in most such schemes. On the other hand in computational algebraic number theory one of the main problem is the principal ideal problem (PIP). Its goal is to find a generator of any principal ideal in the ring of algebraic integers in any number field. In this paper we give a polynomial time reduction from approximate shortest lattice vector problem for principal ideal lattices to their PIP's in cyclotomic integer rings of extension degrees $\phi(n) = 2^{k-1}, k = 2, 3, \ldots$. Thus if a polynomial time quantum algorithm for PIP of arbitrary number fields could be proposed, this would implies that approximate SVP problem for principal ideal lattices within a polynomial factor in this kind cyclotomic integer rings can be solved by a polynomial time quantum algorithm.

1 Introduction

A lattice $\mathbf{L}$ is a discrete subgroup in $\mathbf{R}^n$ generated by several linear independent vectors $\mathbf{b}_1, \ldots, \mathbf{b}_m$ over the ring of integers, where $m \leq n$ $\mathbf{L} := \{a_1\mathbf{b}_1 + \cdots + a_m\mathbf{b}_m : a_1 \in \mathbf{Z}, \ldots, a_m \in \mathbf{Z}\}$. The volume $vol(\mathbf{L})$ of this lattice is $\sqrt{det(\mathbf{B} \cdot \mathbf{B}^\tau)}$, where $\mathbf{B} := (b_{ij})$ is the $m \times n$ generator matrix of

*Hao Chen is with the Department of Mathematics, School of Sciences, Hangzhou Dianzi University, Hangzhou, Zhejiang Province, 310018, China, haochen@hdu.edu.cn.
This research is supported by NSFC Grants 11371138 and 11531002.

this lattice, where $\mathbf{b}_i = (b_{i1}, \ldots, b_{in}) \in \mathbf{R}^n$, $i = 1, \cdots, m$, are the base of this lattice. The length of the shortest non-zero lattice vector is denoted by $\lambda_1(\mathbf{L})$. The famous shortest vector problem (SVP) is: given a $\mathbf{Z}$ basis of an arbitrary lattice $\mathbf{L}$ to find a lattice vector with length $\lambda_1(\mathbf{L})$. The approximate SVP is to find some lattice vectors of length within $f(n)\lambda_1(\mathbf{L})$ where $f(n)$ is some approximate factor ([18]). A breakthrough result of M. Ajtai [1] showed that SVP is NP-hard under the randomized reduction. Another breakthrough by Micciancio proved that approximate SVP within some constant factor is NP-hard under the randomized reduction ([17]). For the latest development we refer to Khot [14]. It has been proved that approximate SVP within a quasi-polynomial factor is NP-hard under the randomized reduction.

Because lattice-based cryptography has been very active in recent years, some spacial structured lattices such as ideal lattices have been used for example in Gentry's fully homomorphic encryption scheme [11], collision-resistant hash functions [19] and multi-linear maps [12]. In particular principal ideal lattices in cyclotomic integer rings have been considered suitable for efficient implementation. Lattice based cryptography has been considered suitable for post-quantum cryptography because of the belief that there is no polynomial time quantum algorithm for approximate SVP problem (conjecture 1.2 in [19] and [11, 12, 15, 16, 18, 21, 22]).

Let ξ_n be a primitive n-th root of unity, the n-th cyclotomic polynomial Φ_n is defined as $\prod_{j=1,gcd(j,n)=1}^{n}(x - \xi_n^j)$. This is a monic irreducible polynomial in $\mathbf{Z}[x]$ of degree $\phi(n)$, where ϕ is the Euler function. The n-th cyclotomic field is $Q(\xi_n) = \mathbf{Q}[x]/(\Phi_n(x))$ and the ring of integers in $\mathbf{Q}(\xi_n)$ is exactly $\mathbf{Z}[\xi_n] = \mathbf{Z}[x]/(\Phi_n(x))$ (see [8, 23]). For example when $n = 2^k$, the n-th cyclotomic polynomial is $\Phi_{2^k}(x) = x^{2^{k-1}} + 1$. When $n = p$ is an odd prime $\Phi_p(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$ and when $n = p^k$, $\Phi_{p^k}(x) = \Phi_p(x^{p^{k-1}}) = (x^{p^{k-1}})^{p-1} + \cdots + x^{p^{k-1}} + 1$. Interestingly there have been many works on the forms of cyclotomic polynomials (see [20, 23]).

Let K be an algebraic number field and $\mathbf{O}_K$ is its ring of integers, it is well-known there is a positive definite inner product on the lattice $\mathbf{O}_K$ defined by $< u, v >= tr_{K/Q}(uv^*)$ where v^* is its complex conjugate (see [8, 15]). Sometimes we use $||u||_{tr}$ to represent $tr_{K/Q}(uu^*)^{1/2}$. Generally $|| \cdot ||$ is the ordinary Euclidean norm of coordinates with respect to some base and $< u, v >_{Euclid}$ is the ordinary Euclidean inner product.

For an ideal $\mathbf{I} \subset \mathbf{O}_K$ if we can find one generator $\mathbf{g}$, this ideal is called a principal ideal generated by $\mathbf{g}$. The following principal ideal problem is one of the main problems in computational algebraic number theory.

Principal Ideal Problem. Given a $\mathbf{Z}$-basis of a principle ideal $\mathbf{I}$, find one generator of this principal ideal.

In this paper we will show the following result.

Main Result. There exist a fixed positive integer c and a positive constant C not depending on $n = 2^k$ such that for cyclotomic integer rings $\mathbf{Z}[\xi_n] = \mathbf{Z}[x]/(\Phi_n(x))$ where $n = 2^k, k = 2, 3, \ldots$, if a generator of an arbtrary principal ideal $\mathbf{I} \subset \mathbf{Z}[\xi_n]$ has been found, then we can find a lattice vector $\mathbf{v} \in \mathbf{I}$ of length within $Cd^c\lambda_1(\mathbf{I})$ by using at most d^3 operations in $\mathbf{R}$. Here $d = \phi(n) = 2^{k-1}$ is the degree of the extension.

The PIP problem has been studied by many authors and we refer to [2, 3 , 4, 5, 6, 9, 13] for the latest development. A possible polynomial time quantum algorithm to solve the PIP for all algebraic number fields have been worked by some authors. Combining with our reduction this would implies that approximate SVP for principal ideal lattices in some cyclotomic integer rings within a polynomial factor is easy in quantum computing setting.

2 Short lattice vectors

The following proposition is useful in this paper.

Proposition 2.1. *If $\mathbf{x} \in \mathbf{I} \subset \mathbf{Z}[\xi_n]$ is an element of an ideal $\mathbf{I}$ in the ring of n-th cyclotomic integers. Then $(vol(\mathbf{I}))^{1/d} \leq ||(\mathbf{x}||_{tr}$. Here $d = \phi(n)$ is the degree of the degree of Φ_n. In particular $(vol(\mathbf{I}))^{1/d} \leq \lambda_1(\mathbf{I})$.*

Proof. It is clear $tr_{Q(\xi_n)/Q}(\mathbf{g}\mathbf{g}^*) = tr_{Q(\xi_n)/Q}(\mathbf{g}\xi_n^t\mathbf{g}^*(\xi_n^t)^*) = tr_{Q(\xi_n)/Q}(\mathbf{g}\mathbf{g}^*\xi_n^t(\xi_n^t)^*)$. Thus $\mathbf{g}, \mathbf{g}\xi_n, \ldots, \mathbf{g}\xi_n^{d-1}$ span a (full-rank) sub-lattice in $\mathbf{I}$ and $\prod_{t=0}^{d-1} ||\mathbf{g}\xi^t||_{tr} = ||\mathbf{g}||_{tr}^d \geq vol(\mathbf{I})$. The conclusion follows directly.

In the case of $n = 2^k$, Let $\mathbf{g} = g_0 + g_1\xi_n + \cdots + g_{d-1}\xi_n^{d-1} \in \mathbf{Z}[\xi_n]$ be a fixed cyclotomic integer, then the Gram matrix of the principal ideal lattice

$\mathbf{I}$ generated by $\mathbf{g}$ is $2^{k-1}\mathbf{GR_g} \cdot \mathbf{GR_g}^{\tau}$, where $\mathbf{GR_g}$ is the following matrix. Here τ is the transposition and $d = 2^{k-1}$.

$$\begin{pmatrix} g_0 & g_1 & g_2 & \cdots & g_{d-2} & g_{d-1} \\ -g_{d-1} & g_0 & g_1 & \cdots & g_{d-3} & g_{d-2} \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ -g_1 & -g_2 & -g_3 & \cdots & -g_{d-1} & g_0 \end{pmatrix}$$

Then the key problem is to lower bound $\frac{det\mathbf{GR_g}}{(||\mathbf{g}||)^d}$. The following Proposition 2.2 and 2.3 can be proved by a direct computation.

Proposition 2.2. *For any* $\mathbf{f} = f_0 + f_1\xi_n + \cdots + f_{d-1}\xi_n^{d-1} \in \mathbf{Z}[\xi_n]$*, the coefficients of* $\mathbf{gf} = u_0 + u_1\xi_n + \cdots + u_{d-1}\xi_n^{d-1}$ *is of the form* $(u_0, u_1, \ldots, u_{d-1}) = \mathbf{A_g} \cdot \mathbf{f}$*, where* $\mathbf{f} = (f_0, f_1, \ldots, f_{d-1})^{\tau}$ *and* $\mathbf{A_g}$ *is the following matrix.*

$$\begin{pmatrix} g_0 & -g_{d-1} & -g_{d-2} & \cdots & -g_2 & -g_1 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ g_{d-2} & g_{d-3} & g_{d-4} & \cdots & g_0 & -g_{d-1} \\ g_{d-1} & g_{d-2} & g_{d-3} & \cdots & g_1 & g_0 \end{pmatrix}$$

.

Proposition 2.3. *The* d *eigenvalues of this matrix* $\mathbf{GR_g}$ *is of the form* $(g_0 + g_1\xi_n^t + \cdots + g_{d-1}\xi_n^{t(d-1)})$ *with the eigenvector* $(1, \xi_n^t, \ldots, \xi_n^{t(d-1)})$*, where* t *are* 2^{k-1} *odd integers* $1, 3, \ldots, 2^{k-1} - 1$*. The* d *eigenvalues of this matrix* $\mathbf{A_g}$ *is of the form* $(g_{d-1} + g_{d-2}\xi_n^t + \cdots + g_0\xi_n^{t(d-1)})$ *with the eigenvector* $(1, \xi_n^t, \ldots, \xi_n^{t(d-1)})$*, where* t *are* 2^{k-1} *odd integers* $1, 3, \ldots, 2^{k-1} - 1$*.*

We note the $d = 2^{k-1}$ eigenvectors $(1, \xi_n^t, \ldots, \xi_n^{t(d-1)})$, where t are 2^{k-1} odd integers $1, 3, \ldots, 2^{k-1} - 1$, are orthogonal in Euclidean inner products, since $\xi_{2^k}^2$ is a 2^{k-1}-th root of unity.

Proposition 2.4. *The matrix* $\mathbf{GR_{gf}}^{\tau}$ *of the element* $\mathbf{gf}$ *is of the form* $\mathbf{A_g} \cdot \mathbf{F}$ *where* $\mathbf{F}$ *is the following matrix. It is actually the matrix* $\mathbf{A_f}$*.*

$$\begin{pmatrix} f_0 & -f_{d-1} & -f_{d-2} & \cdots & -f_2 & -f_1 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ f_{d-2} & f_{d-3} & f_{d-4} & \cdots & f_0 & -f_{d-1} \\ f_{d-1} & f_{d-2} & f_{d-3} & \cdots & f_1 & f_0 \end{pmatrix}$$

.

Proof. From Proposition 2.2 and a direct computation.

We denote $Re(1, \xi_n^t, \ldots, \xi_n^{t(d-1)})$ and $Im(1, \xi_n^t, \ldots, \xi_n^{t(d-1)})$ the real and the imaginary part of the vector $(1, \xi_n^t, \ldots, \xi_n^{t(d-1)})$, that is, $(1, \xi_n^t, \ldots, \xi_n^{t(d-1)}) = Re(1, \xi_n^t, \ldots, \xi_n^{t(d-1)}) + iIm(1, \xi_n^t, \ldots, \xi_n^{t(d-1)}), Re(1, \xi_n^t, \ldots, \xi_n^{t(d-1)}) \in \mathbf{R}^d$, $Im(1, \xi_n^t, \ldots, \xi_n^{t(d-1)}) \in \mathbf{R}^d$. Then we have the following relation.

Proposition 2.5. *Suppose t is an odd number. Then the two vectors $Re(1, \xi_n^t, \ldots, \xi_n^{t(d-1)})$ and $Im(1, \xi_n^t, \ldots, \xi_n^{t(d-1)})$ are orthogonal under the Euclidean inner product. The Euclidean norm of these two vectors are $\frac{2^{k-1}+1}{2}$ and $\frac{2^{k-1}-1}{2}$.*

Proof. $Re(1, \xi_n^t, \ldots, \xi_n^{t(d-1)}) = (1, \cos(\frac{2t\pi}{2^k}), \ldots, \cos((\frac{2t(2^{k-1}-1)\pi}{2^k}))$ and $Im(1, \xi_n^t, \ldots, \xi_n^{t(d-1)}) = (0, \sin(\frac{2t\pi}{2^k}), \ldots, \sin(\frac{2t(2^{k-1}-1)\pi}{2^k}))$. It is clear $\cos(\frac{2tj\pi}{2^k}) \cdot \sin(\frac{2tj\pi}{2^k}) = \frac{1}{2}\sin(\frac{2tj\pi}{2^{k-1}})$. Then the inner product of these two vectors is $\Sigma_{j=1}^{2^{k-1}-1}\frac{1}{2}\sin(\frac{2tj\pi}{2^{k-1}})$. It is the imaginary part of the complex number $\frac{1}{2}\Sigma_{j=0}^{2^{k-1}-1}\xi_{2^{k-1}}^t$, which is zero. Here $\xi_{2^{k-1}}$ is a 2^{k-1}-th primitive root of the unity.

From the relation $\cos(\frac{2t\pi}{2^k}) = \sin(\frac{2^{k-1}\pi}{2^k} - \frac{2t\pi}{2^k})$ and $\sin(\frac{-2tj\pi}{2^k}) = \sin(t\pi - \frac{2tj\pi}{2^k}) = \sin(\frac{(2^{k-1}-j)2t\pi}{2^k})$, we have the Euclidean norms of the two vectors $(0, \cos(\frac{2t\pi}{2^k}), \ldots, \cos((\frac{2t(2^{k-1}-1)\pi}{2^k}))$ and $(0, \sin(\frac{2t\pi}{2^k}), \ldots, \sin(\frac{2t(2^{k-1}-1)\pi}{2^k}))$ are the same. The second conclusion follows directly.

From proposition 2.3 we only need to check the least value of $|(g_0 + g_1\xi_n^t + \cdots + g_{d-1}\xi_n^{t(d-1)})|$. This is an inner product of $(g_0, \ldots, g_{d-1}) \in \mathbf{Z}^d$ with a vector $(1, \xi_n^t, \ldots, \xi_n^{t(d-1)})$

Corollary 2.1. *If there exist a positive constant C not depending on d and a function M of d, such that the absolute values of the Euclidean inner products of $\mathbf{g} = (g_0, g_1, \ldots, g_{d-1})$ with the above d orthogonal vectors with length 2^{k-1} is lower bounded by $\frac{C2^{k-1}||\mathbf{g}||}{M}$. Then $||\mathbf{g}||_{tr} \leq CM\lambda_1(\mathbf{I})$. In particular, if we can find a polynomial function $f(d) = M$, then $\mathbf{g}$ is a "short" generator.*

From Corollary 2.1 we know that a generator of a principal ideal $\mathbf{I}$ which

is "far" from the above orthogonal vectors is a "short" generator.

3 Reduction

The following Proposition 3.1 is a direct consequence of Proposition 2.4.

Proposition 3.1. *We have* $\frac{det(\mathbf{GR_{gf}})}{(||\mathbf{gf}||||)^d} = \frac{det(\mathbf{A_g})}{(||\mathbf{g}||)^d} \cdot \frac{(||\mathbf{g}||)^d \cdot (||\mathbf{f}||)^d}{(||\mathbf{gf}||)^d} \cdot \frac{det(\mathbf{F})}{(||\mathbf{f}||)^d}$. *Here* $||\mathbf{gf}|| = ||\mathbf{A_g} \cdot \mathbf{f}||$.

Then $|\frac{det(\mathbf{A_g})}{(||\mathbf{g}||)^d}| = \prod_{t=odd}(|\frac{(g_{d-1}+g_{d-2}\xi_n^t+\cdots+g_0\xi_n^{t(d-1)})}{||\mathbf{g}||}| = d^d \cdot \prod_{t=odd} |\cos\theta_t| \geq (d|\cos\theta_0|)^d$, where θ_t is the angle between the vector $(g_{d-1}, \ldots, g_0)$ and $(1, \xi_n^t, \ldots, \xi_n^{t(d-1)})$. Set θ_{t_0} to be the angle such that $|\cos\theta_t|$ is the smallest one among $|\cos\theta_1|, |\cos\theta_3|, \ldots, |\cos\theta_{2^k-1}|$.

The main idea of reduction is as follows. Since $\frac{(||\mathbf{g}||)^d \cdot (||\mathbf{f}||)^d}{(||\mathbf{gf}||)^d} = \frac{(||\mathbf{g}||)^d \cdot (||\mathbf{f}||)^d}{(||\mathbf{A_g} \cdot \mathbf{f}||)^d}$, if we take the vector $\mathbf{f} \in \mathbf{Z}^d$ which is very close to the real line spanned by the vector $Re(1, \xi_n^{t_0}, \ldots, \xi_n^{(d-1)t_0})$, then $\mathbf{A_g} \cdot \mathbf{f}$ is very close to the real line spanned by the vector $Re(g_{d-1} + g_{d-2}\xi_n^{t_0} + \cdots + g_0\xi_n^{t_0(d-1)})Re(1, \xi_n^{t_0}, \ldots, \xi_n^{(d-1)t_0}) - Im(g_{d-1}+g_{d-2}\xi_n^{t_0}+\cdots+g_0\xi_n^{t_0(d-1)})Im(1, \xi_n^{t_0}, \ldots, \xi_n^{(d-1)t_0})$, since $(1, \xi_n^{t_0}, \ldots, \xi_n^{(d-1)t_0})$ is an eigenvector of $\mathbf{A_g}$. Then $|\frac{det(\mathbf{A_gf})}{||\mathbf{g}||\cdot||\mathbf{f}||}|$ is very close to $|\frac{det(\mathbf{A_g}Re(1,\xi_n^{t_0},\ldots,\xi_n^{(d-1)t_0})}{||\mathbf{g}||\cdot||Re(1,\xi_n^{t_0},\ldots,\xi_n^{(d-1)t_0})||}|$ which satisfies $|\frac{det(\mathbf{A_g}Re(1,\xi_n^{t_0},\ldots,\xi_n^{(d-1)t_0})}{||\mathbf{g}||\cdot||Re(1,\xi_n^{t_0},\ldots,\xi_n^{(d-1)t_0})||}| \leq 2|\cos\theta_0|$ from Proposition 2.5. If we can take $\mathbf{f}$ as a fixed degree polynomial (of d) vector then the reduction can be done.

Since

$$\cos x = 1 - \frac{x^2}{2!} + \frac{x^4}{4!} - \frac{x^6}{6!} + \cdots +$$

holds when $|x| < \infty$. On the other hand $\lim_{n\longrightarrow\infty} \frac{x^n}{n!} = 0$ for fixed $|x| \leq 2\pi$. Thus the coordinates of the the following vector

$$Re(1, \xi_n^{t_0}, \ldots, \xi_n^{(d-1)t_0}) = (1, \cos\frac{2t_0\pi}{2^k}, \cos\frac{4t_0\pi}{2^k}, \ldots, \cos\frac{2t_0(2^{k-1}-1)\pi}{2^k})$$

can be approximated by fixed degree polynomial functions with rational coefficients. The real line spanned by this vector can be approximated by

vectors with fixed degree polynomial coordinates with integer coefficients. Then we have the following result.

Proposition 3.2. *There exists a fixed positive integer c such that we have vector $\mathbf{f} = (f_0, f_1, \ldots, f_{d-1})$ with coordinates $f_i \in \mathbf{Z}[x]$ and $deg(f_i) \leq c$ satisfying*

$$|\frac{det(\mathbf{A_g f})}{||\mathbf{g}|| \cdot (||\mathbf{f}||} | \leq 3|\cos\theta_0|$$

.

Because the computation of θ_0 and t_0 and the approximation in Proposition 3.2 can be done with in d^3 operations in $\mathbf{R}$, the main result is proved.

4 References

[1] M. Ajtai, The shortest vector problem in L_2 is NP-hard for randomized reduction, STOC 1998, 10-19.

[2] D. Bernstein, A subfield-logarithm attack in against some ideal lattices, http://blog.cr.yp.to/20140213-ideal.html.

[3] J.-F. Biasse and C. Fieker, Sub-exponential class group and uint group computation in large degree number fields, LMS J. Comput. Math., 17 (suppl. A), 385-403, 2014.

[4] J.-F. Biasse, Subexponential time relations in the class group of large degree number fields, Adv. Math. Commun., 8(4), 407-425, 2014.

[5] J.-F. Biasse and F. Song, A polynomial time quantum algorithm for computing class groups an solving the principle ideal problem in arbitrary degree number fields, http:// www.lix.polytechnique.fr/Labo/Jean-Francois.Biasse/.2015.

[6] P. Campbell, M. Grovers and D.Shepherd, Soliloquy: A cautionary tale, http://docbox.etsi.org/2014/201410-Crypto/S07-systems-and-Attacks/S07-Grovers-Annex.pdf.

[7] Jung Hee Cheon and Changmin Lee, cryptanalysis of multilinear map on ideal lattices, iacr e-print.

[8] H.Cohen, A Course in computational algebraic number theory, Graduate Texts in Mathematics 238, Springer-Verlag, 1993.

[9] R. Cramer, L. Ducas, C. Peikert and O.Regev, Recovering short generators of principle ideals in cyclotomic rings, iacr e-print 2015.

[10] K. Eisentrager, S. Hallgren, A. Kutaev and F. Song, A quantum algorithm for computing the unit group of an arbitrary degree number field, 46th ACM STOC, 293-302, 2014.

[11] C. Gentry, Fully homomorphic encryption using ideal lattices, S-TOC 2009, 167-178.

[12] S. Garg, C. Grag and S. Halevi, Candidate multilinear maps from ideal lattices, Eurocrypt 2013, 1-17.

[13] S. Hallgren, Polynomial-time quantum algorithms for Pell's equation and the principle ideal problem, Journal of ACM, vol.54(2005), no.1, 34:1-34:33.

[14] S. Khot, Hardness of approximating the shortest vector problem, Journal of ACM, vol.52 (2005), 789-808.

[15] V. Lyubashevsky and C. Peikert and O. Regev, On ideal lattices and learning with errors over rings, J. ACM, 60(6), 1-43, nov., 2013, preliminary version, Eurocrypt 2010.

[16] A. Langlois, D. Stehle and R. Steinfeld, Gghlite: More efficient multilinear maps from ideal lattices, Eurocrypt 2014, 239-256.

[17] D. Micciancio and S. Goldwasser, Complexity of lattice problems,A cryptographic perspective, Kluwer Academic Publishers.

[18] D. Micciancio, Generalized compact knapsaks, cyclic lattices and efficient one-way functions, Computational Complexity, 16(4), 365-411, 2007.

[19] D. Micciancio and O. Regev, Lattice-based cryptography, Book

chapter in Post-quantum Cryptography, D. J. Bernstein and J. Buchmann (eds.), Springer (2008).

[20] A. Migotti, Zur Theorie der Kreisteilungsgleichung, Sitzber. Math. Naturwiss. Classe der Kaiser. Akad. der Wiss. 87(1883) 7-14.

[21] T. Plantard and M. Schneider, Creating a challenge for ideal lattices, iacr e-print.

[22] N. Smart and F. Vercauteren, Fully homomorphic encryption scheme with relatively small key size and ciphertext sizes, PKC 2010.

[23] L. Washington, Introduction to cyclotomic fields, Graduate Texts in Mathematics 83, Springer-Verlag 1997.