CLASS GROUP CRYPTOGRAPHY

SARAH FUJIMORI

ABSTRACT. In this paper, we will cover background related to class groups of quadratic fields and explore how they can be used as the basis for cryptosystems. We then describe the discrete logarithm problem in class groups of imaginary quadratic fields and what conditions on the discriminant are required for the problem to be intractable. This paper assumes basic knowledge of abstract algebra and cryptography, and is dedicated to Kevin Xu for his excellent moral support.

1. BACKGROUND

We begin by defining several key terms relating to fields.

Definition 1.1. A **field extension** of a field K is a field E of which K is a subfield (i.e. a subset of E which is a field under the operations in E restricted to K). We write $K \subseteq E$ when E is a field extension of K.

Example. $\mathbb{Q}(i) = \{a + bi : a, b \in \mathbb{Q}\}$ is a field extension of the field of rational numbers of $\mathbb{Q}$.

Note that a field extension can be considered a vector space over K. Considering this way of viewing a field extension, we can then define a measure of how "large" the field is:

Definition 1.2. The **degree** $[E : K]$ of a field extension E of a field K is its dimension as a vector space over K.

Example. For our previous example, $[\mathbb{Q}(i) : \mathbb{Q}] = 2$ because $\{1, i\}$ is a basis for $\mathbb{Q}(i)$ and has cardinality 2.

In this paper, we will consider number fields, which are defined as follows:

Definition 1.3. An **algebraic number field**, or **number field**, is a finite degree field extension of $\mathbb{Q}$.

Example. Some of the most common examples of number fields are $\mathbb{Q}$ itself and the quadratic field $\mathbb{Q}(\sqrt{d}) = a\sqrt{d} + b : a, b \in \mathbb{Q}$ where d is squarefree.

We will build the class group from structures called ideals:

Definition 1.4. An **ideal** of a ring R is a subgroup I of $(R, +)$ such that for all $y \in R$, $x \in I \implies xy, yx \in I$.

Example. Taking our ring R to be $\mathbb{Z}$, let $I = k\,\mathbb{Z}$, where k is a prime. We can see that I is a group under addition and is therefore a subgroup of $(\mathbb{Z}, +)$, and we can see that I is an ideal as well because for all $n \in \mathbb{Z}$, $kn = nk$ is a multiple of k and is therefore in I.

Definition 1.5. For a domain R, define an equivalence relation on $R \times (R \backslash \{0\})$ as $(x_1, y_1) \sim (x_2, y_2)$ iff $x_1 y_2 = x_2 y_1$. The set of equivalence classes is a field and is called the **field of fractions** or **quotient field**.

Example. The definition of the field of fractions is a generalization of the rational numbers; we can see that the field of fractions of $\mathbb{Z}$ is $\mathbb{Q}$.

Conversely, for an algebraic number field K, we can define its ring of integers:

Definition 1.6. Let a be an element of a number field K. Its **minimal monic polynomial** over $\mathbb{Q}$ is the monic polynomial of minimal degree with coefficients in $\mathbb{Q}$, with a as a root.

Example. Let K be any number field, and let $a \in \mathbb{Z}$. The minimal monic polynomial of a is $x - a$.

Example. Let $K = \mathbb{Q}(i)$, and let $a = 2i + 3$. Its minimal monic polynomial over $\mathbb{Q}$ is $(x-\overline{a})(x-a) = (x-(2i+3))(x-(-2i+3)) = x^2 - 6x + 13$, since it has rational coefficients.

Definition 1.7. An element a of a number field K is called **integral** if its minimal monic polynomial over $\mathbb{Q}$ has coefficients in $\mathbb{Z}$. We then call the ring of integral elements the **ring of integers** of K, denoted by $\mathcal{O}_K$.

Example. An integer is always an integral element; note that this means that $\mathbb{Z}$ is always a subring of $\mathcal{O}_K$.

Example. In the example above, with $K = \mathbb{Q}(i)$ and $a = 2i+3$, the minimal monic polynomial over $\mathbb{Q}$ has integer coefficients, so it is integral. However, $b = \frac{i}{2}$ is not an integral element since its minimal monic polynomial $(x - \overline{b})(x - b) = (x - \frac{i}{2})(x + \frac{i}{2}) = x^2 + \frac{1}{4}$ does not have integer coefficients.

Remark 1.8. In this paper, we will focus on the case where K is an **imaginary quadratic field**, a number field of the form $\mathbb{Q}(\sqrt{d})$ with $d < 0, d \equiv 0, 1 \pmod 4$, and d squarefree. The ring of integers of K is called an imaginary quadratic order.

Definition 1.9. A **fractional ideal** of a domain R is a subset of its quotient field Q of the form $I/c = \{\frac{a}{c} : a \in I\}$ where I is an ideal of R and $c \in R$, $c \neq 0$.

Definition 1.10. We say an ideal I of a ring R is **generated** by a subset S of R if I is the smallest ideal of R that contains S. A **principal ideal** is an ideal generated by a single element.

Example. Every ideal in $\mathbb{Z}$ is a principal ideal, and is generated by a unique nonnegative integer.

In order to put a group structure on the set of fractional ideals, we define a product of ideals:

Definition 1.11. For ideals I and J, define its **product** $IJ = \{\sum_{i=1}^{n} a_i b_i : n \in \mathbb{Z}, a_i \in I, b_i \in J\}$.

Note that the entire ring R is the identity; and for any integral domain R, not all nonzero fractional ideals are invertible with respect to this product, i.e. for an ideal I, there does not always exist an ideal J such that $IJ = R$.

Definition 1.12. Integral domains (that are not fields) with the property that all nonzero fractional ideals are invertible are called **Dedekind domains**.

Remark 1.13. Note that there are many equivalent definitions of a Dedekind domain; the most common definition is related to unique factorization of ideals.

Proposition 1.14. *The ring of integers of a number field is always a Dedekind domain.*

We refer the reader to [Ste04, Proposition 6.1.4] for a proof.

The set of fractional ideals forms a group under this product, and the set of principal fractional ideals forms a subgroup.

Definition 1.15. Let K be a field, and let J_K and P_K denote the group of fractional ideals and its subgroup of principal fractional ideals respectively. Then, we define the **ideal class group**, or **class group** as the quotient group

$$C_K = \frac{J_K}{P_K}.$$

The **class number** is the order of the class group.

2. Class Groups of Imaginary Quadratic Fields

In this section, we will characterize the structures defined above in the case of imaginary quadratic fields.

An important quantity describing a number field is its discriminant; when the number field is an quadratic number field, we define it as follows:

Definition 2.1. Let d be a squarefree integer (note that $d \equiv 1, 2, 3 \pmod 4$); then $K = \mathbb{Q}(d)$ is a quadratic field. We define the **discriminant** of the field as

$$\Delta = \begin{cases} d & d \equiv 1 \pmod 4 \\ 4d & d \equiv 2, 3 \pmod 4 \end{cases}.$$

Conversely, we can identify integers that are the discriminant of some quadratic field; we call these integers fundamental discriminants:

Definition 2.2. A **fundamental discriminant** d is an integer satisfying one of the following conditions:

(1) $d \equiv 1 \pmod 4$, d squarefree
(2) $d = 4m$, $m \equiv 2, 3 \pmod 4$, m squarefree

We then describe the ring of integers of quadratic fields:

Proposition 2.3. *For a squarefree integer d, the ring of integers of the quadratic field $\mathbb{Q}(\sqrt{d})$ are $\mathbb{Z}[g]$, where*

$$g = \begin{cases} \frac{1+\sqrt{d}}{2} & d \equiv 1 \pmod 4 \\ \sqrt{d} & d \equiv 2, 3 \pmod 4 \end{cases}$$

or equivalently, $g = \frac{\Delta+\sqrt{\Delta}}{2}$, where Δ is the discriminant.

Proof. For an element $a + b\sqrt{d} \in \mathbb{Q}(\sqrt{d})$, its minimal monic polynomial over $\mathbb{Q}$ is $(x - a - b\sqrt{d})(x - a + b\sqrt{d}) = x^2 + (2a)x + (a^2 - db^2)$. Write a and b as $\frac{a_1}{a_2}$ and $\frac{b_1}{b_2}$ respectively, where $\gcd(a_1, a_2) = \gcd(b_1, b_2) = 1$. For $a + b\sqrt{d}$ to be integral, $2a$ and $a^2 + db^2$ must be integers. Therefore, $a_2 = 1$ or 2.

If $a_2 = 1$, then $db^2 \in \mathbb{Z}$, so $b \in \mathbb{Z}$ as well since d is squarefree.

It $a_2 = 2$, then $\frac{a_1^2}{4} - \frac{db_1^2}{b_2^2} = \frac{a_1^2 b_2^2 - 4db_1^2}{4b_2^2} \in \mathbb{Z}$. Then, $a_1^2 b_2^2 - 4db_1^2 \equiv 0 \pmod 4$, so $a_1^2 b_2^2 - 4db_1^2 \equiv a_1^2 b_2^2 \equiv b_2^2 \equiv 0 \pmod 4$, since a_1 is relatively prime to a_2. We also have $a_1^2 b_2^2 - 4db_1^2 \equiv 0$

$\pmod{b_2^2}$, so $a_1^2 b_2^2 - 4db_1^2 \equiv 4db_1^2 \equiv 4 \equiv 0 \pmod{b_2^2}$, since b_1 is relatively prime to b_2. Thus, $b_2 = 2$.

Substituting this into $\frac{a_1^2}{4} - \frac{db_1^2}{b_2^2}$, we know that 4 must divide $a_1^2 - db_1^2$. Squares can only be 0 or 1 mod 4, so we can only have odd values of a_1 and b_1 if $d \equiv 1 \pmod 4$. Thus, the ring of integers is $\mathbb{Z}[g]$, where $g = \begin{cases} \frac{1+\sqrt{d}}{2} & d \equiv 1 \pmod 4 \\ \sqrt{d} & d \equiv 2, 3 \pmod 4 \end{cases}$.

Note that we can also take $g = \frac{\Delta + \sqrt{\Delta}}{2}$ where Δ is the discriminant, since Δ is odd iff $d \equiv 1$ mod 4. □

We can then see, from our definition of an ideal, that the ideals in quadratic orders will take on the following form:

Proposition 2.4. *Let d be a squarefree integer congruent to 0 or 1 $\pmod 4$, and let $\mathcal{O}(d)$ denote the quadratic order of discriminant d. Then, each fractional ideal of $\mathcal{O}(d)$ is of the form*

$$I = q\left(a\,\mathbb{Z} + \frac{b+\sqrt{d}}{2}\,\mathbb{Z}\right)$$

where $q \in \mathbb{Q}^+, a \in \mathbb{Z}^+$, and $b \in \mathbb{Z}$. Furthermore, q and a are unique, and b is unique mod $2a$.

We write an equivalence class of $\mathrm{Cl}(\mathcal{O})$ as $[a, b]$, since fractional ideals with different values of q are in the same ideal class.

3. The Discrete Logarithm Problem

Let d be a squarefree fundamental discriminant with $d < 0$, let $\mathcal{O}$ denote the corresponding imaginary quadratic order, and let $\mathrm{Cl}(\mathcal{O})$ denote the class group of $\mathcal{O}$. Compute $h = g^k$, where g is a random element of $\mathrm{Cl}(\mathcal{O})$ and k is a random integer chosen between 0 and 2^t with $t \geq 160$.

Question 3.1. *Given h and g, find $\mathrm{dlog}_g(h)$, which we define as the minimal integer k such that $h = g^k$.*

We will discuss the conditions we require for the DLP to be intractable, and how intractable it is compared to the integer factorization problem; more generally, we want to ensure that it is difficult to determine the order of the group (thus making it more difficult to determine the order of certain elements). We first introduce the L-notation, which is an asymptotic notation that tells us how complex an algorithm:

Definition 3.2. Let n be an increasing variable, let α be a constant with $0 \leq \alpha \leq 1$, and let c be a positive constant. We define $L_n[\alpha, c]$ as

$$e^{(c+o(1))(\ln n)^\alpha (\ln \ln n)^{1-\alpha}}$$

Example. A special case of this notation is when $\alpha = 0$ or $\alpha = 1$. If $\alpha = 0$, then

$$L_n[\alpha, c] = e^{(c+o(1))(\ln n)^\alpha (\ln \ln n)^{1-\alpha}} = e^{(c+o(1))(\ln \ln n)} = (\ln n)^{c+o(1)}$$

If $\alpha = 1$, then

$$L_n[\alpha, c] = e^{(c+o(1))(\ln n)^\alpha (\ln \ln n)^{1-\alpha}} = e^{(c+o(1))(\ln n)} = n^{c+o(1)}$$

Note that if $\alpha = 1$, then the function $L_n[\alpha, c]$ is a polynomial in n, while it is subexponential otherwise, i.e. it is much larger than a polynomial function, but still much smaller than an exponential function.

We also note that for larger values of c and α, we get larger values of $L_n[\alpha, c]$.

In terms of this notation, index calculus algorithms developed to solve the Discrete Logarithm Problem in class groups (Cl-DLP) have a running time proportional to $L_{|\Delta|}[\frac{1}{2}, \frac{3}{4}\sqrt{2}]$ under GRH, as proved in [Vol00]. A variant of the Quadratic Sieve, developed by Jacobson [Jac99], is expected to have a running time proportional to $L_{|\Delta|}[\frac{1}{2}, 1 + o(1)]$ based on empirical data. On the other hand, the best known integer factorization algorithm, the General Number Field Sieve (GNFS), has a running time proportional to $L_n[\frac{1}{3}, (\frac{64}{9})^{\frac{1}{3}}]$; we refer the reader to [Pom96] for an explanation of this algorithm and heuristics for its runtime. It is known that Cl-DLP is at least as hard as IFP, but we are currently unsure of whether it is actually harder.

4. Factorization in Dedekind Domains

In order to discuss Jacobson's Quadratic Sieve method, we first cover background related to factorization in Dedekind domains. We start by defining a prime ideal:

Definition 4.1. An ideal P in a ring R is a **prime ideal** if

(i) For elements $a, b \in R$, $ab \in P \implies a \in P$ or $b \in P$.
(ii) P is not the entire ring R.

Example. If we take $R = \mathbb{Z}$, then an ideal $n\mathbb{Z}$ is a prime ideal iff n is prime.

As mentioned before, the standard definition of a Dedekind domain is about factorization into prime ideals:

Definition 4.2. A nonzero commutative ring is a **Dedekind domain** if the following two hold:

(i) It is an **integral domain**, i.e. the product of any two nonzero elements is also nonzero.
(ii) Every nonzero ideal that is not the whole ring factors into a product of prime ideals.

Example. Recall that the ring of integers of every number field is a Dedekind domain.

In fact, we can show the following about Dedekind domains:

Theorem 4.3. *Let I be a nonzero ideal of the ring of integers of a number field $\mathcal{O}_K$. Then, the prime factorization of I into prime ideals is unique up to order.*

See [Ste04, Theorem 6.1.9] for a proof.

We now address the question of how to factor any ideal of the form $\mathfrak{a} = a\mathbb{Z} + \frac{b+\sqrt{\Delta}}{2}\mathbb{Z}$. Our goal is to construct a mapping N from the set of ideals to $\mathbb{Z}$, so that we can factor an ideal I using the prime factorization of $N(I)$:

Definition 4.4. Let I be an ideal of $\mathcal{O}_K$, where K is a number field. Then, the **norm** of I is $N(I) = [\mathcal{O}_K : I]$.

Example. Taking $K = \mathbb{Q}$ (and thus $\mathcal{O}_K = \mathbb{Z}$, the norm of an ideal of the form $n\mathbb{Z}$ is n.

The following theorem relates the norm of an ideal to its factorization into prime ideals:

Theorem 4.5. *Let $\mathfrak{a} = a\,\mathbb{Z} + \frac{b+\sqrt{\Delta}}{2}\,\mathbb{Z}$, and suppose the norm $N(\mathfrak{a})$ has prime factorization*

$$N(\mathfrak{a}) = \prod_{p \mid N(\mathfrak{a})} p^{t(p)}.$$

Define $\mathfrak{p}(p) = p\,\mathbb{Z} + \frac{b_p+\sqrt{\Delta}}{2}\,\mathbb{Z}$, where b_p satisfies $0 \leq b_p \leq p$ and $b_p^2 \equiv \Delta \pmod{4p}$, and $e(p) \in -1, 1$ Then, the prime factorization of $\mathfrak{a}$ is

$$\prod_{p \mid N(\mathfrak{a})} \mathfrak{p}(p)^{e(p)t(p)}$$

We omit the proof, as it is beyond the scope of this paper.

5. Jacobson's Quadratic Sieve Method

We will now provide an overview of the variants of the Quadratic Sieve developed to compute the structure of the class groups and discrete logarithms; see [JJ99] for a more thorough treatment.

Recall that in the Quadratic Sieve, we attempt to find a pair (x, y) such that $x^2 \equiv y^2 \pmod{n}$; in the Multiple Polynomial Quadratic Sieve, which is a variant of this algorithm, we use multiple of polynomials of the form $y = (Ax + B)^2 - n^2$ (which has similar form to the original polynomial $y = x^2 - n$), running the algorithm on all of these to find (x, y) pairs more quickly. This is useful because it is ideal for parallelization: each processor is given a subset of the polynomials, and separately runs the algorithm.

We first compute a factor base FB of prime ideals such that a subset will generate the class group $\mathrm{Cl}(\Delta)$. We have the following theorem by Bach [Bac90]:

Theorem 5.1. *Assuming the Extended Riemann Hypothesis, the generating set of a class group of a field with discriminant Δ has prime ideal with largest norm at most $12 \log^2 |\Delta|$. If Δ is a fundamental discriminant of a quadratic field, then this bound can be improved to $6 \log^2 |\Delta|$.*

Note that instead of checking up to this bound, we can optimize the algorithm by allowing for a smaller factor base: see [JJ99] for more details.

The key idea in the algorithm is the generation of *relations*, which we define to be a vector $v = (v_1, v_2, \ldots v_k)$ such that $\mathcal{O}_K$ is equivalent to $\prod_{\mathfrak{p} \in FB} \mathfrak{p}^{v_i}$. To generate a relation, we use the theory of quadratic forms:

Definition 5.2. A **quadratic form** Q over a ring R is a polynomial

$$Q(x_1, \ldots, x_n) = \sum_{1 \leq i \leq j \leq n} a_{ij} x_i x_j$$

where each term has degree 2 and the coefficients a_{ij} lie in R.

Example. $3x^2 + 2xy + 5y^2$ is a binary quadratic form, i.e. one in two variables.

Definition 5.3. The **discriminant** of a binary quadratic form $ax^2 + bxy + cy^2$ is $b^2 - 4ac$.

Example. The discriminant of $3x^2 + 2xy + 5y^2$ is $2^2 - 3 * 5 = -11$.

There is a correspondence between quadratic forms with discriminant Δ and ideals of an imaginary quadratic field with discriminant Δ: we map the ideal $\mathfrak{a} = (a, b)$ to the quadratic form $ax^2 + bxy + cy^2$, where $c = \frac{b^2-\Delta}{4a}$ since we need the quadratic form to have discriminant Δ.

So, we start with an ideal $\mathfrak{a} = (a, b)$ which is smooth over our factor base. This corresponds to $ax^2 + bxy + cy^2$, where we take $c = \frac{b^2-\Delta}{4a}$ as before. We then construct another ideal $\mathfrak{a}'$ which is equivalent to $\mathfrak{a}$, so $\mathfrak{a}\mathfrak{a}'^{-1}$ is equivalent to $\mathcal{O}_K$, yielding a relation. We do this with the following proposition:

Proposition 5.4. *Let $Q(x, y) = ax^2 + bxy + cy^2$ be a quadratic form over $\mathbb{Z}$. Then, if there exists integers x_0, y_0 such that $Q(x_0, y_0) = a'$ for some integer a', then there exists some b', c' such that the quadratic form $a'x^2 + b'xy + c'y^2$ is equivalent to Q.*

where we define an equivalence relation for quadratic forms as follows:

Definition 5.5. Two forms Q_1,Q_2 are **equivalent** over a ring R if there exists an invertible matrix M with entries in R such that for all vectors $\vec{x}$ with entries in R, $Q_1(M\vec{x}) = Q_2(\vec{x})$.

Since we want $\mathfrak{a}'$ to be smooth over our factor base of prime ideals as well, we find pairs (x, y) such that $ax^2 + bxy + cy^2$ is smooth. As we would do in the integer factorization quadratic sieve, we then sieve over the quadratic form $ax^2 + bx + c$, where we set $y = 1$.

6. Smooth Class Numbers

For Cl-DLP to be intractable, the class number $h(\Delta)$ should not be smooth.

Suppose we are trying to compute discrete logarithms of an element of $\mathrm{Cl}(\Delta)$, γ. Set $\alpha = \gamma$, and for each prime p_i less than a smoothness bound B, compute $\alpha_i = \alpha_{i-1}^{p_i^{e(p_i,B)}}$, where $e(p_i, B)$ is some function of p_i and B (for example, we can take $e(p_i, B) = \lfloor \log_{p_i} B \rfloor$).

This algorithm is very similar to the $p-1$ factorization algorithm used to factor a number N with a prime factor p such that $p-1$ is smooth, where we set $a_0 = 2^{\lfloor \log_2 N \rfloor} \pmod N$ and then compute $a_i = a_{i-1}^{p_i^{\lfloor \log_{p_i} N \rfloor}} \pmod N$.

The difference here is that we do not know the number N that we are trying to factor, so instead of trying to find a prime factor right away from this sequence, we want these values to eventually reach the identity, $1_{\mathrm{Cl}(\Delta)}$.

If this succeeds and the sequence eventually reaches the identity, then let i be the integer satisfying $\alpha_{i-1} \neq 1_{\mathrm{Cl}(\Delta)}$ and $\alpha_i = 1_{\mathrm{Cl}(\Delta)}$, i.e. the first integer in the sequence that is the identity. Then, we know that p_i must be a prime factor of the order of γ, denoted $\mathrm{ord}_{\mathrm{Cl}(\Delta)}\, \gamma$; in fact, we can see that it must be the largest prime factor.

We can then set $\gamma' = \gamma^{p_i^{e(p_i,B)}}$, and repeat the process; in this way, we compute the second largest prime factor of $\mathrm{ord}_{\mathrm{Cl}(\Delta)}\, \gamma$. Eventually, we obtain the full prime factorization of $\mathrm{ord}_{\mathrm{Cl}(\Delta)}\, \gamma$. Recall that if the order of an element is smooth, we can easily compute discrete logarithms of that element using the Pohlig-Hellman algorithm.

7. A Heuristic For Smooth Class Numbers

We already know how to control the even part of the class number, $v_2(h(\Delta))$. One way to do this, as suggested in [HM00], is to select Δ one of the following ways:

(1) $\Delta = -p$, where p is a prime with $p \equiv 3 \pmod 4$

(2) $\Delta = -8pq$, where $p \equiv 1 \pmod 8, p + q \equiv 8 \pmod{16}$, and $\left(\frac{p}{q}\right) = -1$.

If we choose the discriminant this way, then we can explicitly describe the even part [Kap73]:

Proposition 7.1 (Kaplan)**.** *In the first case, $h(\Delta)$ is odd; in the second case, $v_2(h(\Delta)) = 3$.*

However, we cannot do the same for odd primes, so our strategy will be to pick a discriminant Δ large enough so that the probability that $h(\Delta)$ is smooth will be very small. In order to estimate this probability, we use heuristics developed by Hamdy and Möller in [HM00]. Let $\Pr(E)$ denote the probability of an event happening; our goal is to estimate $\Pr(p^i \mid h(\Delta))$ for a positive integer i and an odd prime p. Cohen and Lenstra give heuristics for the case $i = 1$ in [CL84]:

Conjecture 7.2 (Cohen–Lenstra). *As $\Delta \to -\infty$, $\Pr(p \mid h(\Delta))$ is approximately*

$$1 - \prod_{j=1}^{\infty} \left(1 - \frac{1}{p^j}\right)$$

For $i \geq 2$, Buell conjectured the following based on statistics of class numbers [Bue84]:

Conjecture 7.3 (Buell). *As $\Delta \to -\infty$, $\Pr(p^i \mid h(\Delta))$ is approximately*

$$\frac{1}{p^i} + \frac{1}{p^{i+1}} = \frac{1 + \frac{1}{p}}{p^i}$$

So by these conjectures, we assume that $\Pr(p^i \mid h(\Delta) \leq \frac{1+\frac{1}{p}}{p^i}$.

On the other hand, if x is just any randomly chosen integer from some interval, $\Pr(p^i \mid x)$ is about $\frac{1}{p^i}$. Thus, by our assumptions, the ratio of these two probabilities is

$$\frac{\Pr(p^i \mid h(\Delta))}{\Pr(p^i \mid x)} \leq 1 + \frac{1}{p}$$

so we should expect class numbers to be smooth with higher probability than randomly chosen integers. However, we would like more specific heuristics on how significant this difference is.

Assume the probabilities $\Pr(p^i \mid h(\Delta))$ are independent to each other; then, if we factor some smooth odd integer k as $\prod_{p|k} p^{e_p(k)}$, then we have

$$\frac{\Pr(k \mid h(\Delta))}{\Pr(k \mid x)} = \frac{\prod_{p|k} \Pr(p^{e_p(k)} \mid h(\Delta))}{\prod_{p|k} \Pr(p^{e_p(k)} \mid x)} = \prod_{p|k} \frac{\Pr(p^{e_p(k)} \mid h(\Delta))}{\Pr(p^{e_p(k)} \mid x)} \leq \prod_{p|k} \left(1 + \frac{1}{p}\right)$$

8. Heuristic Bounds for the Ratio of Smoothness Probabilities

Let F_k be the product $\prod_{p|k} \left(1 + \frac{1}{p}\right)$ above. We aim to find an upper bound for F_k, to determine how large this ratio can become.

In order to do this, we refer to the following result by Brauer and Siegel [Bra47]:

Theorem 8.1 (Brauer–Siegel). *As $|\Delta| \to \infty$, we have*

$$\log(h(\Delta)) \sim \log(\sqrt{|\Delta|}).$$

Remark 8.2. Brauer actually proved a more general theorem formulated by Siegel for number fields of degree n; the result stated above is the more simple case of $n = 2$.

Based on this theorem, the maximum should occur around $\sqrt{|\Delta|}$, and we can see that in order for F_k to be large, k should be a product of many small primes, so we set $k = \prod_{p<t} p$; this is called a primorial. We have the following asymptotic for primorials, which is a corollary of the Prime Number Theorem:

Theorem 8.3 (Prime Number Theorem)**.** *Let $\pi(x)$ be the prime counting function $\sum_{p\leq x} 1$. Then,*

$$\pi(x) = \frac{x}{\log x} + o\left(\frac{x}{\log x}\right).$$

Corollary 8.4. *For $n \in \mathbb{Z}$, let $P(n)$ be the product $\prod_{p<n} p$. Then, $P(n) = e^{(1+o(1))(n)}$.*

Proof. Let $\vartheta(x) = \sum_{p\leq x} \log p$. Then, we claim that $\vartheta(x) = x + o(x)$. To prove that this is a corollary of the Prime Number Theory, called Abel Summation:

Lemma 8.5. *Let $a_1, a_2, \ldots$ be a sequence of complex numbers, and define $A(x) = \sum_{1\leq n\leq x} a_n$. Let $\phi : [1, x] \to \mathbb{R}$. be a differentiable function with a continuous derivative. Then, for all $x > 1$, we have*

$$\sum_{1\leq n\leq x} a_n\phi(n) = A(x)\phi(x) - \int_1^x A(u)\phi'(u)du$$

.

Proof. Since $A(x) = A(\lfloor x\rfloor)$, we break up the integral as follows so we can separate out that term from the integral:

$$A(x)\phi(x) - \int_1^x A(u)\phi'(u)du = A(x)\phi(x) - \sum_{i=1}^{\lfloor x\rfloor-1} \int_i^{i+1} A(u)\phi'(u)du - \int_{\lfloor x\rfloor}^x A(u)\phi'(u)du$$

From i to $i + 1$, $A(u) = A(i)$, and $A(x) = A(\lfloor x\rfloor)$, so we can pull those terms out from the integral and evaluate the integral:

$$= A(x)\phi(x) - \sum_{i=1}^{\lfloor x\rfloor-1} A(i)\int_i^{i+1} \phi'(u)du - A(x)\int_{\lfloor x\rfloor}^x \phi'(u)du$$

$$= A(x)\phi(x) - \sum_{i=1}^{\lfloor x\rfloor-1} A(i)(\phi(i+1) - \phi(i)) - A(x)(\phi(x) - \phi(\lfloor x\rfloor)$$

The $A(x)\phi(x)$ terms cancel, and we switch the $\phi(i+1)$ and $\phi(i)$ terms to get rid of the minus sign in front of the summation:

$$= \sum_{i=1}^{\lfloor x\rfloor-1} A(i)(\phi(i) - \phi(i+1)) + A(x)\phi(\lfloor x\rfloor)$$

Expanding the $A(i)$ and $A(x)$ terms yields

$$= \sum_{i=1}^{\lfloor x\rfloor-1} (\phi(i) - \phi(i+1)) \sum_{j=1}^{i} a_j + \sum_{i=1}^{\lfloor x\rfloor} a_i\phi(\lfloor x\rfloor)$$

We now switch the order of the double summations: before, we had i ranging from 1 to $\lfloor x\rfloor - 1$, and j ranging from 1 to i, so that $i \geq j$. Thus, if we have j ranging from 1 to $\lfloor x\rfloor - 1$, i will range from j to $\lfloor x\rfloor - 1$:

$$= \sum_{j=1}^{\lfloor x\rfloor-1} a_j \sum_{i=j}^{\lfloor x\rfloor-1} (\phi(i) - \phi(i+1)) + \sum_{i=1}^{\lfloor x\rfloor} a_i\phi(\lfloor x\rfloor)$$

We can see that all of the terms in $\sum_{i=j}^{\lfloor x\rfloor -1}(\phi(i)-\phi(i+1))$ will cancel out except for the endpoints, so this expression will simplify to $\phi(j)-\phi(\lfloor x\rfloor)$:

$$= \sum_{j=1}^{\lfloor x\rfloor -1} a_j\phi(j) - \sum_{j=1}^{\lfloor x\rfloor -1} a_j\phi(\lfloor x\rfloor) + \sum_{i=1}^{\lfloor x\rfloor} a_i\phi(\lfloor x\rfloor)$$

In the difference of the second and third terms, all terms will cancel out except for $a_{\lfloor x\rfloor}\phi(\lfloor x\rfloor)$; absorbing this term into the first summation yields $\sum_{i=1}^{\lfloor x\rfloor} a_i\phi(i)$ as desired. □

Now, let $a_i = 1$ if i is prime, and 0 otherwise, so that $A(x) = \pi(x)$. Then, $\vartheta(x) = \sum_{p\le x}\log p = \sum_{1\le n\le x} a_n \log(n)$. Applying Abel summation,

$$\vartheta(x) = \pi(x)\log(x) - \int_1^x \pi(u)\frac{1}{u}du$$

Substituting $\pi(x) = \frac{x}{\log x} + o(\frac{x}{\log x}$ by the Prime Number Theorem yields

$$= x + o(x) - \int_1^x \left(\frac{1}{\log u} + o\left(\frac{1}{\log u}\right)\right) du$$
$$= x + o(x)$$

since the integral is positive. Thus since $P(n) = e^{\vartheta(n)}$, $P(n) = e^{(1+o(1))(n)}$. □

Thus, for our maximum, the quantities t, $\log k$, and $\log\sqrt{|\Delta|}$ will be approximately equal to each other. We have

$$\prod_{p<t}\left(1+\frac{1}{p}\right) \approx \prod_{p<\log\sqrt{|\Delta|}}\left(1+\frac{1}{p}\right)$$

To approximate this product, we use Merten's theorem, which is an asymptotic for a similar product:

Theorem 8.6 (Mertens)**.** *Let x be a positive integer. Then,*

$$\prod_{p<x}\left(1-\frac{1}{p}\right) = \frac{1}{e^\gamma \log x} + O\left(\frac{1}{\log^2 x}\right)$$

where γ is the Euler-Mascheroni constant.

We can write our product as

$$\prod_{p<\log\sqrt{|\Delta|}}\left(1+\frac{1}{p}\right) = \frac{\prod_{p<\log\sqrt{|\Delta|}}\left(1-\frac{1}{p^2}\right)}{\prod_{p<\log\sqrt{|\Delta|}}\left(1-\frac{1}{p}\right)}$$
$$= \frac{\prod_{p<\log\sqrt{|\Delta|}}\left(1-\frac{1}{p^2}\right)}{\frac{1}{e^\gamma\log\log\sqrt{|\Delta|}} + O\left(\frac{1}{\log^2\log\sqrt{|\Delta|}}\right)}$$

Now, we approximate both the numerator and denominator. If we let the product in the numerator range over all primes instead of cut off at $\log\sqrt{|\Delta|}$, and took the inverse, we would have $\prod_{p\,\text{prime}}\frac{1}{1-\frac{1}{p^2}} = \prod_{p\text{prime}}(1+\frac{1}{p^2}+\frac{1}{p^4}+\cdots)$. Because of unique factorization in the integers, if we expanded this out, every term would be of the form $\frac{1}{n^2}$, and there would be one of these terms for every integer. This sum $\sum_{n=1}^{\infty} \frac{1}{n^2}$ is the zeta function $\zeta(2)$, and it is well known that this sum converges, and is equal to $\frac{\pi^2}{6}$. Thus, we can approximate the numerator as $\frac{6}{\pi^2}$.

The denominator is the quantity approximated in Merten's theorem, so it is close to $\frac{1}{e^{\gamma} \log(\log \sqrt{|\Delta|})}$ since the error term $O\left(\frac{1}{\log^2(\log(\sqrt{|\Delta|}))}\right)$ approaches 0 as Δ tends to infinity.

Putting this together, we get $\log\log\sqrt{|\Delta|}$ as our final approximation. Using this, we can then find bounds on how large Δ should be, based on how small we want $\Pr(h(\Delta)$ is smooth) to be. Hamdy and Möller suggest $|\Delta| = 2^2 B^{2u}$ if we choose the class number to be odd, and $|\Delta| = 2^8 B^{2u}$ if we choose the class number to be even [HM00].

9. Further Questions

The cryptosystems discussed here have a security level comparable to that of RSA, although they are still vulnerable to quantum attacks. However, cryptosystems based on imaginary quadratic orders are relatively new, and there is still further work to be done on them. We are still unsure of whether the Discrete Logarithm Problem in Imaginary Quadratic Orders is harder than the Integer Factorization Problem, and if there exists a general number field variant of Jacobson's Quadratic Sieve method that is analogous to the Number Field Sieve for integer factorization.

Additionally, there have been proposed generalizations to general number fields, such as Buchmann and Paulus' proposed one way function based on the shortest vector problem [BP97], which is as follows: for a lattice L, given a basis of a vector space V and a norm N, which is often the standard Euclidean norm, find the vector in V that is in L and has the least norm (i.e. the shortest vector in L). Cryptosystems based on lattice problems are currently candidates for post-quantum cryptography. Currently, the best known attack against this proposed function is exponential in the degree of the lattice; more work still has to be done to check if there is a more efficient algorithm.

References

[Bac90] Eric Bach. Explicit bounds for primality testing and related problems. *Mathematics of Computation*, 55(191):355–380, 1990.

[BP97] Johannes A. Buchmann and Sachar Paulus. A one way function based on ideal arithmetic in number fields. In *CRYPTO*, 1997.

[Bra47] Richard Brauer. On the zeta-functions of algebraic number fields. *American Journal of Mathematics*, 69(2):243–250, 1947.

[Bue84] Duncan A Buell. The expectation of success using a monte carlo factoring method—some statistics on quadratic class numbers. *Mathematics of Computation*, 43(167):313–327, 1984.

[CL84] H. Cohen and H. W. Lenstra. Heuristics on class groups of number fields. In Hendrik Jager, editor, *Number Theory Noordwijkerhout 1983*, pages 33–62, Berlin, Heidelberg, 1984. Springer Berlin Heidelberg.

[Gri07] P.A. Grillet. *Abstract Algebra*, volume 242 of *Graduate Texts in Mathematics*. Springer Science+Business Media, second edition, 2007.

[HM00] Safuat Hamdy and Bodo Möller. Security of cryptosystems based on class groups of imaginary quadratic orders. In Tatsuaki Okamoto, editor, *Advances in Cryptology — ASIACRYPT 2000*, pages 234–247, Berlin, Heidelberg, 2000. Springer Berlin Heidelberg.

[Jac99] Michael J Jacobson. *Subexponential class group computation in quadratic orders*. Shaker, 1999.

[JJ99] Michael Jacobson Jr. Applying sieving to the computation of quadratic class groups. *Mathematics of Computation*, 68(226):859–867, 1999.

[Kap73] Pierre Kaplan. *Sur le 2-groupe des classes d'idéaux des corps quadratiques*. Departement de mathematique, 1973.

[Pom96] Carl Pomerance. A tale of two sieves. *Biscuits of Number Theory*, 85:175, 1996.

[Ste04] William Stein. A brief introduction to classical and adelic algebraic number theory, 2004.

[Vol00] Ulrich Vollmer. Asymptotically fast discrete logarithms in quadratic number fields. In *International Algorithmic Number Theory Symposium*, pages 581–594. Springer, 2000.