Two variable polynomial congruences and capacity theory

Ted Chinburg[1,*,†], Brett Hemenway Falk[2,‡], Nadia Heninger[3,§], and Zachary Scherr[4,‡]

[1]Department of Mathematics, Univ. of Pennsylvania, Philadelphia, PA 19104, USA.
[2]Department of Computer Science, Univ. of Pennsylvania, Philadelphia, PA 19104, USA.
[3]Dept. of Computer Science and Engineering, U. C. S. D., La Jolla, CA 92093, USA.
[4]Google, Lewisburg, PA 17837.

Received: 17th January 2022 | Accepted: 14th July 2022

Abstract *Coppersmith's method for finding small solutions of multivariable congruences uses lattice techniques to find sufficiently many algebraically independent polynomials that must vanish on such solutions. We apply adelic capacity theory in the case of two variable linear congruences to determine when there is a second such auxiliary polynomial given one such polynomial. We show that in a positive proportion of cases, no such second polynomial exists, while in a different positive proportion one does exist. This has applications to learning with errors and to bounding the number of small solutions.*

Keywords: Congruence, Lattice, Capacity

2010 Mathematics Subject Classification: 11Y16, 11G30, 11H06

1 INTRODUCTION

Coppersmith's method [13] uses lattice basis reduction to find small solutions of polynomial congruences. This method and its variants have been used to solve a number of problems across cryptography, including attacks against low public exponent RSA [13], demonstrating the insecurity of small private exponent RSA [5], factoring with partial knowledge [13], and the approximate integer common divisor problem [17, 27, 12].

This paper is the second in a series relating Coppersmith's method to adelic capacity theory. In the most common approach to Coppersmith's method, which is the perspective we adopt in this paper, one constructs an auxiliary polynomial that is guaranteed by construction to have the desired solutions as roots. Using adelic capacity theory, we showed in our first paper that in the univariate case, Coppersmith's constructive bounds are tight: Above the bound, no auxiliary polynomial of the form constructed in the algorithm can exist.

Coppersmith's method can also be applied to find solutions to multivariate polynomials or systems of polynomials. Unlike the univariate case, which is a fully rigorous method, the method used in the existing cryptanalytic literature to address the multivariate case is heuristic. In order to solve an m-variable system, one searches for m (or more) suitable auxiliary polynomials in an explicitly constructed lattice, and then solves the system of auxiliary polynomials to find the possible roots. In order for this method to work, one needs to find m suitable algebraically independent polynomials constructed through the lattice. The existing constructions are unable to guarantee the algebraic independence of multiple auxiliary polynomials, and thus the applications of this method all rely on a heuristic assumption of algebraic independence.

In this paper, we apply adelic capacity theory to two-variable linear polynomial congruences. This is the simplest case involving multivariate polynomials, and it includes the hidden number problem and ring learning with errors as special cases. The analysis turns out to already be quite involved, and we cannot apply existing results from adelic capacity theory in a black-box way.

It is always possible to find at least one auxiliary function that is linear from the construction in Coppersmith's method. We show that this function can be used to determine rigorously whether Coppersmith's method can succeed. That is, we show that one can use capacity theory to determine from the first auxiliary function whether there will be a second function that is algebraically independent of the first. This is because the zero locus of the first function is an affine line, to which one can apply the work on capacity theory by Cantor [7] and Rumely [25]. As a consequence of this approach, we will show that the heuristic assumption of algebraic independence does not

†Partially supported by NSF SaTC grants No. 1513671 and 1701785.
‡Partially supported by NSF SaTC grant No. 1513671.
§Partially supported by NSF SaTC grants No. 1513671 and 1651344.
*Corresponding Author: ted@math.upenn.edu

hold in general for all problem instances. In particular, we give an infinite family of examples for which there can be no pair of algebraically independent functions of any degree in Coppersmith's method. However, we have a method for determining rigorously whether such a pair exists in a given case. We also give an infinite family of examples for which such a pair does exist.

If one is looking for small integral solutions of linear polynomial congruences in a particular number field, one can apply lattice techniques directly, without constructing auxiliary functions. Coppersmith's method pertains to finding all such solutions in all number fields, i.e. in the ring of all algebraic integers. In the case of homogenous congruences, one solution produces infinitely many by multiplying all the variables by an arbitrary root of unity. Thus in this case, there are either infinitely many solutions in the ring of all algebraic integers, or no solutions at all. For this reason, if one can use capacity theoretic arguments to show that there are only finitely many solutions, one knows that in fact there are no solutions at all. This leads in §1.2 and §6 to strong bounds on the number of solutions of inhomogeneous congruences as well. In particular, we show in §6 how this approach leads to a computable sufficient criterion for there to exist at most one solution in any number field to a hidden number problem involving two linear congruences.

Our methods amount to giving effective upper and lower bounds to various finite morphism capacities in multivariable capacity theory (see [11]). This is the first time to our knowledge that multivariable capacity theory has been applied to cryptography. For a discussion of how one variable capacity theory pertains to Coppersmith's method, see [10].

ACKNOWLEDGEMENT

The authors would like to thank the two anonymous referees for helpful suggestions.

1.1 THE HIDDEN NUMBER PROBLEM AND RING LEARNING WITH ERRORS

In cryptographic applications, the hidden number problem is defined over the integers as follows. In the usual formulation, there is a public integer modulus n. One is given many samples $\{(c_i, d_i)\}_{i=0}$ in which $c_i, d_i \in \mathbb{Z}/n$. One is told that there is a secret residue class s mod n such that each residue class $c_i s - d_i$ is represented by an unknown but "small" integer $x_i \in \mathbb{Z}$. The problem is to find s mod n from $\{(c_i, d_i)\}_{i=0}$. One can reformulate the problem over an arbitrary commutative ring R by replacing $n\mathbb{Z}$ by an ideal I of R provided one has an appropriate notion of the size of elements of R.

Returning to $R = \mathbb{Z}$ and $I = n\mathbb{Z}$, note that each sample satisfies the linear relation

$$x_i - c_i s + d_i \equiv 0 \bmod n$$

For each relation, the x_i are unknown and small, and the value s is unknown. Suppose c_0 is relatively prime to n, so that $c_0 c_0' \equiv 1 \bmod n$ for a readily computable integer c_0'. The above congruence for $i = 0$ then gives

$$s \equiv c_0'(x_0 + d_0) \bmod n \tag{1.1}$$

Substituting this into the congruences for $i = 1, \ldots, m$ then gives a new system of congruences

$$x_i + t_i x_0 + a_i \equiv 0 \bmod n \quad \text{for} \quad 1 \le i \le m \tag{1.2}$$

in small unknowns x_i and x_0, where $t_i = -c_i c_0'$ and $a_i = d_i - c_i c_0' d_0$ are computable from the given data. Because of (1.1), we can reformulate the problem of finding s mod n as finding a solution $\{x_i\}_{i=0}^m$ to the system of congruences (1.2) with appropriate size bounds on all of the x_i.

The "usual" method used to solve this problem comes from Boneh and Venkatesan [6], and consists of solving a closest vector problem where the solution vector corresponds to the desired solution to the problem. In this paper we consider a dual construction, corresponding to Howgrave-Graham's reformulation of Coppersmith's method [16, 14]: Using lattice methods, we try to construct polynomials in the variables $\{x_i\}_{i=0}^m$ which must vanish on all solutions, and whose common zero locus is finite.

Boneh and Venkatesan give bounds for which with high probability there is a unique solution when the t_i are generated uniformly at random modulo n. In practical applications of this method, one is dealing with fixed parameters. In these cases one can empirically measure the probability of success [1], but a rigorous analysis of the number of possible solutions has not been done in the literature.

In the ring learning with errors problem [20], one has a public commutative ring R, typically an order in the ring of integers O_F of a number field F, and a secret $s \in R$. The input to the problem is a set of samples $\{(c_i, d_i)\}_{i=0}^m$ of pairs of elements of R/I. One is told that there is a secret residue class s in R/I for which d_i is congruent to $c_i \cdot s + e_i$ modulo a given ideal $\mathcal{I} \subset R$, where the $e_i \in R$ are unknown errors that are small in some sense. Typically the e_i must be "short" relative to the complex embeddings of R. One would like to recover s mod I from the data $\{c_i, d_i\}_{i=0}^m$. This is equivalent to the hidden number problem over R on setting $x_i = -e_i$.

1.2 SOLUTION COUNTING AND CAPACITY THEORY

The problem that we consider in this paper unifies both of the above problems, but we limit ourselves to the case of two samples. As noted above, one can eliminate the unknown secret s and obtain a single two-variable linear polynomial where the desired solution for both variables is "small". For a given solution, one can then use the original polynomials to solve for a unique s determined by that solution.

One basic question is: How unique is s? When $m + 1 = 2$, we will show in §6 that there is at most one s when the capacity associated to an adelic set arising from the lattice construction is less than 1.

A peculiarity of this approach is that in the ring-LWE case, we can actually bound the number of solutions in *all* number fields, and not just in a particular F.

We will now describe the three related problems we will study. To describe these we need only the following notions from algebraic number theory: The ring of integers O_F of a number field F, ideals of O_F, the discriminant $D_{F/\mathbb{Q}}$ of F over $\mathbb{Q}$, the numbers $r_1(F)$ and $r_2(F)$ of real embeddings and pairs of complex embeddings of F, and the integral closure $\overline{\mathbb{Z}}$ of O_F in an algebraic closure $\overline{\mathbb{Q}}$ of $\mathbb{Q}$. For background on these concepts, see [26, Chap. III, IV.2] and [18, Chapters I and III].

Let $\mathcal{J}$ be a non-zero ideal of the ring of integers O_F of a number field F. We will suppose a and t are elements of O_F such that $\mathcal{J} + tO_F = O_F$, so that t projects to a unit of $O_F/\mathcal{J}$ if $\mathcal{J} \neq O_F$.

Problem 1.1. *Let F, $\mathcal{J}$, a and t be fixed and satisfy the above hypotheses. Let X and Y be positive real numbers. Give a finite time algorithm for listing all $x, y \in \overline{\mathbb{Z}}$ such that*

1. $x + ty + a \equiv 0$ *mod* $\mathcal{J}\overline{\mathbb{Z}}$ *and*
2. *For every ring embedding $\lambda : \overline{\mathbb{Z}} \to \mathbb{C}$, the images x' and y' of x and y satisfy $|x'| \leq X$ and $|y'| \leq Y$.*

Problem 1.2. *Given F, $\mathcal{J}$, a, t, X and Y as in Problem 1.1, are there only finitely many algebraic integers $x, y \in \overline{\mathbb{Z}}$ having the properties in Problem 1.1?*

Problem 1.3. *Construct non-zero polynomials $g(\mathrm{x}, \mathrm{y}) \in F[\mathrm{x}, \mathrm{y}]$ with the following properties:*

1. *For all $x', y' \in \overline{\mathbb{Z}}$ such that $x' + ty' + a \equiv 0$ mod $\mathcal{J}\overline{\mathbb{Z}}$ the value $g(x', y')$ lies in $\overline{\mathbb{Z}}$.*
2. *Suppose $x', y' \in \mathbb{C}$ and that $|x'| \leq X$ and $|y'| \leq Y$. Then $|\lambda(g)(x', y')| < 1$ for all embeddings $\lambda : F \to \mathbb{C}$, where $\lambda(g)(\mathrm{x}, \mathrm{y}) \in \mathbb{C}[\mathrm{x}, \mathrm{y}]$ is the image of $g(\mathrm{x}, \mathrm{y})$ under the homomorphism $F[\mathrm{x}, \mathrm{y}] \to \mathbb{C}[\mathrm{x}, \mathrm{y}]$ induced by λ.*

Note that Problem 1.1 is a constrained hidden numbers problem of the kind in equation (1.2) over $R = \overline{\mathbb{Z}}$ when $n\mathbb{Z}$ is replaced by $\mathcal{I} = \mathcal{J}\overline{\mathbb{Z}}$ and we set $m = 1$, $t = t_1$, $a = a_1$, $x_0 = y$ and $x_1 = x$. Thus a hidden number problem over this R with $m + 1 = 2$ samples leads to Problem 1.1. If in the hidden number problem we required the residue class s mod I to also be represented by a "small" element s of R, then we could need only 1 sample. This is because $c_0 \cdot s + e_0 = d_0$ mod $\mathcal{I}$ has the form of Problem 1.1 on setting $y = s$ and $e_0 = x$.

Coppersmith's method relates these problems in the following way.

Suppose $\{g_i(\mathrm{x}, \mathrm{y})\}_i$ is a family of polynomials which each have the properties in Problem 1.3. Let $x, y \in \overline{\mathbb{Z}}$ have the properties in Problem 1.2. Then $g_i(x, y)$ will be an algebraic integer. Every embedding of $g_i(x, y)$ into $\mathbb{C}$ lies in $\mathbb{R}$ and has the form $\lambda(g_i)(x', y')$ for some conjugates $x' = \lambda(x)$ of x and $y' = \lambda(y)$ of y and some embedding $\lambda : \overline{\mathbb{Z}} \to \mathbb{C}$. Since $|\lambda(g_i)(x', y')| < 1$ for all such (x', y'), the product formula (see [18, p. 99]) or an easy norm argument shows $g_i(x, y) = 0$.

Suppose now that the common zero locus of the family $\{g_i(\mathrm{x}, \mathrm{y})\}_i$ is finite. It follows that there are finitely $x, y \in \overline{\mathbb{Z}}$ as in Problems 1.1 and 1.2. If one has an algorithm for producing a family of $\{g_i(\mathrm{x}, \mathrm{y})\}_i$ with all of these properties, as well as for finding their finite set of common zeros, one has an algorithm for solving Problem 1.1.

Suppose, to the contrary, that there are infinitely many $x, y \in \overline{\mathbb{Z}}$ as in Problem 1.2. Then the common zero locus of any family $\{g_i(\mathrm{x}, \mathrm{y})\}_i$ of the above kind cannot be finite, and Coppersmith's method cannot lead to a finite time algorithm for finding all the $x, y \in \overline{\mathbb{Z}}$ having the properties in Problem 1.1.

We can now state our main result in qualitative terms; a more quantitative version is given in Theorem 5.4. Let $r_1(F)$ and $r_2(F)$ be the number of real and complex places of F, and let $D_{F/\mathbb{Q}}$ be the disciminant of F.

Theorem 1.4. *Suppose $X > 0$ and $Y > 1/3$ satisfy the inequality*

$$(\pi/2)^{3r_2(F)} \cdot 3^{-3[F:\mathbb{Q}]} \cdot |D_{F/\mathbb{Q}}|^{-3/2} \cdot \mathrm{Norm}_{F/\mathbb{Q}}(\mathcal{J}) > (XY)^{[F:\mathbb{Q}]} \tag{1.3}$$

There exists a non-zero linear function $g_1(\mathrm{x}, \mathrm{y}) = \tau\mathrm{x} + \gamma\mathrm{y} + \delta \in F[\mathrm{x}, \mathrm{y}]$ with the properties in Problem 1.3. Given any such $g_1(\mathrm{x}, \mathrm{y})$, there is a procedure for determining which of the following alternatives hold:

1. *Suppose we decrease both X and Y by arbitrarily small non-zero amounts. Then there is a polynomial $g(\mathrm{x}, \mathrm{y}) \in F[\mathrm{x}, \mathrm{y}]$ for which the conditions in Problem 1.3 hold for which the common zero locus of $g(\mathrm{x}, \mathrm{y})$ and $g_1(\mathrm{x}, \mathrm{y})$ is finite. Such a $g(\mathrm{x}, \mathrm{y})$ leads to a finite time algorithm for finding all $x, y \in \overline{\mathbb{Z}}$ as in Problem 1.1 for the new values of X and Y.*

2. *Suppose we increase both X and Y by arbitrarily small non-zero amounts. Then for these new values of X and Y, all polynomials $g(\mathrm{x},\mathrm{y}) \in F[\mathrm{x},\mathrm{y}]$ of any degree having the properties in Problem 1.3 are divisible by $g_1(\mathrm{x},\mathrm{y})$. There are infinitely many $x, y \in \overline{\mathbb{Z}}$ as in Problem 1.2 for the new values of X and Y, and thus Coppersmith's method in the above form cannot be used to solve Problem 1.1.*

One of these alternatives must hold, and they are not mutually exclusive.

We show in Theorem 5.4 that the case in which both alternatives (1) and (2) occur is when a certain adelic capacity is exactly equal to 1. We construct in Theorem 5.10 infinitely many examples in which option (1) occurs but (2) does not, and infinitely many other examples in which option (2) occurs but (1) does not. For these examples, $F = \mathbb{Q}$, $\mathcal{J} = p\mathbb{Z}$ for a prime p of increasing size and $X = Y = c\sqrt{p}$ for a fixed positive constant c. We show that each of options (1) and (2) occur for a positive proportion (as $p \to \infty$) of pairs of t and a in $\mathbb{Z}/p$ for which t is prime to p.

The methods in this paper lead to explicit results for various families of two variable congruences via an explicit computation of capacities. Here is one example.

Theorem 1.5. *Let F be an imaginary quadratic field and let $|\ |$ be the Euclidean absolute value on F associated to a complex embedding of F. Suppose $a, t \in O_F$ are nonzero and $aO_F + tO_F = O_F$. Let q be a rational prime such that $3|a| < q$, and suppose $X = |a|$ and $Y = |a|/|t|$. We can take*

$$g_1(\mathrm{x},\mathrm{y}) = \frac{\mathrm{x} + t\mathrm{y} + a}{q} \in F[\mathrm{x},\mathrm{y}].$$

Alternative (1) of Theorem 1.4 holds if

$$Y < \frac{8}{3\sqrt{3}} = 1.5396...$$

while alternative (2) of Theorem 1.4 holds if

$$Y > \frac{8}{3\sqrt{3}}.$$

This example shows that when one chooses X and Y appropriately, one has an obvious choice of a first auxiliary function. Given such choice, there is a procedure for computing a capacity that determines which alternative of Theorem 1.4 holds in terms of a and t. In the example, small ratios $|a|/|t|$ lead to an effective finiteness result, while large values $|a|/|t|$ lead to there being an infinite number of solutions $(x, y) \in \overline{\mathbb{Z}}^2$ of Problem 1.1 so that Coppersmith's method cannot be applied. The values $X = |a|$ and $Y = |a|/|t|$ and the bound $3|a| < q$ arise naturally from the fact that then the three terms of $x' + ty' + a$ each have absolute values bounded by $|a|$ and the sum has absolute value less than q whenever x' and y' are complex numbers with $|x'| \le X$ and $|y'| \le Y$.

In §6, we consider bounds on the number of pairs (x, y) as in Problem 1.3 when case (1) of Theorem 1.4 occurs. When a capacity associated to X and Y is sufficiently small, we show in Theorem 6.1 that there is at most one pair (x, y) with the properties in Problem 1.1. This relies on the fact that in the special case when $a = 0$, multiplying both x and y by a root of unity leads to another solution. Therefore when $a = 0$, either one has no solutions or an infinite number. Because of this, if one can show there are only finitely many solutions via capacity theory when $a = 0$, there in fact can be no solutions at all. This fact leads to another phenomenon, namely that when $a = 0$, a small solution to a linear homogeneous congruence prevents the existence of solutions which have uniformly smaller archimedean absolute values. We state one example here: a more general result is shown in Theorem 6.3.

Theorem 1.6. *Suppose n is is a positive integer, $\mathcal{J} = nO_F$, $a = 0$ and $XY \le n/2$. Suppose (x_0, y_0) is a pair of algebraic integers with the properties stated for x and y in Problem 1.1. Assume in addition that x_0, y_0 and n are coprime in the sense that no pair of these numbers is contained in a proper ideal of O_F. Then there is no non-zero pair (x_1, y_1) of algebraic integers having the properties in Problem 1.1 for which the following is true: $|\lambda(x_1)| \le |\lambda(x_0)|$ and $|\lambda(y_1)| \le |\lambda(y_0)|$ for all embeddings $\lambda : \overline{\mathbb{Z}} \to \mathbb{C}$ with strict inequality holding for at least one of x or y for at least one λ.*

2 RELATED RESULTS ON COPPERSMITH'S METHOD

In this section we discuss some literature pertaining to Coppersmith's method that pertains to this paper. In [13] and its references, Coppersmith considered monic polynomials $f(\mathrm{x}) \in \mathbb{Z}[\mathrm{x}]$ of degree δ and a modulus N. He gave an algorithm that is polynomial time in $\log N$ and 2^δ for finding all integers x such that $f(x) \equiv 0 \bmod N$ and $|x| < N^{1/\delta}$. The strategy is to use the LLL algorithm to produce a polynomial $h(\mathrm{x}) \in \mathbb{Q}[\mathrm{x}]$ such that $h(x) = 0$ for all integers x with these properties. Coppersmith also considered irreducible two variable polynomials $p(\mathrm{x},\mathrm{y}) = \sum_{i,j} p_{ij}\mathrm{x}^i\mathrm{y}^j \in \mathbb{Z}[\mathrm{x},\mathrm{y}]$. Suppose $X, Y > 0$ are given and that $W = \max_{ij}|p_{ij}|X^iY^j$. Coppersmith gave an algorithm for finding an integer solution (x, y) of $p(x, y) = 0$ such that $|x| \leq X$ and $|y| \leq Y$, if one exists, provided that $XY < W^{3/(2\delta)}$. The strategy was to produce a polynomial $h(\mathrm{x}, \mathrm{y}) \in \mathbb{Q}[\mathrm{x}, \mathrm{y}]$ not divisible by $p(\mathrm{x}, \mathrm{y})$ such that $h(x, y) = 0$ for all integers x and y as above. Since $p(\mathrm{x}, \mathrm{y})$ was assumed to be irreducible, the common zero locus of $h(\mathrm{x}, \mathrm{y})$ and $p(\mathrm{x}, \mathrm{y})$ is finite. Coppersmith also pointed out in [13] that the method of producing auxiliary functions which must vanish at suitably small solutions of diophantine equalities or congruences can be applied to more general systems of polynomial equations in many variables. There is by now a substantial literature on this problem; see, for example, [21], [24] and their references. Without attempting to review this literature, we will mention here a few specific results.

The paper [23] by May and Ritzenhofen concerns the problem of finding all small integer solutions of systems of one variable polynomial congruences modulo a set of mutually co-prime moduli. The strategy is to show this is equivalent to finding all small solutions of a different congruence involving only one polynomial in one variable. Following an observation by Coppersmith in [14], the authors note that one cannot in general improve the upper bound $|x| < N^{1/\delta}$ to $|x| < N^{1/\delta+\epsilon}$ for $\epsilon > 0$ in Coppermith's original theorem due to the fact that that the number of solutions may then become exponential in N. This will certainly be the case when $f(x) = x^\delta$ and $N = p^\delta$ for some prime p, for example.

A central question has been to determine when the following heuristic holds. Once the geometry of numbers applied to suitable convex symmetric sets of polynomials produces one auxiliary polynomial that must vanish on the desired solution, will there be sufficiently many auxiliary polynomials in a slightly larger convex set of this kind which are algebraically independent? The common zero locus of this larger collection of polynomials will then be finite.

The paper [2] begins with a discussion of experiments by various authors to test the above heuristic. It then develops a sufficient condition for Coppersmith's method to succeed in finding three algebraically independent auxiliary polynomials when one applies it to find small integral zeroes of a polynomial in three variables. This built on work of Bauer in [3] that constructed three variable examples in which the heuristic definitely fails. Some further examples in which the heuristic fails for bivariate polynomials over the integers are discussed in [4] and [22]. Experimental evidence both for and against the heuristic is discussed in [22]. Note in particular the discussion after Figure 3 of [22] of situations in which the heuristic did not hold experimentally.

In [10] we showed that for one variable polynomial congruences of the kind Coppersmith originally considered, there are no auxiliary polynomials of the kind his method requires if one replaces the bound $|x| < N^{1/\delta}$ by $|x| < N^{1/\delta+\epsilon}$ for some $\epsilon > 0$. This is because the capacity theory on curves discussed in the next section shows that there are infinitely many solutions of the same congruence in the ring of all algebraic integers whose conjugates all lie in the disk of radius $N^{1/\delta+\epsilon}$. All such algebraic integers would have to be a zero of an auxiliary polynomial of the kind used in Coppersmith's method. Theorem 1.4 of this paper shows how capacity theory can give a necessary and sufficient condition for the above heuristic to hold in the case of two variable linear polynomial congruences. In this case, the heuristic holds for a positive proportion of the possible initial data, and it fails for a different positive proportion of this data.

3 BACKGROUND ON CAPACITY THEORY

In [10, Section 3] there is a review of the completions of a number field and of capacity theory for the projective line. This material is essential for the proofs in this paper, and we won't repeat it here. Instead we will give a brief overview of the capacity theory on curves developed in [7] and [25]. In fact, we will only need the case of the projective line, but an overview of the theory may still be helpful. We also discuss some explicit techniques for computing capacities that we need in this paper.

For background on curves over fields, see [15, Chap. 1]. The points of a curve C defined over F that lie in an extension field L of F are simply the set $C(L)$ of solutions in L of the equations defining C. The function field $F(C)$ of C over F is the set of functions f that are well defined off a finite set of points of C and that are the restriction to C of ratios of homogeneous polynomials of the same degree with coefficients in F when we embed C into a sufficiently large projective space containing C. The set of points of C where f is not defined is the set of poles of f, and when C is a so-called regular curve, one can assign a well defined order to each of these poles.

Suppose now that F is a number field. The first application we will make of capacity theory on curves C over F is to show the existence of non-zero functions $f \in F(C)$ with two properties. First, the poles of f should lie in a specified finite subset of points of C over an algebraic closure $\overline{F}$ of F. Second, f should have boundedness properties on specified subsets of $C(L)$ as L varies over various extensions of F. The L we consider will either be the complex numbers $\mathbb{C}$ or a completion $\mathbb{C}_p$ of the algebraic closures of p-adic fields. For background on p-adic fields, see [10, Section 3.1] and [12, Chap. II]. When $L = \mathbb{C}$, the boundedness we seek is that for each embedding of F into $\mathbb{C}$, one has $|f(z)| < 1$ when z lies in a specified subset of the points $C(\mathbb{C})$. Here the specified subset can depend on the embedding, and $f(z)$ is the complex number that results from embedding F into $\mathbb{C}$ and evaluating the resulting function at z. When L is $\mathbb{C}_p$ one proceeds in the same way using the embeddings of F into $\mathbb{C}_p$ and a canonical real valued absolute value $|\ |_p$ on $\mathbb{C}_p$. The collection of subsets for L varying as above is called an adelic subset, and this must satisfy various constraints relative to the set of poles that are allowed for f. When an f of the above kind exists, one can use the product formula (see [18, p. 99]) to show that all points of $C(\overline{L})$ that have all of their conjugates in the adelic set in question must be zeros of f. In particular, there are only finitely many such points.

The second application we make of capacity theory is to show that there are in fact infinitely many points of $C(\overline{F})$ that have all of their Galois conjugates over F lying in a specified adelic set. In this case, there can be no function f as above. It was a remarkable discovery going back to the original work of Fekete and Szegö that there is a single real number associated to an adelic set and a collection of allowed poles, called the capacity of this pair, that essentially distinguishes the two cases, apart from boundary cases in which the capacity equals exactly 1. The work of Fekete and Szegö was generalized from subsets of $\mathbb{C}$ to adelic subsets of the projective line by Cantor [7]. Rumely then generalized Cantors work to arbitrary smooth projective curves over a global field (including the case of number fields) in [25].

There are (at least) two distinct ways of trying to produce functions f of the above kind. The first approach, due to Cantor and then generalized by Rumely, is to consider where the zeros of f should lie, and what the orders of the poles of f should be, in order to achieve the desired boundedness properties. This leads to questions in potential theory and game theory. Potential theory enters into this because the logarithm of the absolute value of f at points in specified subsets of $C(\mathbb{C})$ or $C(\mathbb{C}_p)$ involves terms that are well approximated by the potential energy of charge distributions associated to the zeros of f. Game theory becomes useful in deciding the orders of the poles of f at each of the elements of the finite set at which poles are allowed. The approach via potential theory and game theory is very amenable to computation. The optimal distribution of zeros of f arises as an equilibrium distribution minimizing potential energy, while the optimal distribution of poles can be studied using classical two-person multi-option games. We will use this method in §5 to compute various relevant capacities.

An entirely different approach to constructing f arises from the geometry of numbers. One shows that the capacity of an adelic set relative to an allowed set of poles measures the asymptotic rate of growth of a convex symmetric set of adelically defined functions. If this growth rate is sufficiently large, then a Minkowski argument shows that there must in fact be a nonzero element of $F(C)$ that lies in this adelic set, and this f has the required boundedness properties. Depending on the adelic set, one can often translate the problem of finding such an f explicitly to that of finding a small non-zero point of a lattice, so that the LLL algorithm and its generalizations can be applied. This was in fact the approach of Coppersmith [13, 14] before the connection with capacity theory was noticed in [10]. By contrast, to construct f explicitly using potential theory and game theory requires delicate arguments showing that there is in fact a rational function in $F(C)$ whose zero locus is sufficiently close to various equilibrium distributions and whose poles track the results of a game theoretic computation.

The Minkowski approach has the virtue that it may be applied to higher dimensional varieties as well (see [9], [19], [11] and [8]). However, this produces only one useful auxiliary function. As discussed in the previous section, various papers (see [21]) have proposed the heuristic that in natural cases, once there is one useful auxiliary function, there will be enough others that are algebraically independent to be able to show finiteness of the set of global points of a variety satisfying various constraints. We develop here a systematic approach in dimension two for determining when the heuristic does or does not apply by using the first auxiliary function to reduce to a case that can be studied definitively using capacity theory on curves.

4 CONSTRUCTING ONE AUXILIARY FUNCTION

It is well known that the existence of one function of the kind in Problem 1.3 for sufficiently small positive values of X and Y is a consequence of Minkowski's theorem:

Theorem 4.1. *Suppose $X > 0$ and $Y > 1/3$ satisfy the inequality (1.3). There exists a a polynomial $g_1(\mathrm{x},\mathrm{y}) = b_1\mathrm{x} + b_2\mathrm{y} + b_3 \in \mathcal{J}^{-1} \cdot O_F[\mathrm{x},\mathrm{y}]$ with the following properties:*

i. For all embeddings $\lambda : F \to \mathbb{C}$ one has

$$|\lambda(b_1)| < 1/(3X), \quad |\lambda(b_2)| < 1/(3Y), \quad \text{and} \quad |\lambda(b_3)| < 1/3.$$

ii. $g_1(x,y) = 0$ for all pairs of algebraic integers (x,y) as in Problem 1.2.

iii. $b_1 \neq 0$ and $g_1(\mathrm{x},\mathrm{y}) \equiv b_1(\mathrm{x} + t\mathrm{y} + a) \bmod O_F[\mathrm{x},\mathrm{y}]$

All such $g_1(\mathrm{x},\mathrm{y})$ have the properties in Problem 1.3.

Proof. Let $\mathbb{R}_F = \mathbb{R} \otimes_{\mathbb{Q}} F = \oplus_{v \in M_\infty} F_v$ where M_∞ is the set of archimedean places of F . Give $\mathbb{R}_F$ the Euclidean norm resulting from the usual Euclidean norms $|\ |_v$ on the F_v. (Note that the normalized absolute value on F_v is

$|\ |_v^{[F_v:\mathbb{R}]}$.) Let $V = \mathbb{R}_F\mathrm{x} + \mathbb{R}_F\mathrm{y} + \mathbb{R}_F$ be the real vector space of all polynomials of degree at most 1 over $\mathbb{R}_F$. We give V the Euclidean inner product resulting from viewing it as a free $\mathbb{R}_F$-module on $\{\mathrm{x}, \mathrm{y}, 1\}$. Let $L \subset V$ be the O_F-sublattice

$$L = \mathcal{J}^{-1} \cdot (\mathrm{x} + t\mathrm{y} + a) + O_F \cdot \mathrm{y} + O_F. \tag{4.4}$$

Then

$$\mathrm{covolume}(V/L) = 2^{-3r_2(F)}|D_{F/\mathbb{Q}}|^{3/2}\mathrm{Norm}_{F/\mathbb{Q}}(\mathcal{J})^{-1}$$

by [18, Lemma 2, Chap. V.2].

For $d > 0$ define $B(0,d)$ to be the set of all $\xi = (\xi_v)_{v\in M_\infty} \in R_F = \oplus_{v\in M_\infty} F_v$ such that $|x_v| < d$ for all $v \in M_\infty$. Consider the convex symmetric subset

$$S(d_1, d_2, d_3) = \{r_1\mathrm{x} + r_2\mathrm{y} + r_3 : r_1 \in B(0, d_1), r_2 \in B(0, d_2), r_3 \in B(0, d_3)\}.$$

Then

$$\mathrm{vol}(S(d_1, d_2, d_3)) = (2^{r_1(F)}\pi^{r_2(F)})^3(d_1d_2d_3)^{[F:\mathbb{Q}]}.$$

Suppose

$$\mathrm{vol}(S) > 2^{3[F:\mathbb{Q}]}\mathrm{colvolume}(V/L) \tag{4.5}$$

Minkowski's theorem then guarantees that there is a non-zero $g_1(\mathrm{x}, \mathrm{y}) = b_1\mathrm{x} + b_2\mathrm{y} + b_3 \in L \cap S$.

Suppose $(x, y) \in \overline{\mathbb{Z}}^2$ has the properties in Problem 1.2, so that $x + ty + a \in \mathcal{J}\overline{\mathbb{Z}}$, $|\lambda(x)| < X$ and $|\lambda(y)| < Y$ for all embeddings $\lambda : \overline{\mathbb{Z}} \to \mathbb{C}$. From the definition of L and that fact that g_1 is a polynomial in $L \cap X$, we find that $g_1(x, y) \in \overline{\mathbb{Z}}$ and

$$|\lambda(g_1(x, y))| < d_1X + d_2Y + d_3$$

for all λ. Thus if we choose d_1, d_2, d_3 such that

$$d_1X + d_2Y + d_3 = 1 \tag{4.6}$$

we can conclude that $g_1(x, y) = 0$ since the norm of $g_1(x, y)$ to $\mathbb{Z}$ is an integer of absolute value less than 1. The choice of $d_1, d_2, d_3 > 0$ for which (4.6) holds and $\mathrm{vol}(S)$ is maximized is

$$(d_1, d_2, d_3) = (1/(3X), 1/(3Y), 1/3)$$

leading to

$$\mathrm{vol}(S) = (2^{r_1(F)}\pi^{r_2(F)})^3(d_1d_2d_3)^{[F:\mathbb{Q}]} = (2^{r_1(F)}\pi^{r_2(F)})^3 \cdot (3^{-3}/(XY))^{[F:\mathbb{Q}]}.$$

Combining this with the Minkowski inequality (4.5) leads to the conclusion that if XY satisfies the inequality in (1.3), then (i) and (ii) of Theorem 4.1 hold.

Finally, suppose $b_1 = 0$. The definition of L in (4.4) then shows that $g_1(\mathrm{x}, \mathrm{y}) = b_2\mathrm{y} + b_3$ with $b_2, b_3 \in O_F$. However, property (i) of Theorem 4.1 together with our assumption that $Y > 1/3$ forces b_2 and b_3 to have all conjugates of absolute value less than 1. This forces $b_2 = b_3 = 0$ as well, contradicting the fact that $g_1(\mathrm{x}, \mathrm{y})$ is a non-zero polynomial. □

Remark 4.2. There may be many $g_1(\mathrm{x}, \mathrm{y})$ with the properties in Theorem 4.1. Each one will lead to a different adelic capacity in the next section that can be used to study the problems described in §1.2. The numerical values of these capacities will depend on $g_1(\mathrm{x}, \mathrm{y})$, but the conclusions to be drawn concerning the problems in §1.2 will not depend on $g_1(\mathrm{x}, \mathrm{y})$. A more canonical approach would be to compute one associated adelic capacity on a surface, as in [11], rather than using slices of the appropriate surface to reduce to the case of curves. At present, however, capacity theory on surfaces is not as computable as capacity theory on curves.

5 ADELIC SUBSETS OF THE ZERO LOCUS OF THE FIRST AUXILIARY FUNCTION.

The strategy now for studying Problem 1.2 is to use the fact that all solutions must be on the zero locus of the auxillary function described in Theorem 4.1. This zero locus is an affine line. We will determine the adelic constraints that the Galois conjugates of a point on this line must satisfy which are equivalent to providing a solution to Problem 1.2. We then apply adelic capacity theory on the line to determine whether or not there are infinitely many such solutions, and whether there is a second auxillary polynomial with the right adelic properties which is not divisible by the first one produced by Theorem 4.1.

Throughout this section, we fix the following notations.

Definition 5.1. *Let $g_1(\mathrm{x},\mathrm{y}) = b_1\mathrm{x} + b_2\mathrm{y} + b_3$ be a polynomial wth the properties in Theorem 4.1. Let $M_F = M_{F,\mathrm{fin}} \cup M_{F,\mathrm{inf}}$ be the set of all absolute values v of F, where $M_{F,\mathrm{fin}}$ (resp. $M_{F,\mathrm{inf}}$) is the set of finite (resp. infinite) places. Let $\overline{F}_v$ be an algebraic closure of F_v. If $v \in M_{F,\mathrm{fin}}$, let $|\ |_v$ be an extension to $\overline{F}_v$ of the usual normalized absolute value on F_v, Let $|\mathcal{J}|_v$ in this case be the value of $|\ |_v$ on any element of $\mathcal{J} \subset O_F$ which generates the completion of $\mathcal{J}$ at v. If $v \in M_{F,\mathrm{inf}}$, identify $\overline{F}_v$ with $\mathbb{C}$ and let $|\ |_v$ be the usual Euclidean absolute value. Define a subset of E_v of $\overline{F}_v$ in the following way:*

i. If v is non-archimedean, let E_v be the set of $y \in \overline{F}_v$ such that $|y|_v \le 1$, $|b_2y + b_3|_v \le |b_1|_v$ and $|-(b_2y + b_3)/b_1 + ty + a|_v \le |\mathcal{J}|_v$.

ii. If v is archimedean, let E_v be the set of $y \in \overline{F}_v$ such that $|y|_v \le Y$ and $|b_2y + b_3|_v \le |b_1|_v \cdot X$.

Lemma 5.2. *If $v \in M_{F,\mathrm{fin}}$ then E_v is either empty or a disk of the form*

$$D(c_v, r_v) = \{y \in \overline{F}_v : |y - c_v|_v \le r_v\}$$

for some $c_v \in F_v$ and $0 \le r_v \in \mathbb{R}$. For all but finitely many $v \in M_{F,\mathrm{fin}}$ one can take $c_v = 0$ and $r_v = 1$, in which case $E_v = D(0,1)$. If v is archimedean, then E_v is either empty or the non-empty intersection of two disks in $\overline{F}_v = \mathbb{C}$ which have centers at 0 and at a point in F_v. The adelic set $\mathcal{E} = \prod_v E_v$ has capacity relative the point ∞ on $\mathbb{P}^1_F$ equal to

$$\gamma(\mathcal{E}) = \prod_{v \in M_F} \gamma_v(E_v) \tag{5.7}$$

where $\gamma_v(E_v)$ is the local capacity of E_v as a subset of $\mathbb{P}^1(\overline{F}_v) - \{\infty\} = \mathbb{A}^1(\overline{F}_v) = \overline{F}_v$. One has $\gamma_v(E_v) = r_v^{[F_v:\mathbb{Q}_{p(v)}]}$ if v is finite of residue characteristic $p(v)$. If v is infinite, $\gamma_v(E_v)$ is computed in Theorem 5.5 below.

Proof. The description of E_v is clear from Definition 5.1 together with the fact that the intersection of any two non-archimedean disks in $\overline{F}_v$ for $v \in M_{F,\mathrm{fin}}$ is either empty or equal to a disk. The fact that $E_v = D(0,1)$ for all but finitely many $v \in M_{F,\mathrm{fin}}$ follows from the the fact each of the three inequalities defining E_v describes either $D(0,1)$ or all of $\overline{F}_v$ for all but finitely many v. Hence $\mathcal{E}$ has a well defined capacity with respect to ∞, and the formula (5.7) is shown in [25, p. 366]. The fact that $\gamma_v(E_v) = r_v^{[F_v:\mathbb{Q}_{p(v)}]}$ for $v \in M_{F,\mathrm{fin}}$ is shown in [25, p. 352] on taking account our normalization of $|\ |_v$. □

Remark 5.3. The constants c_v and r_v for $v \in M_{F,\mathrm{fin}}$ are readily computed from the coefficients of $g_1(\mathrm{x},\mathrm{y}) = b_1\mathrm{x} + b_2\mathrm{y} + b_3$. The same is true for the centers and radii of the two disks whose intersection is E_v when $v \in M_{F,\mathrm{inf}}$. Thus (5.7) is readily computable from $g_1(\mathrm{x},\mathrm{y})$ using Theorem 5.5.

Theorem 5.4. *Let $\gamma(\mathcal{E})$ be as in (5.7).*

1. *If $\gamma(\mathcal{E}) > 1$ then there are infinitely many solutions (x, y) to Problem 1.2. In this case, any polynomial $g_i(\mathrm{x},\mathrm{y}) \in F[\mathrm{x},\mathrm{y}]$ with the properties in Problem 1.3 must be divisible by $g_1(\mathrm{x},\mathrm{y})$ in $F[\mathrm{x},\mathrm{y}]$. In particular, the intersection of the zero loci of all polynomials $g_i(\mathrm{x},\mathrm{y})$ with the properties in Problem 1.3 is the zero locus of $g_1(\mathrm{x},\mathrm{y})$, which is infinite.*
2. *If $\gamma(\mathcal{E}) < 1$ then there are only finitely many solutions (x, y) to Problem 1.2. The common zero locus of the polynomials in Problem 1.3 is finite.*
3. *Suppose $\gamma(\mathcal{E}) \ne 0$. As a function of $X > 0$ and $Y > 1/3$, the value of $\gamma(\mathcal{E})$ strictly increases when both X and Y are increased. In particular, suppose $\gamma(\mathcal{E}) = 1$ for particular values of X and Y. Any increase of both X and Y leads to the conclusions of part (1), while any decrease of both X and Y leads to the conclusions of part (2). This establishes parts (1) and (2) of Theorem 1.4.*

Proof. Recall that a solution (x, y) to Problem 1.2 is a pair of $x, y \in \overline{\mathbb{Z}}$ such that $x + ty + a \equiv 0 \bmod \mathcal{J}\overline{\mathbb{Z}}$ and all archimedean conjugates x' and y' of x and y' satisfy $|x'| \le X$ and $|y'| \le Y$. We know that

$$g_1(x, y) = b_1x + b_2y + b_3 = 0$$

for all such (x, y), where $b_1 \ne 0$. So we have

$$x = \frac{-b_2y - b_3}{b_1} \tag{5.8}$$

Because of (5.8), these conditions on x and y translate into the condition that all conjugates over F of the element $y \in \overline{F}$ lie in the set $E_v \subset \overline{F}_v$ described in Definition 5.1 for each $v \in M_F$. Parts (1) and (2) of the Theorem are now consequences of 4's results concerning Fekete-Szegö theorems for the projective line (see [7, Theorems 5.1.1 and 5.1.2] and [25, Theorems 6.3.1 and 6.3.2]).

For part (3), note that if $\gamma(\mathcal{E}) \neq 0$ then $\gamma_v(E_v) \neq 0$ for all v. In particular, E_v cannot be empty or a single point. Supose now that $v \in M_{F,\mathrm{inf}}$. Then E_v is intersection of two closed disks, and E_v has non-empty interior. Increasing X and Y to some $X' > X$ and $Y' > Y$ then expands both disks. This puts the set E_v for X and Y into $\lambda \cdot E'_v$ for some positive real $\lambda < 1$ when E'_v is the corresponding intersection of disks for X' and Y'. We thus have $\gamma_\infty(E_v) \le \gamma_\infty(\lambda E'_v) = \lambda \cdot \gamma_\infty(E'_v) < \gamma_\infty(E'_v)$. This proves that $\gamma_\infty(E_v)$ strictly increases when we increase both X and Y, which implies part (3) of the Theorem. □

We now give the formula for the capacity $\gamma_v(E_v)$ for archimedean v which was referred to at the end of the statement of Lemma 5.2. Let $D(a,t)$ be the closed disk in $\mathbb{C}$ with center $a \in \mathbb{C}$ and radius $r \ge 0$.

Theorem 5.5. *Suppose E_v is the intersection in $\overline{F}_v = \mathbb{C}$ of two closed disks, one of which is centered at the origin. Then there is a non-zero complex number ξ such that $E_v = \xi \cdot V$ where $V = D(0,r) \cap D(1,s)$ for some $r, s \ge 0$. One has $\gamma_v(E_v) = (|\xi| \cdot \gamma_\infty(V))^{[K_v:\mathbb{R}]}$ where $\gamma_\infty(V)$ is the classical transfinite diameter of V, which may be computed in the following way. If $V = \emptyset$ or $r + s = 1$ then $\gamma_\infty(V) = 0$. If $r \ge 1 + s$ then $V = D(1,s)$ and $\gamma_\infty(V) = s$. If $s \ge 1 + r$ then $V = D(0,r)$ and $\gamma_\infty(V) = r$. Otherwise, the boundaries of $D(0,r)$ and $D(1,s)$ intersect at two points u and $\overline{u}$ with u in the upper half plane. Let $\alpha \in (0,\pi)$ be the angle between the boundary of $D(0,r)$ and the boundary of $D(1,s)$ at the intersection point u. There is a unique point ζ in the upper half plane such that*

$$\zeta = \left(\frac{\overline{u} - r}{u - r}\right)^{\pi/(2\pi-\alpha)} \tag{5.9}$$

when we compute the complex exponential using the branch of log *with imaginary part lying in $[0, 2\pi]$. One has*

$$\gamma_\infty(V) = \frac{1}{2\mathrm{Im}(\zeta)} \cdot \frac{\pi}{2\pi - \alpha} \cdot |\overline{u} - u| \tag{5.10}$$

To prove this result we will need the following fact from [25, p. 339].

Lemma 5.6. *(Rumely) Suppose E is a connected subset of $\mathbb{C}$. Let E^c be the complement of E in $\mathbb{P}^1(\mathbb{C}) = \mathbb{C} \cup \{\infty\}$. Suppose $f(z)$ is a conformal map which takes E^c to the complement of the closed disc $D(0,R)$ of radius $R > 0$. Suppose further that $\lim_{z\to\infty} f(z)/z = 1$. Then $\gamma_\infty(E) = R$. The Green's function $G(z,\infty : E)$ equals $\log|f(z)/R)|$ for $z \in E^c$ and $G(z,\infty; E) = 0$ for $z \in E$.*

Proof of Theorem 5.5

The first statement is clear on rotating and dilating E_v appropriately, and the formula $\gamma_\infty(E_\infty) = (|\xi|\gamma_\infty(V))^{[K_v:\mathbb{R}]}$ is shown in [25, p. 352]. Since the transfinite diameter of a disk or radius R is R, it will suffice to construct an $f(z)$ for the $E = V$ of Theorem 5.5 on the assumption that the boundaries of $D(0,r)$ and $D(1,s)$ intersect at the distinct points u and $\overline{u}$. The cross ratio

$$w(z) = \frac{(u - z)(\overline{u} - r)}{(u - r)(\overline{u} - z)}$$

has $w(u) = 0$, $w(r) = 1$ and $w(\overline{u}) = \infty$. Since fractional linear transformations send circles to either lines or circles, we find that $z \to w(z)$ sends the arc formed by the boundary of $D(0,r)$ between u and $\overline{u}$ to the union of the non-negative real axis with ∞. Since fractional linear transformations also preserve angles, $z \to w(z)$ sends the arc formed by the boundary of $D(1,s)$ between u and $\overline{u}$ to the union of $\{\infty\}$ with the ray L outward from $w(u) = 0$ which makes an angle of α from the positive real axis and lies in the lower half plane. Thus the image of V under $z \to w(z)$ is the union of $\{\infty\}$ with an angular sector in $\mathbb{C}$ bounded by the non-negative real axis and L. The complement V^c is sent to set $w(V^c)$ of non-zero complex numbers $\tau = |\tau|e^{2\pi i\theta}$ for which $0 < \theta < 2\pi - \alpha$. This is illustrated in Figure 1.

On choosing the branch of the complex logarithm with imaginary part in $[0, 2\pi)$, we have a conformal map ν taking $w(V^c)$ to the upper half plane H defined by $\nu(w) = w^{\pi/(2\pi-\alpha)}$. This map sends $w(\infty) = \frac{\overline{u}-r}{u-r} \in w(V^c)$ to the point ζ in (5.9). We can now use the conformal automorphism h of $\mathbb{P}^1(\mathbb{C})$ defined by $\nu \to h(\nu) = \frac{1}{\nu-\zeta}$ to send ζ to $h(\zeta) = \infty$ and $H = (\nu \circ w)(V^c)$ to the complement in $\mathbb{P}^1(\mathbb{C})$ of a closed disk D which has a diameter going from $0 = h(\infty)$ to $\frac{i}{\mathrm{Im}(\zeta)} = h(\mathrm{Re}(\zeta))$. This is illustrated in Figure 2.

Consider now the composition $f(z) = c \cdot (h \circ \nu \circ w)$, where c is a non-zero constant we will choose so that $\lim_{z\to\infty} f(z)/z = 1$. This f gives a conformal map from V^c to the complement of the image cD of D by multiplication by c. Therefore Lemma 5.6 gives

$$\gamma_\infty(V) = \gamma_\infty(D) = \frac{|c|}{2\mathrm{Im}(\zeta)} \tag{5.11}$$

Figure 1: Constructing the first conformal map.

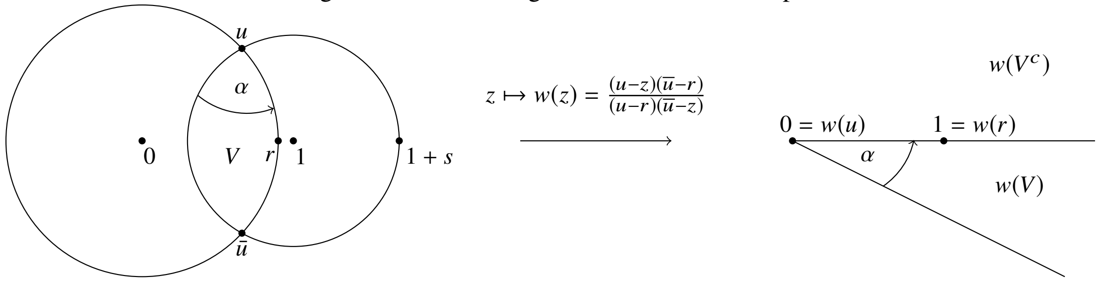
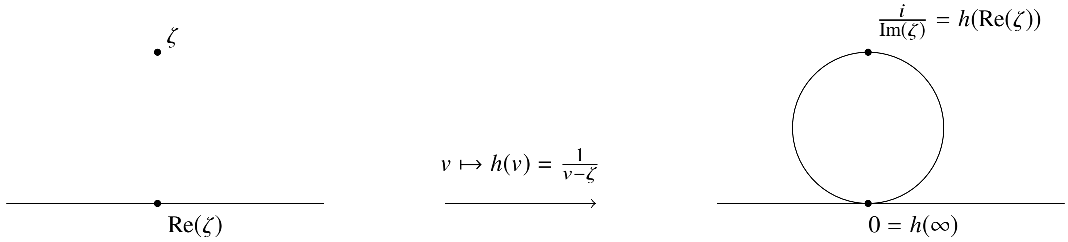


Figure 2: Constructing the third conformal map.



It just remains to find c. Here

$$1/h(\nu(w(z))) = \nu(w(z)) - \nu(w(\infty)) = \left(\frac{(u-z)(\overline{u}-r)}{(u-r)(\overline{u}-z)}\right)^{\pi/(2\pi-\alpha)} - \left(\frac{(\overline{u}-r)}{(u-r)}\right)^{\pi/(2\pi-\alpha)}.$$

Thus

$$z/h(\nu(w(z))) = \zeta \cdot z \cdot \left(\left(\frac{(1-z^{-1}u)}{(1-z^{-1}\overline{u})}\right)^{\pi/(2\pi-\alpha)} - 1\right)$$

since $\zeta = \left(\frac{(\overline{u}-r)}{(u-r)}\right)^{\pi/(2\pi-\alpha)}$. Using that

$$(1-z^{-1}u)/(1-z^{-1}\overline{u}) = 1 + (\overline{u}-u)z^{-1} + \text{higher order terms}$$

we find that on setting

$$c = \lim_{z\to\infty} z/h(\nu(w(z))) = \zeta \cdot \frac{\pi}{2\pi-\alpha} \cdot (\overline{u}-u)$$

we will have $\lim_{z\to\infty} f(z)/z = \lim_{z\to\infty} c \cdot h(\nu(w(z)))/z = 1$, as required. Now (5.11) gives

$$\gamma_\infty(V) = \frac{1}{2\mathrm{Im}(\zeta)} \cdot \frac{\pi}{2\pi-\alpha} \cdot |\overline{u}-u|$$

as claimed in Theorem 5.5 since $|\zeta| = 1$.

Remark 5.7. As a check on Theorem 5.5, consider the case in which s tends toward $1 + r$ from below. Then V becomes closer and closer to being all of $D(0, r)$, and some straightforward estimates show that the formula $\gamma_\infty(V)$ in Theorem 5.5 tends toward $\gamma_\infty(D(0, r)) = r$ as $s \to (1 + r)$ from below.

Example 5.8. Suppose $s = r = 1$. Let $\tau = e^{2\pi i/3}$. Then $u = -\tau^2$, $\overline{u} = -\tau$ and $\alpha = 2\pi/3$. One has

$$\zeta = \left(\frac{\overline{u}-r}{u-r}\right)^{\pi/(2\pi-\alpha)} = \left(\frac{1+\tau^2}{1+\tau}\right)^{3/4} = \sqrt{-1}.$$

Thus

$$\gamma_\infty(V) = \frac{1}{2} \cdot \frac{3}{4}|\tau^2 - \tau| = \frac{3\sqrt{3}}{8} = 0.6495...$$

For all $Y > 0$ one thus has

$$\gamma(Y \cdot V) = \frac{3\sqrt{3}Y}{8}.$$

Example 5.9. We now illustrate the use of the above results when F is an imaginary quadratic field, which we will regard as a subset of $\mathbb{C}$ via a choice of complex embedding. Suppose $aO_F + tO_F = O_F$ and that a and t are non-zero. Let q be a rational prime such that $3|a| < q$, where $|a|$ is the complex absolute value of a. Suppose $X \le |a|$ and $Y = X/|t|$. We first check that

$$g_1(\mathrm{x},\mathrm{y}) = \frac{\mathrm{x} + t\mathrm{y} + a}{q} \in F[\mathrm{x},\mathrm{y}]$$

vanishes on every pair of $x, y \in \overline{\mathbb{Z}}$ such that $g(x,y) = x + ty + a \equiv 0 \bmod q\overline{\mathbb{Z}}$ and $|x'| \le X$ and $|y'| \le Y$ for all conjugates x' of x and y' of y. This follows from the fact that $g_1(x,y) \in \overline{\mathbb{Z}}$ and

$$|g_1(x', y')| = \frac{|x' + ty' + a|}{q} \le \frac{|x'| + |ty'| + |a|}{q} \le \frac{X + |t|Y + |a|}{q} \le \frac{3|a|}{q} < 1$$

for all x' and y' as above. Thus we can use $g_1(\mathrm{x},\mathrm{y})$ in Definition 5.1, so $b_1 = 1/q$, $b_2 = t/q$ and $b_3 = a/q$. For finite places v of F, Definition 5.1 says E_v is the set of $y \in \overline{F}_v$ such that $|y|_v \le 1$, $|b_2 y + b_3|_v \le |b_1|_v$ and $|-(b_2 y + b_3)/b_1 + ty + a|_v \le |\mathcal{J}|_v$. Here $-(b_2 y + b_3)/b_1 + ty + a = 0$ and $|b_2 y + b_3|_v \le |b_1|_v$ is equivalent to $|ty + a|_v \le 1$, which holds whenever $|y|_v \le 1$ since $a, t \in O_F$. Thus $E_v = \{y \in \overline{F}_v : |y|_v \le 1\}$ is the v-adic unit disc with local capacity $\gamma_v(E_v) = 1$ for all finite v. When v_∞ is the unique infinite place of F, $|\ |_{v_\infty}$ is the usual Euclidean absolute on $\overline{F}_v = \mathbb{C}$. In this case, Definition 5.1 says E_{v_∞} is the set of $y \in \overline{F}_v$ such that $|y|_v \le Y$ and $|b_2 y + b_3| \le |b_1| \cdot X$. The second inequality is equivalent to $|ty + a| \le X$ which is equivalent to $|y - (a/t)| \le X/|t| = Y$. Thus E_{v_∞} is the intersection of the closed disc $D(0, Y)$ of radius Y about the origin with the closed disc $D(a/t, Y)$ of radius Y around a/t. Here $|a/t| = X/|t| = Y$ by our choices of X and Y, so E_{v_∞} is a rotation about the origin of the set $Y \cdot V$ dscussed at the end of Example 5.8. Thus that example and Lemma 5.2 shows that the capacity of $\mathcal{E} = \prod_v E_v$ is

$$\gamma(\mathcal{E}) = \prod_v \gamma_v(E_v) = \gamma_{v_\infty}(E_{v_\infty}) = \frac{3\sqrt{3}Y}{8}.$$

This computation and Theorem 5.4 show Theorem 1.5.

We end this section by showing the claim made in the last sentence of the introduction that there are infinitely many examples of each of cases 1 and 2 of Theorem 1.4. We prove a more quantitative result under some additional hypotheses.

Theorem 5.10. *Suppose $F = \mathbb{Q}$, so that $O_F = \mathbb{Z}$. Suppose $\mathcal{J} = p\mathbb{Z}$ for some prime p, and that $X = Y = c\sqrt{p} > 1/3$ for some fixed constant c for which $2/3 > c > 0$.*

i. For sufficiently large primes p there is a positive proportion of pairs $(t, a) \in (\mathbb{Z}/p)^* \times (\mathbb{Z}/p)$ for which the following is true. There is a unique polynomial $g_1(\mathrm{x},\mathrm{y}) = b_1\mathrm{x} + b_2\mathrm{y} + b_3 = (d_1\mathrm{x} + d_2\mathrm{y} + d_3)/p$ with the properties in Theorem 4.1 for which $d_i \in \mathbb{Z}$ for $i = 1, 2, 3$ and $\gcd(d_1, d_2) = 1$ and $d_1 > 0$. Alternative (1) of Theorem 5.4 holds for this $g_1(\mathrm{x},\mathrm{y})$.

ii. For sufficiently large primes p there is a positive proportion of pairs $(t, a) \in (\mathbb{Z}/p)^* \times (\mathbb{Z}/p)$, all the statements in (i) up to the last one are true, but now alternative (2) of Theorem 5.4 holds.

In this result, the condition that $X = Y = c\sqrt{p}$ with $2/3 > c > 0$ is natural in view of the fact that Coppersmith's method should heuristically apply once $XY < p$. Part (i) of Theorem 5.10 shows this heuristic fails for a positive proportion of cases, while part (ii) shows it holds for a positive proportion.

We now describe the strategy of the proof. Rather than begin by choosing (t, a), we instead choose polynomials $b_1\mathrm{x} + b_2\mathrm{y} + b_3 = (d_1\mathrm{x} + d_2\mathrm{y} + d_3)/p$ that will have the properties in Lemma 5.11 for some pair of residue classes t and a mod $p\mathbb{Z}$. In Lemma 5.11 we specify conditions on the d_i which ensure the uniqueness of the associated pair (t, a) mod $p\mathbb{Z}$. In Lemma 5.12 we show that for the t and a which arise from the construction in Lemma 5.11, any polynomial with the properties in Theorem 4.1 for t and a must arise from an integer multiple of the polynomial in Lemma 5.11 that gives rise to t and a. These steps are needed because in the end we will count the polynomials produced in Lemma 5.11 which lead to the capacity $\gamma(\mathcal{E})$ associated to the triple $\{b_1\mathrm{x} + b_2\mathrm{y} + b_3, t, a\}$ in Definition 5.1 and Lemma 5.2 being greater than 1 (respectively less than 1). We compute these capacities in Lemma 5.13. To complete the proof of Theorem 5.10 we then produce ranges for d_1, d_2 and d_3 which lead to $\gamma(\mathcal{E}) > 1$ (respectively $\gamma(\mathcal{E}) < 1$). We show that these ranges lead to positive proportion of the possible residue classes of (t, a) mod p satisfying conditions (i) (resp. (ii)) of Theorem 5.10.

Lemma 5.11. *Recall that $2/3 > c > 0$, so $0 < 3c/2 < 1$. Let w, z be real numbers such that $0 < w \leq 2$ and $0 \leq z < 1$. Consider the set $S(w,z)$ of all triples (d_1, d_2, d_3) of integers such that*

$$w \cdot 3c\sqrt{p}/4 \leq d_1 \leq 3c\sqrt{p}/2 < \sqrt{p}; \quad 1 \leq d_2 \leq 3c\sqrt{p}/2 < \sqrt{p}; \quad 0 \leq d_3 < zp \quad \text{and} \quad \gcd(d_1, d_2) = 1. \tag{5.12}$$

There is an injective map $\lambda : S(w,z) \to \mathbb{Z}/p \times \mathbb{Z}/p$ which sends (d_1, d_2, d_3) to the class in $\mathbb{Z}/p \times \mathbb{Z}/p$ of (t, a) when t and a are the smallest non-negative integers for which $d_1 \cdot (1, t, a) \equiv (d_1, d_2, d_3)$ mod p. One has $t \not\equiv 0$ mod p and $d_1 \not\equiv 0$ mod p.

Proof. Suppose $(d_1, d_2, d_3) \in S(w,z)$. Since $0 < w \cdot 3c/2 < w$ we have $d_1 \not\equiv 0$ mod p and $d_2 \not\equiv 0$ mod p. Hence t and a are uniquely determined by (d_1, d_2, d_3) and $t \not\equiv 0$ mod p. Suppose $\lambda(d_1, d_2, d_3) = \lambda(d_1', d_2', d_3')$ for some $(d_1', d_2', d_3') \in S(w,z)$. Then $d_2 \equiv td_1$ mod p and $d_2' \equiv td_1'$ mod p, so $d_2 d_1' - d_2' d_1 \equiv td_1 d_1' - td_1' d_1 \equiv 0$ mod p. But d_1, d_2, d_1', d_2' all lie in the interval $(0, 3c\sqrt{p}/2) \subset (0, \sqrt{p})$, we have $0 < d_2 d_1' < p$ and $0 < d_2' d_1 < p$. So $d_2 d_1' \equiv d_2' d_1$ mod p forces $d_2 d_1' = d_2' d_1$. Now since the d_i are positive and $\gcd(d_1, d_2) = \gcd(d_1', d_2')$, we conclude $(d_1, d_2) = (d_1', d_2')$. Now $d_3 \equiv d_1 a \equiv d_1' a \equiv d_3'$ mod p, so $z < 1$ forces $d_3 = d_3'$. Hence λ is injective. □

Lemma 5.12. *With the notations and assumptions of Lemma 5.11, suppose $\lambda(d_1, d_2, d_3) = (t, a)$ and $z \leq 3wc^2$. Suppose $g_1(\mathrm{x}, \mathrm{y}) = b_1 \mathrm{x} + b_2 \mathrm{y} + b_3 \in \mathbb{Q}[\mathrm{x}, \mathrm{y}]$ has the properties in Theorem 4.1 for t and a. Then $e_1 = pb_1$, $e_2 = pb_2$ and $e_3 = pb_3$ are in $\mathbb{Z}$. Let $q = \gcd(e_1, e_2, e_3)$. Then $b_1 \neq 0$ and*

$$g_1(\mathrm{x}, \mathrm{y}) = \mathrm{sign}(b_1) \cdot q \cdot (d_1 \mathrm{x} + d_2 \mathrm{y} + d_3)/p.$$

Furthermore, $(d_1 \mathrm{x} + d_2 \mathrm{y} + d_3)/p$ also has all the properties in Theorem 4.1 for t and a.

Proof. By Theorem 4.1, $0 \neq pg_1(\mathrm{x}, \mathrm{y}) = e_1 \mathrm{x} + e_2 \mathrm{y} + e_3 \in \mathbb{Z}[\mathrm{x}, \mathrm{y}]$ has $e_1 \mathrm{x} + e_2 \mathrm{y} + e_3 \equiv e_1(\mathrm{x} + t\mathrm{y} + a)$ mod $p\mathbb{Z}[\mathrm{x}, \mathrm{y}]$, so $(e_1, e_2, e_3) \equiv e_1(1, t, a)$ mod p. Furthermore,

$$0 < |e_1| < p/(3X) = \sqrt{p}/(3c); \quad |e_2| < p/(3Y) = \sqrt{p}/(3c); \quad \text{and} \quad |e_3| < p/3. \tag{5.13}$$

These properties are preserved if we divide $g_1(\mathrm{x}, \mathrm{y})$ by the g.c.d. of e_1, e_2 and e_3 or if we multiply $g_1(\mathrm{x}, \mathrm{y})$ by -1. We will assume in what follows that this has been done, so that $\gcd(e_1, e_2, e_3) = 1$ and $e_1 > 0$.

Since $\lambda(d_1, d_2, d_3) = (t, a)$, we have $d_1(1, t, a) \equiv (d_1, d_2, d_3)$ mod p. Since $(e_1, e_2, e_3) \equiv e_1(1, t, a)$ mod p we conclude $e_1 d_2 - d_1 e_2 \equiv 0$ mod p. However,

$$|e_1 d_2 - d_1 e_2| < p$$

since $|e_i| < \sqrt{p}/(3c)$ and $|d_i| \leq 3c\sqrt{p}/2$ for $i = 1, 2$. Hence $e_1 d_2 - d_1 e_2 = 0$. Since $\gcd(d_1, d_2) = 1$, this forces $(e_1, e_2) = e(d_1, d_2)$ for some $e \in \mathbb{Z}$. Now $w3c/2\sqrt{p} \leq d_1$ so $|e|w3c\sqrt{p}/2 \leq |ed_1| = |e_1| < \sqrt{p}/(3c)$ because of (5.13). So

$$|e| < \frac{2}{(3c)^2 w}. \tag{5.14}$$

Since $d_1 \not\equiv 0$ mod p, $d_1 d_1' \equiv 1$ mod p for some integer d_1'. Therefore

$$(ed_1, ed_2, e_3) = (e_1, e_2, e_3) \equiv e_1(1, t, a) \equiv e_1 d_1'(d_1, d_2, d_3) \quad \text{mod } p.$$

So $e \equiv e_1 d_1'$ mod p and $e_3 \equiv e_1 d_1' d_3 \equiv ed_3$ mod p. Thus $(e_1, e_2, e_3) - e(d_1, d_2, d_3) \equiv (0, 0, 0)$ mod p, where $e_1 = ed_1$ and $e_2 = ed_2$. We conclude that

$$pg_1(\mathrm{x}, \mathrm{y}) = e_1 \mathrm{x} + e_2 \mathrm{y} + e_3 = e(d_1 \mathrm{x} + d_2 \mathrm{y} + d_3) + h$$

when $h = e_3 - ed_3 \equiv 0$ mod p. Here

$$|ed_3| = |e| \cdot |d_3| < \frac{2zp}{(3c)^2 w} \leq 2p/3$$

because of (5.14), $|d_3| < zp$ and the assumption that $z \leq w3c^2$. Since $|e_3| < p/3$ we get $|h| = |e_3 - ed_3| < p/3 + 2p/3 < p$, which forces $h = 0$ since $h \equiv 0$ mod p. Thus $pg_1(\mathrm{x}, \mathrm{y}) = e_1 \mathrm{x} + e_2 \mathrm{y} + e_3 = e(d_1 \mathrm{x} + d_2 \mathrm{y} + d_3)$. Since $\gcd(e_1, e_2, e_3) = 1$ and e_1 and d_1 are positive, we must have $e = 1$ and $g_1(\mathrm{x}, \mathrm{y}) = (d_1 \mathrm{x} + d_2 \mathrm{y} + d_3)/p$. □

Lemma 5.13. *Let $\mathcal{E} = \prod_v E_v$ be the adelic set associated by Definition 5.1 to $g_1(\mathrm{x}, \mathrm{y}) = \frac{1}{p}(d_1 \mathrm{x} + d_2 \mathrm{y} + d_3)$ for some $(d_1, d_2, d_3) \in S(w,z)$ under the assumption that $z \leq 3wc^2$ in Lemma 5.12. Define*

$$\delta_1 = \max(-c, \frac{-d_1 c}{d_2} - \frac{d_3}{\sqrt{p} d_2}) \quad \text{and} \quad \delta_2 = \min(c, \frac{d_1 c}{d_2} - \frac{d_3}{\sqrt{p} d_2}) \tag{5.15}$$

Suppose d_1 and d_2 are relatively prime. The capacity $\gamma(\mathcal{E})$ of $\mathcal{E}$ is 0 if $\delta_1 > \delta_2$. Otherwise,

$$\gamma(\mathcal{E}) = \prod_v \gamma_v(E_v) = d_1^{-1}\gamma_\infty(E_\infty) \geq \frac{\sqrt{p}(\delta_2 - \delta_1)}{4d_1} \tag{5.16}$$

where E_∞ is the component of $\mathcal{E}$ at the archimedean place of $\mathbb{Q}$.

Proof. From Definition 5.1, the intersection of the real line with E_∞ is trivial if $\delta_1 > \delta_2$, in which case E_∞ is empty and $\gamma_\infty(E_\infty) = 0 = \gamma(\mathcal{E})$. If $\delta_1 \leq \delta_2$ then E_∞ intersects the real line in the interval $[\sqrt{p}\delta_1, \sqrt{p}\delta_2]$. In this case, we have

$$\gamma_\infty(E_\infty) \geq \gamma_\infty([\sqrt{p}\delta_1, \sqrt{p}\delta_2]) = \frac{\sqrt{p}}{4}(\delta_2 - \delta_1). \tag{5.17}$$

Suppose now that v is a finite place of $\mathbb{Q}$. From Definition 5.1 and the equality $b_1\mathrm{x}+b_2\mathrm{y}+b_3 = p^{-1}(d_1\mathrm{x}+d_2\mathrm{y}+d_3)$, we see that E_v is the set of $y \in \overline{\mathbb{Q}}_v$ satisfying these conditions:

i. $|y|_v \leq 1$

ii. $|(d_2y + d_3)/d_1|_v \leq 1$ and

iii. $|-(d_2y + d_3)/d_1 + ty + a|_v \leq |\mathcal{J}|_v$

where $|\mathcal{J}|_v = 1$ if $v \neq p$ and $|\mathcal{J}|_p = p^{-1}$. Let us first show (i) and (ii) imply (iii). If $v \neq p$, this is clear from $t, a \in \mathbb{Z}$. Suppose now that $v = p$. We know d_1 is prime to p, and that $(d_1, d_2, d_3) \equiv d_1(1, t, a) \bmod p$. So $d_2 \equiv d_1 t \bmod p$ and $d_3 \equiv d_1 a \bmod p$. Thus

$$|(-d_2/d_1 + t)y|_v = |d_1|_v^{-1} \cdot |-d_2 + td_1|_v \cdot |y|_v \leq p^{-1} \quad \text{if} \quad |y|_v \leq 1$$

and

$$|-d_3/d_1 + a|_v = |d_1|^{-1} \cdot |-d_3 + ad_1|_v \leq p^{-1} \quad \text{if} \quad |y|_v \leq 1$$

so (iii) is implied by (i) when $v = p$. Thus E_v is the set of $y \in \overline{\mathbb{Q}}_v$ satisfying (i) and (ii).

Recall now that d_1, d_2, d_3 are non-zero integers and that by assumption $\gcd(d_1, d_2) = 1$. Thus if $|d_1|_v < 1$ then $|d_2|_v = 1$, and otherwise $|d_1|_v = 1$. If $|d_1|_v = 1$, then (i) implies $|(d_2y + d_3)/d_1|_v = |d_2y + d_3|_v \leq 1$, so (ii) holds. If $|d_1|_v < 1$, then $|d_2|_v = 1$ so (ii) is equivalent to $|y - (-d_3/d_2)|_v \leq |d_1/d_2|_v = |d_1|_v < 1$. Since $|-d_3/d_2|_v = |-d_3|_v \leq 1$, condition (ii) implies (i) if $|d_1|_v < 1$. We thus find that for all finite v, E_v is a v-adic disc of radius $r_v = |d_1|_v$ around point of $\mathbb{Q}$.

We can now calculate the capacity of $\mathcal{E} = \prod_v E_v$. The product of the local capacities at finite places is

$$\prod_{v \text{ finite}} \gamma_v(E_v) = \prod_{v \text{ finite}} r_v = \prod_{v \text{ finite}} |d_1|_v = d_1^{-1}$$

by the product formula since d_1 is a positive integer. We thus find as in Lemma 5.2 and (5.17) that

$$\gamma(\mathcal{E}) = \prod_v \gamma_v(E_v) = d_1^{-1}\gamma_\infty(E_\infty) \geq \frac{\sqrt{p}(\delta_2 - \delta_1)}{4d_1}.$$

□

Proof of Theorem 5.10

Let $d_1 = 3c\chi_1\sqrt{p}/2$, $d_2 = 3c\chi_2\sqrt{p}/2$ and $d_3 = \chi_3 p$ be as in Lemma 5.12, so that $w \leq \chi_1 \leq 1$, $0 < \chi_2 \leq 1$ and $0 \leq \chi_3 \leq z$. We have supposed $0 < w$, $0 < 3c/2 < 1$, $0 \leq z < 1$ and $z \leq 3wc^2$. For $i = 1, 2$ let

$$z_i(\chi_1, \chi_2, \chi_3) = \frac{1}{6c\chi_1} \cdot \left(\frac{(-1)^i\chi_1 c}{\chi_2} - \frac{2\chi_3}{3c\chi_2}\right) = \frac{(-1)^i c}{6c\chi_2} - \frac{\chi_3}{9c^2\chi_1\chi_2}.$$

Then

$$\frac{\sqrt{p}}{4d_1}\delta_2 = \frac{\delta_2}{6c\chi_1} = \min\left(\frac{c}{6c\chi_1}, z_2(\chi_1, \chi_2, \chi_3)\right) = \min\left(\frac{1}{6\chi_1}, \frac{1}{6\chi_2} - \frac{\chi_3}{9c^2\chi_1\chi_2}\right) \tag{5.18}$$

$$\frac{\sqrt{p}}{4d_1}\delta_1 = \frac{\delta_1}{6c\chi_1} = \max\left(-\frac{c}{6c\chi_1}, z_1(\chi_1, \chi_2, \chi_3)\right) = \max\left(\frac{-1}{6\chi_1}, \frac{-1}{6\chi_2} - \frac{\chi_3}{9c^2\chi_1\chi_2}\right) \tag{5.19}$$

Suppose we let $w = 1/24$ and $z = 9c^2/(24)^2 < 9(2/3)^2/(24)^2 < 1$. Then $z \leq 3wc^2 = c^2/8$, so all conditions on c, w and z are satisfied. Suppose χ_1, χ_2 are in the interval $[1/24, 1/12]$ and χ_3 is in the interval $[0, z]$. Then

$$\frac{\sqrt{p}}{4d_1}\delta_2 = \min\left(\frac{1}{6\chi_1}, \frac{1}{6\chi_2} - \frac{\chi_3}{9c^2\chi_1\chi_2}\right) \geq \min(2, 2 - 1) \geq 1.$$

Since $\frac{\sqrt{p}}{4d_1}\delta_1 < 0$, we will then have

$$\gamma((E)) \geq \frac{\sqrt{p}(\delta_2 - \delta_1)}{4d_1} > 1.$$

Suppose I_1 and I_2 are intervals on the non-negative real axis of lengths $q_1, q_2 > 0$. By a sieving argument, as $r \to +\infty$, the number of coprime integers (d_1, d_2) in a product $rI_1 \times rI_2$ is asymptotically $r^2 q_1 q_2 \prod_{\ell \text{ prime}}(1 - \ell^{-2}) = r^2 q_1 q_2 6/\pi^2$. Applying this to $I_1 = [w3c\sqrt{p}/2, 3c\sqrt{p}/2]$ and $I_2 = [0, 3c\sqrt{p}/2]$ for $w = 1/12$ as above, we see that as $p \to \infty$, the number of triples $(d_1, d_2, d_3) \in S(w, z)$ that have d_1 and d_2 coprime and $\gamma(\mathcal{E}) > 1$ is bounded below by a positive constant times $\sqrt{p}^2 \cdot p = p^2$. Since the number of elements of $S(w, z)$ grows as a positive constant times p^2, Lemmas 5.11 and 5.12 show that a positive fraction of all pairs $(t, a) \in (\mathbb{Z}/p)^* \times (\mathbb{Z}/p)^*$ lead to $\gamma(\mathcal{E}) > 1$.

To prove that there are a positive proportion of pairs (t, a) such that $\gamma(\mathcal{E}) = 0$, note that (5.18) and (5.19) give

$$\frac{\chi_1\chi_2\delta_2}{6c} \leq \frac{\chi_1}{6} - \frac{\chi_3}{9c^2} \quad \text{and} \quad \frac{\chi_1\chi_2\delta_1}{6c} \geq -\frac{\chi_2}{6}$$

so

$$\frac{\chi_1\chi_2}{6c}(\delta_2 - \delta_1) < \frac{\chi_1}{6} - \frac{\chi_3}{9c^2} + \frac{\chi_2}{6}.$$

The constraints on χ_1, χ_2 and χ_3 are that $w \leq \chi_1 \leq 1$, $0 < \chi_2 \leq 1$ and $0 \leq \chi_3 \leq z$, where $0 < w < 1$, $0 < 3c/2 < 1$, $0 \leq z < 1$ and $z \leq 3wc^2$. We now assume $0 < w < 1/2$. Let $\chi_2 \to 0^+$, $\chi_1 \to w^+$, $\chi_3 \to z^-$ and $z = 3wc^2 < 3c^2/2 < c < 2/3$. Then $\frac{\chi_1}{6} - \frac{\chi_3}{9c^2} + \frac{\chi_2}{6}$ has limit

$$\frac{w}{6} - \frac{z}{9c^2} + 0 = w \cdot (\frac{1}{6} - \frac{3c^2}{9c^2}) = -\frac{w}{6} < 0.$$

Thus taking χ_1, χ_2 and χ_3 near these limits leads (via the same seiving argument used before) to a positive proportion of $(t, a) \in (\mathbb{Z}/p)^* \times (\mathbb{Z}/p)^*$ for which $\delta_2 < \delta_1$. Lemma 5.13 shows $\gamma(\mathcal{E}) = 0$ for such (t, a).

Theorem 5.4, together with the above constructions of a positive proportion of (t, a) with $\gamma(\mathcal{E}) > 1$ and of a positive proportion of (t, a) for which $\gamma(\mathcal{E}) = 0$ now proves Theorem 5.10.

6 BOUNDS ON THE NUMBER OF SOLUTIONS OF PROBLEM 1.1.

We will be concerned with finding upper bounds on the number $N(t, a, \mathcal{J}, X, Y)$ of pairs (x, y) of algebraic integers having the properties in Problem 1.1, where $N(t, a, \mathcal{J}, X, Y)$ may be infinite. This is relevant to the following case of the hidden number problem.

Suppose we are given two pairs (a_1, b_1) and (a_2, b_2) of elements of O_F such that for an unknown secret $s \in O_F$, one has $b_i = sa_i + e_i \bmod \mathcal{J}$ for a small error $e_i \in O_F$. Then $e_2 = b_2 - sa_2 = b_2 - (b_1 - e_1)a_1^{-1}a_2 \bmod \mathcal{J}$. Thus if we let $x = e_2$, $y = e_1$, $t = a_1^{-1}a_2 \bmod \mathcal{J}$ and $a = -b_2 + b_1 a_1^{-1} a_2 \bmod \mathcal{J}$, we wil have $x + ty + a \equiv 0 \bmod \mathcal{J}$ with x and y small. Therefore $N(t, a, \mathcal{J}, X, Y)$ gives a bound on the number of secrets s which can solve this case of the hidden number problem.

To bound $N(t, a, \mathcal{J}, X, Y)$, it is simplest to deal with the case $a = 0$. This gives an upper bound for arbitrary a at the cost of halving the allowed sizes of archimedean conjugates.

Theorem 6.1. *The following is true for all t, $\mathcal{J}$, X and Y.*

1. *When $a = 0$, there are either no (x, y) with the properties in Problem 1.1 or there are infinitely many such (x, y).*
2. *Suppose $a = 0$ and $\gamma(\mathcal{E}) < 1$ in Theorem 5.4. Then there are no (x, y) satisfying the conditions in Problem 1.1, i.e. $N(t, 0, \mathcal{J}, X, Y) = 0$.*
3. *For all a one has $N(t, a, \mathcal{J}, X/2, Y/2) \leq 1 + N(t, 0, \mathcal{J}, X, Y)$. Thus either $N(t, 0, \mathcal{J}, X, Y) = \infty$ or $N(t, 0, \mathcal{J}, X, Y) = 0$ and $N(t, a, \mathcal{J}, X/2, Y/2) \leq 1$.*

Proof. For part (1), observe that if $(x, y) \in \overline{\mathbb{Z}} \times \overline{\mathbb{Z}}$ has the properties in Problem 1.1 when $a = 0$, then so does $(\zeta x, \zeta y)$ for any root of unity ζ. To prove (2), note that Theorem 5.4 shows $N(t, 0, \mathcal{J}, X, Y)$ is finite if $\gamma(\mathcal{E}) < 1$. Then part (1) forces $N(t, 0, \mathcal{J}, X, Y) = 0$. Part (3) follows from the fact that the difference of two solutions (x, y) and (x', y') to Problem 1.1 for given t, a, $\mathcal{J}$, $X/2$ and $Y/2$ is a solution $(x'', y'') = (x' - x, y' - y)$ to Problem 1.1 for t, 0, $\mathcal{J}$, X and Y. □

Remark 6.2. The proof of parts (1) and (2) illustrates the advantages of working over the ring $\overline{\mathbb{Z}}$ of all algebraic integers, rather than in the integers of a particular number field. This makes it possible to promote a finiteness result coming from capacity theory to a proof that a homogenous linear congruence has no small solutions at all. Note that in part (3), we do not obtain any information about $N(t, a, \mathcal{J}, X/2, Y/2)$ for $a \neq 0$ in the event that $N(t, 0, \mathcal{J}, X, Y) = \infty$.

We illustrate this result with a concrete application to the hidden number problem. Suppose as in §1.1 that we are given an ideal $\mathcal{J}$ of the integers O_F of a number field F and a real number X. For a secret integer $s \in O_F$ we are given samples $(c_i, d_i) \in O_F \times O_F$ for $i = 0, 1$ for which c_0 is prime to $\mathcal{J}$ and the following is true. There is an (unknown) element $x_i \in O_F$ such that

$$c_i s - d_i \equiv x_i \mod \mathcal{J} \tag{6.20}$$

and $|\lambda(x_i)| \le X/2$ for all embeddings $\lambda : F \to \mathbb{C}$. We would like to determine s mod $\mathcal{J}$ from this information. Theorem 6.1 leads in the following way to a computable criterion for there to exist at most one solution s mod $\mathcal{J}$.

As in §1.1, we find $c_0' \in O_F$ such that $c_0 c_0' \equiv 1$ mod $\mathcal{J}$. Then (6.20) for $i = 0$ gives

$$s \equiv c_0'(x_0 + d_0) \mod \mathcal{J}.$$

Substituting this into (6.20) when $i = 1$ gives

$$x_1 + t_i x_0 + a_1 \equiv 0 \mod \mathcal{J} \tag{6.21}$$

where $t_1 = -c_1 c_0'$ and $a_1 = d_1 - d + c_1 c_0' d_0$. Thus the problem of finding all s mod $\mathcal{J}$ satsifying the above conditions is converted to finding all solutions $(x_0, x_1) \in O_F \times O_F$ of the congruence (6.21) such that $|\lambda(x_i)| < X/2$ for $i = 0, 1$ and all embeddings $\lambda : F \to \mathbb{C}$.

We bound the number of solutions s mod $\mathcal{J}$ in the following way. Using lattice basis reduction, find a polynomial $b_1\mathrm{x} + b_2\mathrm{y} + b_3 \in \mathcal{J}^{-1}O_F[\mathrm{x}, \mathrm{y}]$ with the properties in Theorem 4.1 for $Y = X$, $t = -c_1 c_0'$ and $a = 0$. Calculate the capacity $\gamma(\mathcal{E})$ of the adelic set $\mathcal{E}$ associated to this adelic set in Definition 5.1, using Lemma 5.2 and Theorem 5.5. If $\gamma(\mathcal{E}) < 1$, then parts (2) and (3) of Theorem 6.1 show $N(t, a, \mathcal{J}, X/2, X/2) \le 1$. Thus there is at most one pair (x_0, x_1) as above, and at most one integer s mod $\mathcal{J}$ which solves the above case of the hidden number problem.

We conclude this paper with another example illustrating Theorem 6.1. Suppose $a = 0$, $t \in O_F$ and that $\mathcal{J} = O_F\alpha$ is a non-zero principal ideal of O_F. Suppose $(x_0, y_0) \in O_F$ satisfy the congruence

$$x_0 + t y_0 \equiv 0 \mod \mathcal{J} \tag{6.22}$$

and that

$$|x_0 \cdot y_0|_v \le |\alpha|_v/2 \quad \text{for all} \quad v \in M_{F,\mathrm{inf}}. \tag{6.23}$$

Suppose as before that t is prime to $\mathcal{J} = O_F\alpha$, and that x_0, y_0 and α are pairwise relatively prime, in the sense that the ideal generated by any two of them is O_F.

Theorem 6.3. *With the above hypotheses, there are no non-zero pairs $(x, y) \in \overline{\mathbb{Z}} \times \overline{\mathbb{Z}}$ with the following properties:*

1. *$x + ty \equiv 0$ mod $\mathcal{J} \cdot \overline{\mathbb{Z}}$, and*
2. *For all embeddings $\lambda : \overline{\mathbb{Z}} \to \mathbb{C}$, one has*

$$|\lambda(x)| \le |\lambda(x_0)| \quad \text{and} \quad |\lambda(y)| \le |\lambda(y_0)|$$

with at least one of these inequalities being strict for at least one λ.

Thus in a small non-zero solution of the homogenous congruence resulting from setting $a = 0$ prevents the existence of non-trivial solutions with smaller archimedean absolute values. Concerning the relation of the inequality (6.23) to Problem 1.1, note that if $0 < \alpha \in \mathbb{Z}$, then (6.23) follows from requiring $|x_0|_v \le X$ and $|y_0| \le Y$ for some real X, Y such that $|XY| \le \alpha/2$.

Proof of Theorem 6.3

Define a polynomial in the variables x and y by

$$b_1\mathrm{x} + b_2\mathrm{y} = (y_0\mathrm{x} - x_0\mathrm{y})/\alpha. \tag{6.24}$$

Hypothesis (6.22) shows $x_0 + t y_0 = \alpha z_0$ for some $z_0 \in O_F$. Therefore

$$b_1\mathrm{x} + b_2\mathrm{y} = y_0(\mathrm{x} + t\mathrm{y})/\alpha - z_0\mathrm{y} \in \mathcal{J}^{-1} \cdot (\mathrm{x} + t\mathrm{y}) + O_F \cdot \mathrm{y}. \tag{6.25}$$

We now substitute for the variables x and y a pair of elements of $\overline{\mathbb{Z}}$ satisfying conditions (1) and (2) of Theorem 6.3. The inequalities in condition (2) of Theorem 6.3 show that for each embedding $\lambda : \overline{\mathbb{Z}} \to \mathbb{C}$ we have

$$|\lambda(b_1 x + b_2 y)| = |\lambda(\frac{y_0 x - x_0 y}{\alpha})| \le |\frac{\lambda(y_0)\lambda(x)}{\alpha}| + |\frac{\lambda(x_0)\lambda(y)}{\alpha}|. \tag{6.26}$$

Now (6.23) gives

$$|\frac{\lambda(y_0)}{\alpha}| \le \frac{1}{2|\lambda(x_0)|} \quad \text{and} \quad \frac{|\lambda(x_0)|}{\alpha} \le \frac{1}{2|\lambda(y_0)|}.$$

Substituting this into (6.26) gives

$$|\lambda(b_1 x + b_2 y)| \le \frac{|\lambda(x)|}{2|\lambda(x_0)|} + \frac{|\lambda(y)|}{2|\lambda(y_0)|}.$$

Hypothesis (2) of Theorem 6.3 now implies $|\lambda(b_1 x + b_2 y)| \le 1$ with strict inequality for at least one λ. Since $b_1 x + b_2 y$ is an algebraic integer, we conclude that

$$b_1 x + b_2 y = 0 \quad \text{when} \quad b_1 = y_0/\alpha \quad \text{and} \quad b_2 = -x_0/\alpha. \tag{6.27}$$

We enlarge F so that it includes x and y. There is then an archimedean place v_∞ of F at which either $|x|_{v_\infty} < |x_0|_{v_\infty}$ or $|y|_{v_\infty} < |y_0|_{v_\infty}$. For simplicity we will suppose that $r_{v_\infty} = |y|_{v_\infty}/|y_0|_{v_\infty} < 1$, the other case being similar. Define $r_v = 1$ if $v_\infty \ne v \in M_{F,\mathrm{inf}}$.

We now define an adelic set $\mathcal{E} = \prod_{v\in M_F} E_v$ associated to $b_1\mathrm{x} + b_2 y$ in the following way. Set $b_3 = 0$ in Definition 5.1. If $v \in M_{F,\mathrm{fin}}$ is finite, let E_v be as in part (i) of Definition (5.1). If $v \in M_{F,\mathrm{inf}}$ is an infinite place, define

$$E_v = \{y \in \overline{F}_v : |y|_v \le r_v|y_0|_v \quad \text{and} \quad |x|_v = |b_2 y/b_1|_v = |-x_0 y/y_0|_v \le |x_0|_v\} = \{y \in \overline{F}_v : |y|_v \le r_v|y_0|_v\} \tag{6.28}$$

where we have used $r_v \le 1$.

As in the proof of part (2) of Theorem 5.4, if $\gamma(\mathcal{E}) < 1$, then there will be only finitely many pairs $(x, y) \in \overline{\mathbb{Z}} \times \overline{\mathbb{Z}}$ satisfying the conditions in Theorem 6.3 and for which $|y|_v \le r_v|y_0|_v$. Then Theorem 6.1 shows that in fact there are no such pairs, contradicting the hypothesis above that such a pair exists. We conclude that to prove Theorem 6.3 if will suffice to show $\gamma(\mathcal{E}) < 1$.

We first need to describe explicitly the set E_v when $v \in M_{F,\mathrm{fin}}$. From Definition 5.1 and (6.24) we see that E_v is the set of $y \in \overline{F}_v$ satisfying

i. $|y|_v \le 1$
ii. $|-x_0 y/y_0|_v \le 1$ and
iii. $|x_0 y/y_0 + ty|_v \le |\mathcal{J}|_v = |\alpha|_v$.

Let us first show (i) and (ii) imply (iii). If $|\alpha|_v = 1$, this is clear from $t \in O_F$. Suppose now that $|\alpha|_v < 1$. We know y_0 is prime to α, so $|y_0|_v = 1$. We have $(y_0, -x_0) \equiv y_0(1, t) \bmod \mathcal{J}$ by multiplying the first equality in (6.25) by α, so $|x_0 + ty_0|_v \le |\mathcal{J}|_v$. Thus

$$|(x_0/y_0 + t)y|_v = |y_0|_v^{-1} \cdot |x_0 + ty_0|_v \cdot |y|_v \le |\mathcal{J}|_v \quad \text{if} \quad |y|_v \le 1.$$

Therefore (iii) is implied by (i) when $|\alpha|_v$. Thus E_v is the set of $y \in \overline{F}_v$ satisfying (i) and (ii).

Recall now that y_0 and $-x_0$ are coprime elements of O_F by assumption. Thus if $|y_0|_v < 1$ then $|-x_0|_v = 1$, and otherwise $|y_0|_v = 1$. If $|y_0|_v = 1$, then (i) implies $|-x_0 y/y_0|_v = |-x_0 y|_v \le 1$, so (ii) holds. If $|y_0|_v < 1$, then $|-x_0|_v = 1$ so (ii) is equivalent to $|y|_v \le |y_0/(-x_0)|_v = |y_0|_v < 1$. Hence condition (ii) implies (i) if $|y_0|_v < 1$. We thus find that for all finite v, E_v is a v-adic disc of radius $r_v = |y_0|_v$ around $0 \in F_v$. The local capacity of E_v is therefore

$$\gamma_v(E_v) = |y_0|_v^{[F_v:\mathbb{Q}_{p(v)}]} = ||y_0||_v \quad \text{for} \quad v \in M_{F,\mathrm{fin}} \tag{6.29}$$

where $p(v)$ is the residue characteristic of v and $||\ ||_v$ is the normalized valuation at v.

We now consider archimedean $v \in M_{F,\mathrm{inf}}$. From (6.28) we see that E_v is the closed disc around 0 in $\overline{F}_v = \mathbb{C}$ of radius $r_v|y_0|_v$. Thus the local capacity is

$$\gamma_v(E_v) = (r_v|y_0|_v)^{[F_v:\mathbb{R}]} = r_v^{[F_v:\mathbb{R}]}||y_0||_v \quad \text{for} \quad v \in M_{F,\mathrm{inf}}. \tag{6.30}$$

Now (6.29) and (6.30) together with the product formula give the global capacity of $\mathcal{E}$ as

$$\gamma(\mathcal{E}) = \prod_v \gamma_v(E_v) = \prod_{v\in M_{F,\mathrm{inf}}} r_v^{[F_v:\mathbb{R}]} \cdot \prod_{v\in M_F} ||y_0||_v = \prod_{v\in M_{F,\mathrm{inf}}} r_v^{[F_v:\mathbb{R}]} < 1$$

which completes the proof of Theorem 6.3.

REFERENCES

[1] Martin R. Albrecht and Nadia Heninger. *On Bounded Distance Decoding with Predicate: Breaking the "Lattice Barrier" for the Hidden Number Problem*, In: Advances in Cryptology - EUROCRYPT 2021, Part I, volume 12696 of Lecture Notes in Computer Science, Anne Canteaut and François-Xavier Standaert, editors, Zagreb, Croatia, October 17 - 21, 2021, Springer, Heidelberg, Germany, pp. 528–558.

[2] Aurélie Bauer and Antoine Joux, *Toward a Rigorous Variation of Coppersmith's Algorithm on Three Variables*, In: Advances in Cryptology - EUROCRYPT 2007, volume 4515 of Lecture Notes in Computer Science, Moni Naor, editor, Barcelona, Spain, May 20 - 24, 2007, Springer, Berlin Heidelberg New York, pp. 361–378.

[3] Aurélie Bauer, *Vers une généralisation rigoureuse des méthodes de Coppersmith pour la recherche de petites racines de polynômes*, Ph.D. thesis, Université de Versailles Saint-Quentin-en-Yvelines, 2008.

[4] Johannes Blömer and Alexander May, *Low Secret Exponent RSA Revisited*, In: Cryptography and Lattices, CaLC 2001, Providence R. I., U. S. A., March 29 - 30, 2001, Springer, Berlin Heidelberg New York, pp. 4–19.

[5] Dan Boneh and Glenn Durfee, *Cryptanalysis of RSA with Private Key d Less than $N^{0.292}$*, In Advances in Cryptology - EUROCRYPT 1999, Jaques Stern editor, volume 1592 of Lecture Notes in Computer Science, Prague, Czech Republic, May 2 - 6, 1999, Springer, Heidelberg, Germany, pp. 1–11.

[6] Dan Boneh and Ramarathnam Venkatesan. *Hardness of Computing the Most Significant Bits of Secret Keys in Diffie-Hellman and Related Schemes*, In Advances in Cryptology - CRYPTO '96, volume 1109 of Lecture Notes in Computer Science, Neal Koblitz editor, Santa Barbara, CA, USA, August 18 - 22, 1996, Springer, Heidelberg, Germany, pp. 129–142.

[7] David Cantor, *On an extension of the definition of transfinite diameter and some applications*, J. Reine Angew. Math., Vol. 316, 1980, pp. 160–207.

[8] H. Chen, Convergence des polygones de Harder-Narasimhan, Mem. de la Société Mathématique de France, no. 120 (2010).

[9] Ted Chinburg, *Capacity theory on varieties*, Compositio Math. 80 (1991), no. 1, 75–84.

[10] Ted Chinburg, Brett Hemenway, Nadia Heninger and Zachary Scherr, *Cryptographic Applications of Capacity Theory: On the Optimality of Coppersmith's Method for Univariate Polynomials*, Advances in Cryptology - ASIACRYPT 2016, Jung Hee Cheon and Tsuyoshi Takagi, editors, Part 1, Volume 10031 of Lecture Notes in Computer Science, Hanoi, Vietnam, December 4 - 8, 2016, Springer, Heidelberg, Germany, pp. 759–788.

[11] Ted Chinburg, Laurent Moret-Bailly, Georgios Pappas and Martin J. Taylor, *Finite morphisms to projective space and capacity theory*, J. Reine Angew. Math., Vol. 727, 2017, pp. 69–84.

[12] Henry Cohn and Nadia Heninger, *Approximate common divisors via lattices*, In: ANTS X - Proceedings of the Tenth Algorithmic Number Theory Symposium, volume 1 of Open Book Series, Berkeley, CA, 2013, Mathematical Science Publishers, pp. 271–293.

[13] Don Coppersmith, *Small solutions to polynomial equations, and low exponent RSA vulnerabilities*, J. Cryptology, 10(4), September 1997, pp. 233–260.

[14] Don Coppersmith, *Finding Small Solutions to Small Degree Polynomials* In: Cryptography and Lattices, J. Silverman editor, Springer Berlin Heidelberg, 2001, pp. 20–31.

[15] Robin Hartshorne, *Algebraic Geometry*, Graduate Texts in Mathematics vol. 52, Springer, 1977.

[16] Nicholas Howgrave-Graham, *Finding small roots of univariate modular equations revisited*, In: Cryptography and Coding, Michael Darnell editor, Springer Berlin Heidelberg, 1997, pp. 131–142.

[17] Nicholas Howgrave-Graham, *Approximate Integer Common Divisors*, In: Cryptography and Lattices, Joseph Silverman editor, Springer Berlin Heidelberg, 2001, pp. 51–66.

[18] Serge Lang, *Algebraic Number Theory*, Springer Graduate Texts in Mathematics, vol. 110, second edition, Springer-Verlag, New York, 1994.

[19] Chi Fong Lau, Robert Rumely and Robert Varley, *Existence of the sectional capacity*, Mem. Amer. Math. Soc. 145 (2000), no. 690, viii+130 pp.

[20] Vadim Lyubashevsky, Chris Peikert and Oded Regev, *On Ideal Lattices and Learning with Errors over Rings*, In: Advances in Cryptology - EUROCRYPT 2010, Henri Gilbert editor, volume 611- of Lecture Notes in Computer Science, French Riveira, May 30 - June 3, 2010, Springer, Heidelberg, Germany, pp. 1–23.

[21] Alexander May, *Using LLL-reduction for solving RSA and factorization problems*. In: Nguyen, P., Vallee, B. (eds.) The LLL Algorithm. Information Security and Cryptography. Springer, Berlin (2009), pp. 315–348.

[22] Alexander May, Julian Nowakowski and Santanu Sarkar, *Approximate Divisor Multiples - Factoring with Only a Third of the Secret CRT-Exponents*, In: Advances in Cryptology EUROCRYPT 2022, Trondheim, Norway, May 30 - June 3, 2022, Proceedings, Part III, Orr Dunkelman and Stefan Dziembowski editors, Lecture Notes in Computer Science 13277, Springer, Berlin Heidelberg New York, pp. 147–167.

[23] Alexander May and Maike Ritzenhofen, *Solving Systems of Modular Equations in One Variable: How Many RSA-encrypted Messages Does Eve Need to Know?* In: Public Key Cryptogaphy - PKC 2008, Proceedings of the 11^{th} International Workshop on Practice and Theory in Public Key Cryptography, Ronald Cramer editor, Barcelona, Spain, March 9 - 12, 2008, Lecture Notes in Computer Science vol. 4939, Springer, Berlin Heidelberg New York, pp. 37–46.

[24] Stephen D. Miller, Bhargav Narayanan and Ramarathnam Venkatesan, *Coppersmith's lattices and "focus groups": an attack on small-exponent RSA*, J. Number Theory 222 (2021), pp. 376–392.

[25] Robert Rumely, *Capacity theory on algebraic curves*, volume 1378 of Lecture Notes in Mathematics, Springer-Verlag, Berlin, 1989.

[26] Pierre Samuel, *Algebraic Theory of Numbers*, Hermann, 1970.

[27] Marten van Dijk, Craig Gentry, Shai Halevi and Vinod Vaikuntanathan, *Fully Homomorphic Encryption over the Integers*, In: Advances in Cryptology - EUROCRYPT 2010, Henri Gilbert, editor, volume 6110 of Lecture Notes in Computer Science, French Riviera, May 30 - June 3, 2010, Springer, Heidelberg, Germany, pp. 24–43.