# Random Ideals

Katharina Boudgoust

December 26, 2020

## 1 Introduction

Number theory, as the name indicates, is the mathematical study of numbers. Given two integers $x$ and $y$ in $\mathbb{Z}$, one can do a lot of funny things with them, as we learned in school. One can compute their sum $x + y$, their product $x \cdot y$ or even their *greatest common divisor* $\gcd(x, y)$, which is the smallest integer that divides both $x$ and $y$. If the $\gcd(x, y)$ is 1, we call them *relatively prime*. An interesting result in number theory says that the probability that two random positive integers are relatively prime is $6/\pi^2$. This happens to be exactly the value of $1/\zeta(2)$, where $\zeta$ is the Riemann zeta function. More generally, one can prove that the probability that $n$ positive integers are relatively prime is $1/\zeta(n)$. We can even further generalize this statement for any algebraic number field $K$ with associated ring of integers $\mathcal{O}_K$. We call two nonzero ideals $\mathfrak{a}$ and $\mathfrak{b}$ of $\mathcal{O}_K$ *relatively prime* if there does not exist a prime ideal $\mathfrak{p} \subseteq \mathcal{O}_K$ such that $\mathfrak{p}|\mathfrak{a}$ and $\mathfrak{p}|\mathfrak{b}$. Sittinger and DeMoss show in (DS19) the following result:

**Theorem 1.1.** *Fix a positive integer $n$. Then, the probability that $n$ nonzero ideals of $\mathcal{O}_K$ are pairwise relatively prime equals*

$$\begin{aligned} P_n &= \prod_{\mathfrak{p}} \left(1 - \frac{1}{\mathfrak{N}(\mathfrak{p})}\right)^n + \frac{n}{\mathfrak{N}(\mathfrak{p})} \cdot \left(1 - \frac{1}{\mathfrak{N}(\mathfrak{p})}\right)^{n-1} \\ &= \prod_{\mathfrak{p}} \left(1 - \frac{1}{\mathfrak{N}(\mathfrak{p})}\right)^{n-1} \cdot \left(1 + \frac{n-1}{\mathfrak{N}(\mathfrak{p})}\right), \end{aligned}$$

*where the product runs over all prime ideals $\mathfrak{p}$ in $\mathcal{O}_K$ and where $\mathfrak{N}$ denotes the norm of an ideal.*

In general it is quite tricky to compute an *infinite* product. However, in many cases, it is sufficient to only know an approximate value of this probability. Sittinger and DeMoss (DS19) give a lower bound on the number $N$ of prime ideals that we need to use in the product in order to have a satisfying approximation of the probability $P_n$. More precisely, let $d$ denote the degree of $\mathcal{O}K$ and $t$ denote the decimal point accuracy for $P_n$ that we want to achieve. In this case

$$N \geq \frac{d(n-1)^2 \cdot 10^t + (n-3)}{2}$$

is sufficient. In (DS19, Fig.1), the authors give approximations of this probability for different examples of number fields. For example, for the case of the 5-th cyclotomic number field, the probability is approximately 0.9155.

In this repository, we include a sage code to compute this probability for any cyclotomic number field.

## 2 Cyclotomic Fields

In order to understand the sage code, it is crucial to understand how some specific ideals behave in the ring of integers $\mathcal{O}_K$, when $K$ is a cyclotomic number field. We only recall some important results that we use without proving or motivating them. We refer an interested reader to (LPR13) and (Con) for more details.

A *number field* $K = \mathbb{Q}(\zeta)$ of degree $d$ is a finite extension of the rational number field $\mathbb{Q}$ obtained by adjoining an algebraic number $\zeta$. The set of all algebraic integers of $K$ defines a ring, called the *ring of integers* which we denote by $\mathcal{O}_K$.

A first fact that we need to know is that the norm of a prime ideal $\mathfrak{p}$ in $\mathcal{O}_K$ is a power of a prime. Further, for every prime $p$ the norm of the ideal generated by $p$ has norm $p^d$, where $d$ is the degree of the number field. Thus, in order to find all prime ideals in $\mathcal{O}_K$, it is sufficient to compute the prime ideal factorization of the ideals $\langle p \rangle$, where $p$ is a prime. Fortunately, this factorization in $\mathcal{O}_K$ exists and is unique (we call those rings Dedekind domains). In the special case of cyclotomic number fields, we exactly know the factoring behavior of those ideals.

A number field $K$ is called the $m$-th *cyclotomic field*, when $\zeta$ is a primitive $m$-th root of unity. In this case the equality $\mathcal{O}_K = \mathbb{Z}[\zeta]$ holds. We denote by $\varphi(m) = d$ the degree of $\mathcal{O}_K$, where $\varphi$ denotes Euler's totient function. To give a concrete example, let $m = 2^k$ be a power of two. Then we can think of $\zeta$ as $\exp(2\pi i/m)$ and $\mathcal{O}_K$ will be isomorphic to $\mathbb{Z}[x]/\langle x^{m/2} + 1 \rangle$.

In the case of cyclotomic number fields, we know how the prime ideal factorization of principal ideals generated by prime numbers behaves. In more details, for an integer prime $p \in \mathbb{Z}$, the factorization of the principal ideal $\langle p \rangle subseteq \mathcal{O}_K$ is as follows. Let $\ell \geq 0$ be the largest integer such that $p^\ell$ divides $m$, let $h = \varphi(p^\ell)$, and let $f \geq 1$ be the multiplicative order of $p$ modulo $m/p^\ell$. Further let $g = d/(hf)$. Then the ideal $\langle p \rangle$ splits in exactly $g$ distinct prime ideals each of norm $p^f$, i.e., $\langle p \rangle = \mathfrak{p}_1^h \cdots \mathfrak{p}_g^h$.

To illustrate this, we may look at the specific case where $p = 1 \bmod m$. Then we know that the ideal generated by $p$ totally splits in $d$ distinct primes, each of norm $p$ (use $\ell = 0$, $h = 1$, $f = 1$). Another example is the case where $m$ is prime and thus for every $p \neq m$ we know that $\ell = 0$ and $h = 1$. Thus, the multiplicative order of $p$ modulo $m$ fully determines how the ideal $\langle p \rangle$ splits in $\mathcal{O}_K$.

## References


[Con] K. Conrad. The different ideal. http://www.math.uconn.edu/~kconrad/blurbs/gradnumthy/different.pdf.

[DS19] Ryan D. DeMoss and Brian D. Sittinger. The probability that ideals in a number ring are k-wise relatively r-prime, 2019.

[LPR13] V. Lyubashevsky, C. Peikert, and O. Regev. On ideal lattices and learning with errors over rings. *J. ACM*, 60(6):43:1–43:35, 2013.