Codes from Algebraic Number Fields

H.W. Lenstra, Jr.
Universiteit van Amsterdam, Mathematisch Instituut
P.O. Box 19268, 1000 GG Amsterdam, The Netherlands

Introduction

The geometry of numbers, coding theory, the Riemann hypothesis - the list of *key words* for this lecture can be read as a partial history of the *Stichting Mathematisch Centrum*. The lecture itself attempts to reflect the spirit of the *SMC* by displaying a new connection between these subjects. Using ideas from the *geometry of numbers* one can construct a class of *codes* from algebraic number fields, and the study of the asymptotic properties of these codes depends on the *generalized Riemann hypothesis.*

The construction described in this lecture is a generalization to algebraic number fields of the following idea to make a code. Let P be a finite set of prime numbers, and consider, for a suitable positive integer k, the set C of all elements

$$c_i = (i \bmod p)_{p \in P} \in \prod_{p \in P} \mathbb{Z}/p\mathbb{Z}, \quad i = 1, 2, \ldots, k.$$

If, for $i > j$, the elements c_i, c_j of this set agree on many coordinates then the difference $i - j$ is divisible by many primes, so also by their product. But this difference is less than k, which may lead to a contradiction. This gives us control over the minimum distance of C.

The codes just described have several undesirable properties. First, they are *mixed* codes in the sense that the alphabet size p is not constant. Secondly, they are non-linear, although they are still 'half-linear' in the sense that for any two distinct $x, y \in C$ one of $x - y$, $y - x$ belongs to C. Thirdly, for bounded alphabet size the above construction gives only finitely many codes. This means that the usual 'asymptotic' way of judging the quality of a class of codes, which we discuss in Section 1, does not apply to them. Finally, the

codes that we described are in all respects inferior to the codes that are obtained in an analogous way if one replaces the ring $\mathbb{Z}$ by the polynomial ring $\mathbb{F}_q[X]$ in one variable over a suitably chosen finite field $\mathbb{F}_q$, and P by a collection of polynomials of the form $X-\alpha$ with $\alpha \in \mathbb{F}_q$. These codes, the *generalized Reed-Solomon codes* [6, Chapter 10, Section 8], have at least the same minimum distance and dimension, they are linear and non-mixed, but they do have the third shortcoming just mentioned.

If we generalize the construction to algebraic number fields, as we do in Section 2, the situation changes only slightly. For any algebraic number field different from $\mathbb{Q}$ it is true that the ring of integers has different prime ideals with isomorphic residue class fields. Hence it would seem possible to make non-mixed codes by the same recipe. However it turns out that it is better to make non-mixed codes by starting from mixed codes that have a slight variation in the alphabet size. This leaves at least the possibility open to obtain satisfactory asymptotic results (see the remark on $r=q$ at the end of Section 3).

Our codes remain non-linear, even the 'half-linearity' mentioned above disappears.

For fixed alphabet size, the new construction gives infinitely many codes, so that in principle their quality can be analyzed asymptotically. Section 3 contains upper and lower bounds for how good our codes are. These bounds can be substantially improved if one assumes the truth of the generalized Riemann hypothesis, but even then there is a considerable gap between the upper and the lower bound.

The new codes are the analogues, for number fields, of the codes constructed by Goppa and Tsfasman [7, 12] from curves over finite fields. For the analogy between number fields and curves over finite fields, see [1, 14]. If the generalized Riemann hypothesis is true our codes are, asymptotically speaking, not as good as those of Goppa and Tsfasman. Also, the latter codes are linear and non-mixed.

We finally note that there is a non-constructive element in the description of our codes, so that it is still too early to ask for encoding and decoding algorithms. It can be imagined that lattice basis reduction algorithms [5] play a role in this context.

1 Codes

In this section we follow Manin [7, Section 2], except that we do not require codes to be linear.

Let q be an integer, $q>1$, and V a set of cardinality q, to be referred to as the *alphabet*. For each integer $n \geqslant 0$ we define a metric w on the set V^n by letting $w(x,y)$ be the number of coordinates where x and y differ. A *code* over V is a non-empty set C that for some integer $n \geqslant 0$ is a subset of V^n. The number n is called the *word length* of the code. The *dimension* $\dim(C)$ of the code is defined to be $(\log \# C)/(\log q)$, where $\#$ denotes cardinality. The *minimum distance* or simply *distance* $d(C)$ of the code C is the minimum of the numbers $w(x,y)$ if (x,y) runs over all pairs of distinct elements of C, for $\# C = 1$ this is $+\infty$.

We are interested in finding codes for which the dimension and the distance are large as functions of the word length. Each code C of positive word length n and positive dimension gives rise to a point $(d(C)/n, \dim(C)/n)$ of the unit square $[0,1]^2$. If C runs over all such codes we obtain a sequence of points in the unit square, and we denote by U_q the set of limit points of this sequence (If q is a prime power, this set contains the corresponding set from [7].)

As in [7] we have the following result (but not necessarily with the same function α_q)

THEOREM (1.1). *There is a continuous function* $\alpha_q : [0,1] \to [0,1]$ *such that*

$$U_q = \{(x,R): 0 \leqslant x \leqslant 1,\ 0 \leqslant R \leqslant \alpha_q(x)\}$$

The function α_q *assumes the value* 1 *in* $x = 0$, *is strictly decreasing on the interval* $[0,(q-1)/q]$, *and vanishes on the interval* $[(q-1)/q, 1]$ *Moreover, for* $0 \leqslant x \leqslant (q-1)/q$ *one has*

$$\beta_q(x) \leqslant \alpha_q(x) \leqslant 1 - \frac{q}{q-1}x$$

where

$$\beta_q(x) = 1 - \frac{x\log(q-1) - x\log x - (1-x)\log(1-x)}{\log q}$$

PROOF (sketch). It is easy to make codes that show that the points in the unit square that lie on the coordinate axes belong to U_q. Next let $(x,R) \in U_q$. Trivial constructions on codes, such as omitting code words or changing letters, show that the rectangle $[0,x] \times [0,R]$ is contained in U_q. Other constructions, such as projecting a code $C \subset V^n$ to V^{n-1} or intersecting it with a suitably embedded $V^{n-1} \subset V^n$, show that the line segments connecting (x,R) with $(0,R/(1-x))$ and $(x/(1-R),0)$ are contained in U_q (These line segments form part of the lines connecting (x,R) with $(1,0)$ and $(0,1)$.)

These results imply that U_q can be described, as in the theorem, by means of a non-increasing function α_q, that α_q is continuous except possibly at 0, and that it is strictly decreasing on the interval where it does not vanish

The Plotkin bound [13, Theorem 5.2.5] implies that α_q vanishes on $[(q-1)/q, 1]$, and by the above results this leads to the upper bound stated in the theorem. The lower bound is the Gilbert-Varshamov bound [13, Theorem 5.1.9] It implies continuity of α_q at $x = 0$

This concludes the proof of the theorem

For better upper bounds on α_q we refer to [13, Chapter 5] Only recently a better lower bound was found, and only for relatively large q. This was done with the help of modular curves and Shimura curves over finite fields [12].

The following result is useful in comparing the asymptotic properties of the codes that we shall construct with the Gilbert-Varshamov bound

PROPOSITION (1 2) *Let $r\in\mathbb{R}$, $r\geqslant 1$ Then the line*

$$R=(1-x)\frac{\log r}{\log q}-\frac{\log((q+r-1)/q)}{\log q}$$

is tangent to the graph of β_q at the point (x_0,R_0), where

$$x_0=\frac{q-1}{q+r-1},$$

$$R_0=\frac{r\log r}{(q+r-1)\log q}-\frac{\log((q+r-1)/q)}{\log q}$$

The proof is straightforward

2 NUMBER FIELDS

Let K be a *number field*, i e a field that is of finite degree m over the field $\mathbb{Q}$ of rational numbers, and let $s,t\in\mathbb{Z}$ be such that there is an isomorphism $K\otimes_{\mathbb{Q}}\mathbb{R}\cong\mathbb{R}^s\times\mathbb{C}^t$ of $\mathbb{R}$-algebras Denote by A the ring of integers of K, and by Δ the absolute value of its discriminant over $\mathbb{Z}$ The *norm* $\mathfrak{N}(\mathfrak{p})$ of a non-zero prime ideal $\mathfrak{p}$ of A is the cardinality of its residue class field $A/\mathfrak{p}$ For background on algebraic number theory we refer to [2, 11]

THEOREM (2 1) *Let K be a number field, and s,t,Δ as above Let r,q be integers satisfying $1<r\leqslant q$, and write*

$$n=s+t+\#\{\mathfrak{p}\ \ r\leqslant\mathfrak{N}(\mathfrak{p})^{k(\mathfrak{p})}\leqslant q \text{ for some } k(\mathfrak{p})\in\mathbb{Z}_{>0}\},$$

here $\mathfrak{p}$ ranges over the non-zero prime ideals of the ring of integers of K Then for any positive integer d there exists a code of word length n over an alphabet of q letters with distance at least d and dimension at least

$$(n+1-d)\frac{\log r}{\log q}-\frac{\log\sqrt{\Delta}}{\log q}$$

PROOF Let it first be assumed that K is *totally real*, i e $s=m$, $t=0$ Under the embedding $K\subset K\otimes_{\mathbb{Q}}\mathbb{R}\cong\mathbb{R}^m$ the ring A becomes a lattice, and if F denotes a fundamental domain for A then F has volume $\mathrm{vol}(F)=\sqrt{\Delta}$

Let U be the set of those $(x_i)_{i=1}^m\in\mathbb{R}^m$ for which

$$0<x_i<r^{(n+1-d)/m} \text{ for } 1\leqslant i\leqslant m$$

This is an open subset of $\mathbb{R}^m$, and $\mathrm{vol}(U)=r^{n+1-d}$

In analogy with the construction mentioned in the introduction one would now be inclined to make a code from the set $U\cap A$ A basic principle of the geometry of numbers suggests that $\#U\cap A$ is approximately equal to $\mathrm{vol}(U)/\sqrt{\Delta}$, but it turns out that the error term may dominate To solve this problem we average over all translations of U, which is a 'non-constructive' element in the description of the code

Let χ denote the characteristic function of U We have

$$\int_{z\in F} \#((z+U)\cap A)dz = \sum_{y\in A}\int_{z\in F}\chi(y-z)dz = \sum_{y\in A}\int_{z\in y-F}\chi(z)dz$$

$$= \int_{z\in\mathbb{R}^m}\chi(z)dz = \mathrm{vol}(U) = \int_{z\in F}\frac{\mathrm{vol}(U)}{\sqrt{\Delta}}dz,$$

where we use that $\mathbb{R}^m$ is the disjoint union of the sets $y-F$, $y\in A$. It follows that there exists $z\in F$ with $\#((z+U)\cap A)\geq \mathrm{vol}(U)/\sqrt{\Delta}$. Let such a z be chosen, and put $C=(z+U)\cap A$. Then we have

$$\#C \geq \frac{\mathrm{vol}(U)}{\sqrt{\Delta}} = \frac{r^{n+1-d}}{\sqrt{\Delta}}.$$

Let $V=\{0,1,\cdots,q-1\}$. For each $j\in\{1,2,\cdots,m\}$ we define a map $z+U\to V$ by dividing the projection of $z+U$ on the j-th coordinate axis into q intervals of equal length; i.e., the point $z+(x_i)_{i=1}^m\in z+U$ is mapped to $v\in V$ if

$$\frac{vr^{(n+1-d)/m}}{q} \leq x_j < \frac{(v+1)r^{(n+1-d)/m}}{q}.$$

Restricting this map to C we obtain a map $f_j: C\to V$.

For each $\mathfrak{p}$ as in the definition of n choose a positive integer $k(\mathfrak{p})$ with $r\leq \mathfrak{N}(\mathfrak{p})^{k(\mathfrak{p})}\leq q$ and an injective map $A/\mathfrak{p}^{k(\mathfrak{p})}\to V$. Let $f_{\mathfrak{p}}: C\to V$ be the composed map $C\subset A\to A/\mathfrak{p}^{k(\mathfrak{p})}\to V$.

Combining all maps f_j, $f_{\mathfrak{p}}$ we obtain a map $f: C\to V^n$. We claim that

$$\text{if } x,y\in C,\ x\neq y,\ \text{then } w(f(x),f(y))\geq d$$

where w denotes the Hamming distance (see Section 1). To prove this, let a be the number of j's for which $f_j(x)=f_j(y)$ and b the number of $\mathfrak{p}$'s for which $f_{\mathfrak{p}}(x)=f_{\mathfrak{p}}(y)$, so that $a+b=n-w(f(x),f(y))$. Denote by $N: K\to\mathbb{Q}$ the absolute value of the norm function. We estimate $N(x-y)$ in two ways. On the one hand, all conjugates of $x-y$ are less than $r^{(n+1-d)/m}$ in absolute value, and a of them are even a factor q smaller, so

$$N(x-y) < r^{n+1-d}/q^a \leq r^{n+1-d-a}.$$

On the other hand, $x-y$ is a non-zero algebraic integer belonging to b of the ideals $\mathfrak{p}^{k(\mathfrak{p})}$, which each have norm at least r, so that

$$N(x-y)\geq r^b.$$

It follows that $b<n+1-d-a$, so $w(f(x),f(y))=n-a-b\geq d$. This proves the claim.

It follows in particular that f is injective. Hence the code $f[C]\subset V^n$ has dimension $(\log\#C)/(\log q)$, which is at least $((n+1-d)\log r-\log\sqrt{\Delta})/(\log q)$. By the claim, the distance of $f[C]$ is at least d.

This proves the theorem in the case that K is totally real. To deal with the general case in the same way one needs an analogue, in the complex plane, of a real interval that is divided into q intervals that are q times as small. More precisely, one needs the following result.

For every positive integer q there exists a subset of the euclidean plane that has area $q/2$ and diameter $\leqslant \sqrt{q}$, and that can be written as the union of q sets of diameter $\leqslant 1$.

If q is a square this is proved by subdividing a square of area $q/2$ into q squares in the obvious way. We leave the elementary proof of the general case to the reader. The result can actually be improved, which gives rise to a slightly better lower bound for the dimension of the code, if $t>0$.

This completes the proof of the theorem.

To describe the asymptotic properties of the codes from Theorem (2.1) we introduce the following quantity. Let r,q be as in the theorem. Then we define

$$A(q,r) = \liminf_K \frac{\log\sqrt{\Delta}}{n\log q},$$

the liminf ranging over all number fields K, up to isomorphism, with n, Δ as in the theorem.

COROLLARY (2.2). *The segment of the line*

$$R = (1-x)\frac{\log r}{\log q} - A(q,r)$$

for which $0\leqslant x$, $R\leqslant 1$ lies entirely in the code domain U_q.

This is an immediate consequence of Theorem (2.1) and the results of Section 1.

3. ASYMPTOTICS

Let $A(q,r)$ be as defined in Section 2.

PROPOSITION (3.1). *There are positive constants c_1, c_2 such that $A(q,r)\geqslant c_1/q$ and $A(q,q)\geqslant c_2/\log q$ for all integers r,q with $1<r\leqslant q$.*

PROOF. For a number field K, let m,Δ,n be as in Section 2. Known lower bounds for discriminants (see [9]) imply that there is a positive constant c_3 such that $\log\Delta\geqslant c_3 m$ for all $K\neq\mathbb{Q}$. Moreover, it is obvious that $n\leqslant m\cdot(1+\pi(q))$, where $\pi(q)$ denotes the number of prime numbers $\leqslant q$, and that $n\leqslant 2m$ if $r=q$. Since $\pi(q)\leqslant c_4 q/\log q$ for some positive constant c_4 and all q, the proposition follows. This proves (3.1).

It is amusing to note that the first inequality of (3.1) can also be deduced from (1.1) and (2.2), as follows. It is easy to see that n is maximal if r is the least integer $\geqslant\sqrt{q}$; so let this be the case. Putting $x=(q-1)/q$ in (2.2) and using that α_q vanishes in this point one finds that

$$\frac{1}{q}\cdot\frac{\log r}{\log q} - A(q,r) \leqslant 0$$

so $A(q,r) \geqslant 1/(2q)$, as required.

The second inequality of (3.1) is best possible, apart from the value of the constant, as we shall see in (3.4). The first inequality of (3.1) can be sharpened if we assume the *generalized Riemann hypothesis*:

(GRH) *for every number field K, the Dedekind zeta function ζ_K has no complex zeroes with real part larger than $1/2$.*

PROPOSITION (3.2). *Let for every integer $q>1$ and every number field K the quantity $B_q(K)$ be defined by*

$$B_q(K) = \Big(\frac{1}{2}(\log 8\pi + \gamma + \frac{\pi}{2})s + (\log 8\pi + \gamma)t + \sum_{\mathfrak{p}, \mathfrak{N}(\mathfrak{p}) \leqslant q} \frac{\log \mathfrak{N}(\mathfrak{p})}{\sqrt{\mathfrak{N}(\mathfrak{p})} - 1}\Big)/\log\sqrt{\Delta}.$$

Here the summation ranges over non-zero prime ideals $\mathfrak{p}$ of the ring of integers of K, and $s,t,\Delta,\mathfrak{N}(\mathfrak{p})$ are as in Section 2. Further, γ denotes Euler's constant. Suppose moreover that (GRH) *is true. Then for every integer $q>1$ we have*

$$\limsup_K B_q(K) \leqslant 1,$$

the limsup *ranging over all number fields K, up to isomorphism.*

PROOF. This is an easy consequence of Weil's 'explicit formulae' in the theory of prime numbers, cf. [9, 10, 4]. This proves (3.2).

PROPOSITION (3.3). *Assume* (GRH). *Then for all integers r,q with $1<r\leqslant q$ one has*

$$A(q,r) > \frac{1}{\sqrt{q} - 1}.$$

PROOF. This follows from (3.2) by a direct calculation. This proves (3.3).

Next I consider upper bounds.

PROPOSITION (3.4). *There is a positive constant c_5 such that $A(q,r) \leqslant c_5/\log q$ for all integers r, q with $1<r\leqslant q$.*

PROOF. By the theory of infinite class field towers [2, Chapter IX] there exists a number field E such that the maximal totally unramified extension L of E is of infinite degree over E. We let K range over the finite extensions of E that are contained in L, and for each K we let m,Δ,s,t,n be as in Section 2. Each K is unramified over E, so the number $\Delta^{1/m}$ is independent of K. Also, one has $n \geqslant s+t \geqslant m/2$. It follows that

$$\liminf_{K, E \subset K \subset L} \frac{\log\sqrt{\Delta}}{n \log q} \leqslant \frac{c_5}{\log q}$$

for some positive constant c_5. This proves (3.4).

By (3.1), the inequality of (3.4) is best possible for $r=q$, apart from the value of the constant. If r is much smaller than q we can again use the generalized Riemann hypothesis to obtain a better result. For the sake of definiteness I choose r to be the least integer $\geqslant q/2$.

PROPOSITION (3.5). *Suppose that* (GRH) *is true. Then there is a positive constant* c_6 *such that for every integer* $q>1$ *we have* $A(q,[(q+1)/2]) \leqslant c_6(\log q)/q^{1/4}$.

The proof depends on two lemmas.

LEMMA (3.6). *Suppose that* q *is an integer,* $q>1$, *and that* k,l *are positive integers. Write*

$$d = 4\cdot\prod_{i=1}^{l} p_i,$$

where p_i *denotes the i-th prime number. Suppose that the following two conditions are satisfied.*

(i) $k+1 \leqslant \frac{1}{4}(l-1)^2-(l-1)$;

(ii) *there are at least* k *prime numbers* p *with* $\sqrt{q/2} \leqslant p \leqslant \sqrt{q}$ *for which the Legendre symbol* $(\frac{-d}{p})$ *equals* -1.

Then we have

$$A(q,\ [(q+1)/2]) \leqslant \frac{\log d}{2(k+1)\log q}.$$

PROOF. Let E be the imaginary quadratic field with discriminant $-d$. Each p as in (ii) generates a principal prime ideal $\mathfrak{p}$ of the ring of integers of E with $q/2 \leqslant \mathfrak{N}(\mathfrak{p}) \leqslant q$. Let S be a set of k such prime ideals. Denote by L the maximal totally unramified extension of E in which all $\mathfrak{p}\in S$ split completely. Using a slight generalization of the theory of infinite class field towers (see [4, Section 14]) one deduces from inequality (i) that L is of infinite degree over E. (Since all $\mathfrak{p}\in S$ are principal, the number t from [4, Section 14] equals $l-1$, and $\rho=k+1$.) To prove the lemma, let now K range over the finite extensions of E that are contained in L, as in the proof of (3.4). As before, the number $\Delta^{1/m}$ is independent of K, and putting $K=E$ one sees that it equals $\sqrt{d}$. Also, since each $\mathfrak{p}\in S$ splits completely in K one has $n \geqslant t+[K:E]\cdot\#S=\frac{1}{2}m(1+k)$ for each K. This proves (3.6).

LEMMA (3.7). *Assume* (GRH). *Then for every positive real number* c_7 *there is a positive real number* c_8 *with the following property.*

Let d *be a positive integer for which* $-d$ *is the discriminant of a quadratic*

field. Then for every real number x with $x \geqslant c_8(\log d)^2$ the number of odd prime numbers p for which

$$x/\sqrt{2} \leqslant p \leqslant x, \quad \left(\frac{-d}{p}\right) = -1$$

is at least $c_7(\log d)^2/\log\log d$.

PROOF. This is proved by a slight adaptation of the proof of [8, Theorem 13.1; pp. 120, 123, 124] (the weight function $(1-n/N)$ should be changed so as to count primes in the right interval). I thank H.L. MONTGOMERY for pointing this out to me.

PROOF OF (3.5). For any integer $l \geqslant 7$, let $k = k(l)$ be the largest integer satisfying (3.6)(i), and let $d = d(l)$ be as in (3.6). Then we have

$$\log d \sim l \cdot \log l, \quad k \sim (1/4)(\log d)^2/(\log\log d)^2$$

for $l \to \infty$, so there is certainly a positive constant c_7 such that $k \leqslant c_7(\log d)^2/\log\log d$ for all $l \geqslant 7$. Let c_8 be the number that Lemma (3.7) guarantees to exist.

Now let q be an integer, $q > 1$, and choose the integer l as large as possible subject to the condition $\sqrt{q} \geqslant c_8(\log d(l))^2$. We suppose that q is sufficiently large for l to be well-defined and $\geqslant 7$. By the choice of c_7 and Lemma (3.7), the conditions of (3.6) are satisfied for $k = k(l)$ and l, so (3.6) gives us an upper bound on $A(q, [(q+1)/2])$. We have

$$\log d \sim c_9 q^{1/4}, \quad k \sim (1/4)(\log d)^2/(\log\log d)^2 \sim c_{10}\sqrt{q}/(\log q)^2$$

for certain positive constants c_9, c_{10}, as $q \to \infty$. It follows that the upper bound from (3.6) leads to the upper bound stated in Proposition (3.5), at least for q sufficiently large. For the remaining values of q one can apply (3.4). This proves (3.5).

We discuss the implications of our estimates for coding theory.

The first inequality of (3.1) yields a rather crude upper bound for how good we can expect our codes to be. I do not know how this bound compares to the best upper bounds that are known for the function α_q of Section 1. It is conceivable that these, together with (2.2), lead to a better lower bound for $A(q,r)$.

The second inequality of (3.1) shows that it is not advisable to apply our construction only with $r = q$. By (1.2) that would at best lead to codes that are comparable to the codes realizing the Gilbert-Varshamov bound.

Proposition (3.3) is the analogue of the result that was proved by DRINFELD and VLADUT [3] for function fields of curves over finite fields. For very small q, such as $q = 2$, it shows that one should not expect our codes to lead to a point (x,R) of the code domain U_q with x and R *positive*. For large q, Propositions (3.3) and (1.2) show that one can still hope to find codes that beat the Gilbert-Varshamov bound. In the case of function fields this hope was indeed

realized for certain values of q, see [12].

It is apparently harder to construct good codes from number fields. Proposition (3.4) leads to codes whose performance is comparable to the Gilbert-Varshamov bound. Proposition (3.5) shows that much better codes can be made, for large q, if one again accepts (GRH). However, these codes are not as good as those made with function fields, and there remains a substantial gap between the bounds of (3.3) and (3.5). The analogy with function fields suggests that (3.3) is nearer to the truth than (3.5).

References

1. E. Artin, G. Whaples (1945). Axiomatic characterization of fields by the product formula for valuations. *Bull. Amer. Math. Soc. 51,* 469-492; pp. 202-225 in: *The Collected Papers of Emil Artin,* Addison-Wesley Publishing Company, Reading 1965.
2. J.W.S. Cassels, A. Fröhlich (eds.) (1967). *Algebraic Number Theory,* Academic Press, London.
3. V.G. Drinfeld, S.G. Vladut (1983). On the number of points on an algebraic curve (in Russian). *Funktsional. Anal. i. Prilozhen. 17 (1),* 68-69; English translation: *Functional Anal. Appl. 17,* 53-54.
4. Y. Ihara (1983). How many primes decompose completely in an infinite unramified Galois extension of a global field? *J. Math. Soc. Japan 35,* 693-709.
5. A.K. Lenstra, H.W. Lenstra, Jr., L. Lovász (1982). Factoring polynomials with rational coefficients. *Math. Ann. 261,* 515-534.
6. F.J. MacWilliams, N.J.A. Sloane (1978). *The Theory of Error-Correcting Codes,* North-Holland Publishing Company, Amsterdam.
7. Yu.I. Manin, (1981). What is the maximum number of points on a curve over $\mathbb{F}_2$? *J. Fac. Sci. Univ. Tokyo Sect. IA Math. 28,* 715-720.
8. H.L. Montgomery (1971). *Topics in Multiplicative Number Theory, Lecture Notes in Math. 227,* Springer-Verlag, Heidelberg.
9. G. Poitou (1977). Minorations de discriminants (d'après A.M. Odlyzko). *Séminaire Bourbaki 28 (1975/76), no. 479,* pp. 136-153 in: *Lecture Notes in Math. 567,* Springer-Verlag, Heidelberg.
10. G. Poitou. Sur les petits discriminants. *Séminaire Delange-Pisot-Poitou (Théorie des nombres) 18 (1976/77), no. 6.*
11. P. Samuel (1967). *Théorie Algébrique des Nombres,* Hermann, Paris; English translation: *Algebraic Theory of Numbers,* Houghton Mifflin Company, Boston 1970.
12. M.A. Tsfasman, S.G. Vladut, Th. Zink (1982). Modular curves, Shimura curves, and Goppa codes, better than Varshamov-Gilbert bound. *Math. Nachr. 109,* 21-28.
13. J.H. van Lint (1982). *Introduction to Coding Theory, Graduate Texts in Math. 86,* Springer-Verlag, New York.
14. A. Weil (1939). Sur l'analogie entre les corps de nombres algébriques et les corps de fonctions algébriques. *Revue Scient. 77,* 104-106; pp. 236-240 in: *Oeuvres Scientifiques / Collected Papers,* vol. I, Springer-Verlag, New York 1979.