Part one

Preliminaries

1

Introduction

The main subject of this book can be described as a study of various properties of the distribution of integer powers g^x of some integer $g > 1$ modulo a prime number p with $\gcd(g, p) = 1$. We are also interested in applications of such results to various problems. In particular, we consider several well-known problems from algebraic number theory, the theory of function fields over a finite field, complexity theory, the theory of linear congruential pseudo-random number generators, cryptography, and coding theory.

To describe more precisely the type of questions which we study in this book and which arise in the aforementioned applications, let us denote by t the multiplicative order modulo p of an integer $g > 1$ with $\gcd(g, p) = 1$.

For $(a, p) = 1$, $1 \le N \le t$, $0 \le M < p$, $1 \le H \le p$, we denote by $T_a(N, M, H)$ the number of solutions of

$$ag^x \equiv M + u \pmod{p}, \qquad 1 \le x \le N, \ 1 \le u \le H.$$

Typically, the aforementioned problems lead to one of the following questions about the distribution of residues of an exponential function.

- What is the largest value of $|T_a(N, M, H) - NH/p|$ over all $a = 1, \dots, p-1$ and $M = 0, \dots, p-1$?
- What are the restrictions on N and H, under which $T_a(N, M, H) > 0$ for every M?
- For how many integers i, $0 \le i \le p/H - 1$, is $T_a(N, iH, H) > 0$?
- What is the largest value of H (as a function of N) for which $T_a(N, M, H) = 0$ for some M?
- What is the smallest value of H (as a function of N) for which $T_a(N, M, H) = N$ for some M?

These questions may be asked:

- for all $a \in \mathbb{F}_p^*$;
- for some special a, say $a = 1$;
- for 'almost all' $a \in \mathbb{F}_p^*$;
- for at least one 'good' $a \in \mathbb{F}_p^*$;

and in several other cases.

Similar questions can be considered modulo composite numbers and, even more generally, for finitely generated multiplicative groups of algebraic number fields which are reduced modulo an integer ideal of that field.

Looking at the subjects that interest us, it should not be a big surprise that our main tool is various bounds for character sums. Thus we start this book with a collection of known relevant bounds as well as several new ones. In particular, we obtain new bounds of Gaussian sums. Indeed, it is easy to see that many questions about the distribution of g^x modulo p are equivalent to similar questions about the distribution of the x^n modulo p, where $n = (p-1)/t$, and this leads to Gaussian sums. Certainly the last subject is of great independent interest and we consider this topic as well. Then we present a series of new results on the structure of multiplicative shifts of multiplicative subgroups and arbitrary subsets of $\mathbb{F}_p^*$. In subsequent chapters, we give a wide spectrum of applications of these basic results.

As we have mentioned, studying the distribution of residues g^x modulo p is our central interest and is most important for the majority of our applications. Nevertheless, in some cases we need to consider the more general situation with finitely generated groups in algebraic number fields. This is why we formulate our main results concerning bounds of exponential sums in terms of such groups (even if the actual result is applicable only to the $g^x \pmod p$). The reader who is not interested in applications to algebraic number fields may always assume that 'integer ideal' means 'integer', 'prime ideal' means 'prime number', 'algebraic number field K' means just 'field of rationals $\mathbb{Q}$', finitely generated groups have rational integer generators, and so on.

There are also some technical reasons to work in a more general setting for arbitrary algebraic number fields. In fact, some of our results are proved (and formulated, of course) for the basic case of $g^x \pmod p$. Nevertheless, we believe they hold in the full generality. Obtaining such generalizations would be very important for a number of applications. In particular, we believe that in many of our statements, the words 'let $\mathfrak{p}$ be a prime ideal of first degree' (which essentially refer to the distribution modulo p) can be simplified to just 'let $\mathfrak{p}$ be a prime ideal'. We should remark that, as far as we can see, such generalizations will not be simple exercises but will require some new ideas.

In fact we hope that such new ideas could turn out to be useful for obtaining further results about the distribution of g^x modulo p as well.

Let $\mathbb{K}$ be an algebraic number field of degree n over the field of rational numbers $\mathbb{Q}$, and let $\mathbb{Z}_{\mathbb{K}}$ be its ring of integers. For an integer ideal $\mathfrak{q}$, we denote by $\Lambda_{\mathfrak{q}}$ the residue ring modulo $\mathfrak{q}$ and by $\Lambda_{\mathfrak{q}}^*$ the multiplicative group of units of this ring.

Given a finitely generated multiplicative group V of $\mathbb{K}$

$$V = \{\lambda_1^{x_1} \dots \lambda_r^{x_r} \ : \ x_1, \dots, x_r \in \mathbb{Z}\},$$

we denote its reduction modulo $\mathfrak{q}$ by $V_{\mathfrak{q}}$. We shall always suppose that the generators $\lambda_1, \dots, \lambda_r$ are multiplicatively independent.

There are a great many results on the behavior of groups V in $\mathbb{K}$ [29, 30, 13]. Here we concentrate on their reductions $V_{\mathfrak{q}}$. In the simplest, but probably the most important case, when $\mathbb{K} = \mathbb{Q}$ and $r = 1$, this is a classical question about the distribution of residues of an exponential function equivalent to considering the quality of the linear congruential pseudo-random number generator [37, 67, 69]. We shall consider this and other applications which rely on results which are not so widely known concerning the distribution of $V_{\mathfrak{q}}$ in $\Lambda_{\mathfrak{q}}$.

As we have mentioned, in many situations it is enough to study the case $\mathbb{K} = \mathbb{Q}$, $r = 1$ and moreover $\mathfrak{q} = p$ is a rational prime number.

Such applications include but are not limited to:

- Egami's question about smallest norm representatives of the residue classes modulo $\mathfrak{q}$ and Euclid's algorithm [12, 79];
- Prediction of the $1/M$-pseudo-random number generator of Blum, Blum, and Shub [6] and the linear congruential generator [16];
- Girstmair's problem about the relative class number of subfields of cyclotomic fields [20, 21, 22] and Myerson's problem about Gaussian periods [62, 63];
- Kodama's question about supersingular hyperelliptic curves [64, 68, 92, 93];
- Tompa's question about lower bounds for the QuickSort algorithm using a linear congruential pseudo-random number generator [36, 90];
- Lenstra's constants modulo $\mathfrak{q}$ and Győry's arithmetical graphs [29, 30, 48, 49, 65, 70];
- Estimating the dimension of BCH codes [5, 54];
- Robinson's question about small mth roots modulo p [75];
- Håstad, Lagarias, and Odlyzko's question about the average value of smallest elements in multiplicative translations of sets modulo p [31];
- Niederreiter's problem about the multiplier of linear congruential pseudo-random number generators [67, 69];

- Stechkin's question about the constant in the estimate of Gaussian sums with arbitrary denominators [86];
- Odlyzko and Stanley's problem about 0, 1-solutions of a certain congruence modulo p [71].

It is easy to extend the list of problems which are related to questions on the distribution or residues of finitely generated groups. As an example, we note papers [9, 23] where links to the weight distribution of arithmetic codes are displayed.

Another example is paper [51] where some properties of finitely generated groups were used to study certain algebraic questions. All these properties (combinations of Artin's conjecture and Tchebotarev's density theorem) were established (under the Extended Riemann Hypothesis, of course) in [60] which was motivated by [51].

Many other problems about the minimal polynomials of Gaussian periods (over rationals as well as over finite fields) are considered in [19, 24, 25, 26, 27, 28]. We also refer to [88, 89] for good expositions of various basic properties of Gaussian periods and related questions. Perhaps the methods of the present book can be applied to some of them. Indeed, in Chapter 10 we consider the problem about the norm of Gaussian periods. A more general question of computing their minimal polynomials is of great interest too (for details see the papers above). It turns out that several higher coefficients can be expressed in terms of the numbers $R(k, t, p)$, $k = 1, 2, \ldots$, of solutions of the equations

$$g_1 + \cdots + g_k = 0, \qquad g_1, \ldots, g_k \in G_t,$$

(we follow the notation of Chapter 10). Thus using various bounds of exponential sums, one can estimate (or even find an asymptotic formula for) $T(k, t, p)$ and then apply them to studying higher coefficients.

Of course any improvement of bounds of exponential sums used in this book would entail further progress in this area. The same is true for any improvement of Lemma 9.7.

Also, many questions about the distribution of residues of multiplicative groups can be reformulated in the dual form as questions about the distribution of indices and therefore bounds of multiplicative character sums, including the celebrated Burgess estimate, can be used. For example, see the remarks made in Chapter 15 and Chapter 7, and another example of using character sums in this kind of question is given in [23].

Generally, we do not try to extract all possible results accessible by our methods, nor do we try to get the best possible values of some (important) constants. Rather, we attempt to demonstrate different approaches from

various areas of mathematics in one attack on certain problems. One of the examples is Theorem 6.7 which is based on some delicate combinations of tools from mathematical analysis, geometry of numbers, and algebraic geometry. We pose several problems of different levels of difficulty. Some of them can probably be solved within the framework of this book, others will require some radically new ideas (although in general we try to avoid posing hopeless problems). We would like to believe that this book will stimulate further research in this very important and mathematically attractive area.

Finally, we stress that it would be interesting to consider similar questions for some other groups, say for finitely generated matrix groups, for groups of points on elliptic curves, or for finitely generated groups in function fields.

2

Notation and Auxiliary Results

Here we collect some notation and useful facts which we use repeatedly throughout this book.

We denote by $\log x$ the binary logarithm of x and by $\ln x$ the natural logarithm of x.

Several of our estimates include iterations of logarithmic functions and do not make any sense for some values of arguments. To save space and avoid using expressions like $\log \max\{2, \log \max\{2, k\}\}$, we define

$$\operatorname{Log} x = \max\{2, \log x\}, \qquad \operatorname{Ln} x = \max\{2, \ln x\}.$$

For a complex $z \in \mathbb{C}$, we denote by $\Re z$ its real part.

For a prime number p and an integer $a \neq 0$, we denote by $\operatorname{ord}_p a$ the p-adic order of a, that is the largest power of p which divides a.

For brevity, we set

$$\mathbf{e}(z) = \exp(2\pi i z).$$

As usual, $\pi(x)$ denotes the number of prime numbers which do not exceed x and $\pi(x, k, l)$ denotes the number of primes which do not exceed x and are congruent to l modulo k.

We also make use of the following estimates:

$$k - 1 \geq \varphi(k) \gg \frac{k}{\operatorname{Ln} \ln k}, \qquad \omega(k) \ll \frac{\ln k}{\operatorname{Ln} \ln k},$$

where $\varphi(k)$ is the Euler function and $\omega(k)$ is the number of prime divisors of integer $k \geq 2$, and

$$\tau(k) \leq \exp\left((\ln 2 + o(1)) \frac{\ln k}{\ln \ln k}\right), \qquad k \to \infty,$$

where $\tau(k)$ is the number of integer positive divisors of $k \geq 2$.

They easily follow from the Prime Number Theorem and can be found in [74] and many other sources.

For an element ϑ of a ring $\mathcal{R}$ we define the multiplicative order of ϑ as the smallest integer $t > 0$ for which $\vartheta^t = 1$, if such an integer exists, otherwise the multiplicative order is undefined. It is easy to see that if $\mathcal{R}$ is a finite ring and ϑ is not a zero divisor that the multiplicative order is always defined.

For an algebraic extension $\mathbb{L}$ of a field $\mathbb{K}$, $\mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(\alpha)$ and $\mathrm{Nm}_{\mathbb{L}/\mathbb{K}}(\alpha)$ denote the trace and the norm of $\alpha \in \mathbb{L}$ in $\mathbb{K}$, respectively. That is,

$$\mathrm{Tr}_{\mathbb{L}/\mathbb{K}}(\alpha) = \sum_{i=1}^{s} \sigma_i(\alpha) \quad \text{and} \quad \mathrm{Nm}_{\mathbb{L}/\mathbb{K}}(\alpha) = \prod_{i=1}^{s} \sigma_i(\alpha),$$

where σ_i, $i = 1, \ldots, s$, are distinct embeddings of $\mathbb{L}$ into the algebraic closure of $\mathbb{K}$, $s = [\mathbb{L} : \mathbb{K}]$. It is easy to verify that for a chain of extensions $\mathbb{F} \subseteq \mathbb{K} \subseteq \mathbb{L}$ we have

$$\mathrm{Tr}_{\mathbb{L}/\mathbb{F}}(\alpha) = \mathrm{Tr}_{\mathbb{L}/\mathbb{K}}\left(\mathrm{Tr}_{\mathbb{K}/\mathbb{F}}(\alpha)\right)$$

and

$$\mathrm{Nm}_{\mathbb{L}/\mathbb{F}}(\alpha) = \mathrm{Nm}_{\mathbb{L}/\mathbb{K}}\left(\mathrm{Nm}_{\mathbb{K}/\mathbb{F}}(\alpha)\right).$$

Let $\mathbb{K}$ be an algebraic number field of degree n over the field of rational numbers $\mathbb{Q}$. We denote by $\mathbb{Z}_{\mathbb{K}}$ the ring of integers of $\mathbb{K}$, that is the ring of elements of $\mathbb{K}$ whose minimal polynomial over $\mathbb{Q}$ is monic.

For an integer ideal $\mathfrak{q}$, we denote by $\Lambda_{\mathfrak{q}}$ the residue ring modulo $\mathfrak{q}$ and by $\Lambda_{\mathfrak{q}}^*$ the multiplicative group of units of this ring. It is well known that $|\Lambda_{\mathfrak{q}}| = \mathrm{Nm}(\mathfrak{q})$ and actually this can be taken as a definition of $\mathrm{Nm}(\mathfrak{q})$.

For any prime ideal $\mathfrak{p}$, $\mathrm{Nm}(\mathfrak{p}) = p^d$ for some prime p and integer d, $1 \le d \le n$, which is called the degree of $\mathfrak{p}$.

If $\mathfrak{p}$ is a prime ideal of degree d then $\Lambda_{\mathfrak{p}} \simeq \mathbb{F}_{p^d}$, a finite field of $p^d = \mathrm{Nm}(\mathfrak{p})$ elements.

It is easy to see that $\mathfrak{p} | p$ in $\mathbb{Z}_{\mathbb{K}}$. The ideal $\mathfrak{p}$ is called ramified if $\mathfrak{p}^2 | p$ and unramified otherwise.

If $\mathfrak{p}$ is an unramified prime ideal of first degree then $\Lambda_{\mathfrak{p}^k} \simeq \mathbb{Z}/(p^k)$ where $p = \mathrm{Nm}(\mathfrak{p})$.

We also have $|\Lambda_{\mathfrak{q}}^*| = \varphi(\mathfrak{q})$, where $\varphi(\mathfrak{q})$ is the Euler function in $\mathbb{Z}_{\mathbb{K}}$, which has properties very similar to these of the Euler function in $\mathbb{Z}$. For example, it is multiplicative and

$$\varphi(\mathfrak{p}^r) = \mathrm{Nm}(\mathfrak{p})^{r-1}\left(\mathrm{Nm}(\mathfrak{p}) - 1\right)$$

for any prime ideal power $\mathfrak{p}^r$.

The residue ring $\Lambda_{\mathfrak{q}}$ has $\mathrm{Nm}(\mathfrak{q})$ additive characters χ which are functions $\chi : \Lambda_{\mathfrak{q}} \to \mathbb{C}$ such that

$$\chi(z_1 + z_2) = \chi(z_1)\chi(z_2) \quad \text{and} \quad |\chi(z)| = 1$$

for any $z_1, z_2, z \in \Lambda_{\mathfrak{q}}$. The character χ_0 with $\chi_0(z) = 1$, $z = \Lambda_{\mathfrak{q}}$ is called trivial. Multiplicative characters are defined in a similar way with respect to the group $\Lambda_{\mathfrak{q}}^*$.

For a rational integer q the corresponding characters are of the form $\chi_a(z) = \mathbf{e}(az/q)$ for $a = 0, \ldots, q-1$. For a prime ideal $\mathfrak{p}$ of norm $\mathrm{Nm}(\mathfrak{p}) = p^d$ the characters of $\Lambda_{\mathfrak{p}}$ are of the form

$$\chi_a(z) = \mathbf{e}\left(\mathrm{Tr}_{\mathbb{K}/\mathbb{Q}}(az)/p\right), \qquad a \in \Lambda_{\mathfrak{p}}.$$

In both cases $a = 0$ corresponds to the trivial character.

Finally we mention two our very frequently used tools. The first one is the Cauchy inequality

$$\sum_{i=1}^{N} A_i B_i \le \left(\sum_{i=1}^{N} A_i^{\alpha}\right)^{1/\alpha} \left(\sum_{i=1}^{N} B_i^{\beta}\right)^{1/\beta}$$

which holds for any two sequences of positive numbers A_i, B_i, $i = 1, \ldots, N$ and any positive α, β with $\alpha^{-1} + \beta^{-1} = 1$.

The second one is the Hadamard inequality

$$|\det A|^2 \le \prod_{i=1}^{N} \sum_{j=1}^{N} |a_{ij}|^2$$

for the determinant of a matrix $A = \left(a_{ij}\right)_{i,j=1}^{N}$ with complex elements.

Part two

Bounds of Character Sums