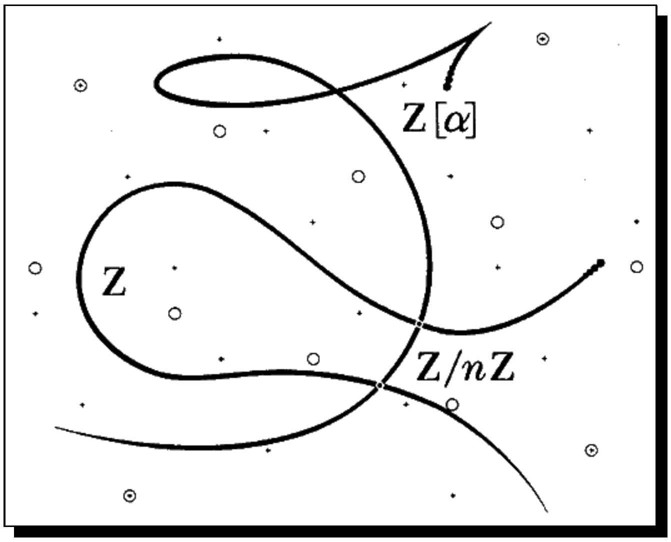
Factoring Primes in Rings of Integers

William A. Stein (was@math.harvard.edu)

March 8, 2002



A diagram from [3].

"The obvious mathematical breakthrough would be development of an easy way to factor large prime numbers."

–Bill Gates, *The Road Ahead*, pg. 265

1 Introduction

A *prime ideal* of a commutative ring R is an ideal $\mathfrak{p}$ such that $R/\mathfrak{p}$ is an integral domain, and an ideal $\mathfrak{p}$ is *maximal* if $R/\mathfrak{p}$ is a field. Let $K = \mathbb{Q}(\alpha)$ be a number field, and let $\mathcal{O}_K$ be the ring of all elements of K that are integral over $\mathbb{Z}$. As you know, $\mathcal{O}_K$ is a Dedekind domain.

In order to employ our geometric intuition, we may view $\mathcal{O}_K$ as a one-dimensional "scheme"

$$X = \mathrm{Spec}(\mathcal{O}_K) = \{ \text{ all prime ideals of } \mathcal{O}_K \text{ } \}$$

“over”

$$Y = \mathrm{Spec}(\mathbb{Z}) = \{(0)\} \cup \{p\mathbb{Z} : p \in \mathbb{Z} \text{ is prime }\}.$$

There is a natural map $f : X \to Y$ that sends a prime ideal $\mathfrak{p} \in X$ to $\mathfrak{p} \cap \mathbb{Z} \in Y$. For much more on this point of view, see [2, Ch. 2].

Ideals were originally introduced by Kummer because in rings of integers of number fields ideals factor uniquely as products of primes ideals, which is something that is not true for general algebraic integers. (The failure of unique factorization for algebraic integers was used by Liouville to “destroy” Lamé’s purported 1847 “proof” of Fermat’s Last Theorem.)

If $p \in \mathbb{Z}$ is a prime number, then the ideal $p\mathcal{O}_K$ of $\mathcal{O}_K$ factors uniquely as a product $\prod \mathfrak{p}_i^{e_i}$, where the $\mathfrak{p}_i$ are maximal ideals of $\mathcal{O}_K$. Viewed *geometrically*, the decomposition of $p\mathcal{O}_K$ into prime ideals in $\mathcal{O}_K$ is the same as the fiber $f^{-1}(p\mathbb{Z})$ (plus ramification data). We are concerned with how to compute $f^{-1}(p\mathbb{Z})$ in practice.

Example 1.1. The following Magma session shows the commands needed to compute the factorization of $p\mathcal{O}_K$ in Magma for K the number field defined by a root of $x^5 + 7x^4 + 3x^2 - x + 1$.

```
> K<a> := NumberField(x^5+7*x^4+3*x^2-x+1);
> OK := MaximalOrder(K);
> I := 2*OK;
> Factorization(I);
[
<Principal Prime Ideal of OK
Generator:
[2, 0, 0, 0, 0], 1>
]
> Factorization(Discriminant(OK));
[ <5, 1>, <353, 1>, <1669, 1> ]
> J := 5*OK;
> Factorization(J);
[
<Prime Ideal of OK
Two element generators:
[5, 0, 0, 0, 0]
[2, 1, 0, 0, 0], 1>,
<Prime Ideal of OK
Two element generators:
[5, 0, 0, 0, 0]
[3, 1, 0, 0, 0], 2>,
<Prime Ideal of OK
Two element generators:
```

```
[5, 0, 0, 0, 0]
[2, 4, 1, 0, 0], 1>
]
> [K!OK.i : i in [1..5]];
[ 1, a, a^2, a^3, a^4 ]
```

Thus $2\mathcal{O}_K$ is already a prime ideal, and

$$5\mathcal{O}_K = (5, 2+a)\cdot(5, 3+a)^2\cdot(5, 2+4a+a^2).$$

Notice that in this example $\mathcal{O}_K = \mathbb{Z}[a]$. But be warned—in general, one can not find an a such that $\mathcal{O}_K = \mathbb{Z}[a]$ (see Example 4.2 below). When $\mathcal{O}_K = \mathbb{Z}[a]$ it is very easy to factor $p\mathcal{O}_K$, as we will see below. The following factorization gives a hint as to why:

$$x^5 + 7x^4 + 3x^2 - x + 1 \equiv (x+2)\cdot(x+3)^2\cdot(x^2+4x+2) \pmod{5}.$$

The exponent 2 of $(5, 3+a)^2$ in the factorization of $5\mathcal{O}_K$ above suggests "ramification", in the sense that the cover $X \to Y$ has less points (counting their "size", i.e., their residue class degree) in its fiber over 5 than it has generically. Here's a suggestive picture:

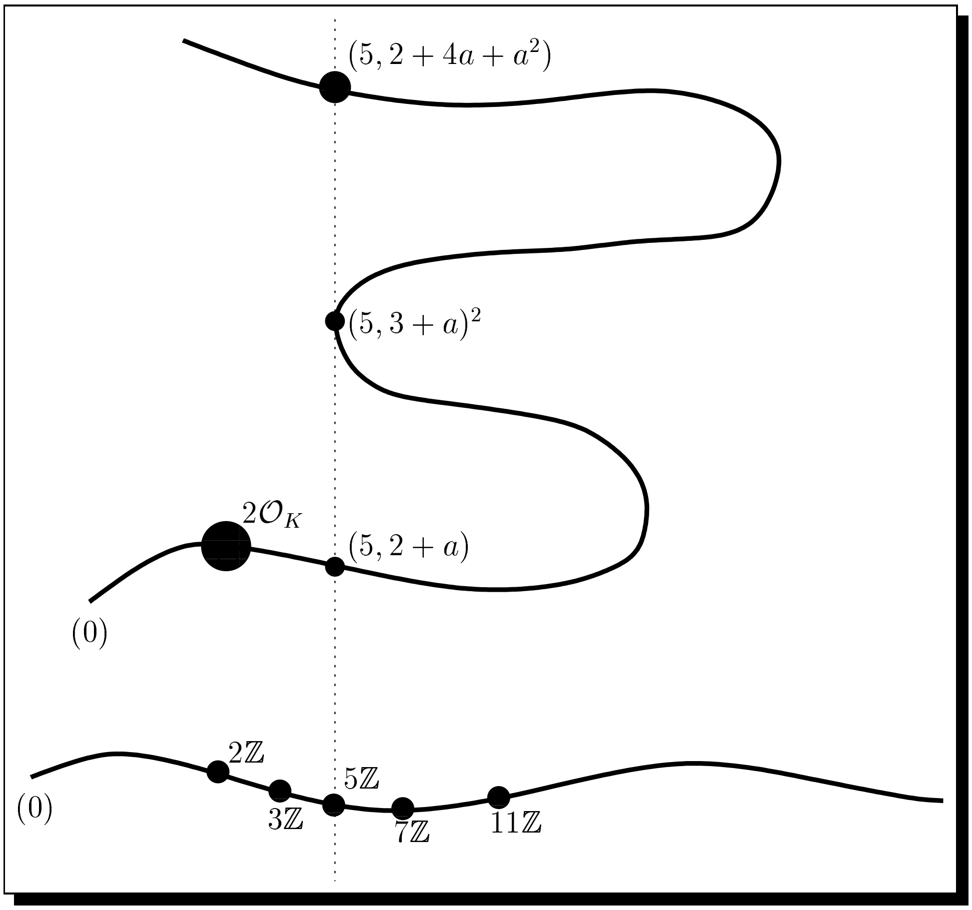


Diagram of $\mathrm{Spec}(\mathcal{O}_K) \to \mathrm{Spec}(\mathbb{Z})$

2 A Method that Usually Works

Suppose $\alpha \in \mathcal{O}_K$ is such that $K = \mathbb{Q}(\alpha)$, and let $g(x)$ be the minimal polynomial of α. Then $\mathbb{Z}[\alpha] \subset \mathcal{O}_K$, and we have a diagram of schemes

$$\begin{tikzcd}
(??) \arrow[r, hook] \arrow[d] & \mathrm{Spec}(\mathcal{O}_K) \arrow[d] \\
\bigcup \mathrm{Spec}((\mathbb{Z}/p\mathbb{Z})[x]/(\overline{g}_i^{e_i})) \arrow[r, hook] \arrow[d] & \mathrm{Spec}(\mathbb{Z}[\alpha]) \arrow[d] \\
\mathrm{Spec}(\mathbb{Z}/p\mathbb{Z}) \arrow[r, hook] & \mathrm{Spec}(\mathbb{Z})
\end{tikzcd}$$

where $\overline{g} = \prod_i \overline{g}_i^{e_i}$ is the factorization of the image of g in $(\mathbb{Z}/p\mathbb{Z})[x]$.

The cover $\mathrm{Spec}(\mathbb{Z}[\alpha]) \to \mathrm{Spec}(\mathbb{Z})$ is easy to understand because it is defined by the single equation $g(x)$. To give a maximal ideal $\mathfrak{p}$ of $\mathbb{Z}[\alpha]$ such that $f(\mathfrak{p}) = p\mathbb{Z}$ is the same as giving a homomorphism $\mathbb{Z}[x]/(g) \to \overline{\mathbb{F}}_p$, which is in turn the same as giving a root of g in $\overline{\mathbb{F}}_p$ (an allowed place where x can go). If the index of $\mathbb{Z}[\alpha]$ in $\mathcal{O}_K$ is coprime to p, then the primes $\mathfrak{p}_i$ in the factorization of $p\mathcal{O}_K$ don't decompose further going from $\mathbb{Z}[\alpha]$ to $\mathcal{O}_K$, so we are done (the homomorphisms $\mathbb{Z}[\alpha] \to \overline{\mathbb{F}}_p$ are in bijection with the homomorphisms $\mathcal{O}_K \to \overline{\mathbb{F}}_p$). We formalize this in the following theorem:

Theorem 2.1. *Let $g(x)$ denote the minimal polynomial of α over $\mathbb{Q}$. Let p be a prime number that does not divide $[\mathcal{O}_K : \mathbb{Z}[\alpha]]$. Suppose that*

$$\overline{g} = \prod_{i=1}^{t} \overline{g}_i^{e_i} \in (\mathbb{Z}/p\mathbb{Z})[x]$$

with the $\overline{g}_i$ distinct monic irreducible polynomials. Let $\mathfrak{p}_i = (p, g_i(\alpha))$ with $g_i \in \mathbb{Z}[x]$ any polynomial whose image is $\overline{g}_i$ in $(\mathbb{Z}/p\mathbb{Z})[X]$. Then

$$p\mathcal{O}_K = \prod_{i=1}^{t} \mathfrak{p}_i^{e_i}.$$

Geometrically,

$$f^{-1}(p\mathbb{Z}) = \{\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_t\},$$

(with multiplicities e_i).

3 Method that Always Works

Unfortunately, there are numbers fields K such that $\mathcal{O}_K$ is not of the form $\mathbb{Z}[\alpha]$ for any $\alpha \in K$. Even worse, Dedekind found a field K such that $2 \mid [\mathcal{O}_K : \mathbb{Z}[\alpha]]$ for *all* $\alpha \in \mathcal{O}_K$, so Theorem 2.1 can not be used to factor 2 (see Example 4.2 below).

I looked in a large handful of algebraic number theory books, and found only one (see [1, §6.2]) that reports on how to solve the general problem of computing the maximal ideals of $\mathcal{O}_K$ over a given prime p. In general, this appears to be a surprising problem, in the sense that the algorithms to solve it are much more sophisticated than Theorem 2.1. However, these complicated algorithms all run very quickly in practice.

For simplicity we consider the following slightly easier problem, whose solution contains the key ideas. Let $\mathcal{O}$ be any *order* in $\mathcal{O}_K$, i.e., a subring of $\mathcal{O}_K$ such that the additive abelian group $\mathcal{O}_K/\mathcal{O}$ is finite. Let $[\mathcal{O}_K : \mathcal{O}] = \#(\mathcal{O}_K/\mathcal{O})$.

Problem 3.1. For any prime $p \in \mathbb{Z}$, compute the set of maximal ideals of $\mathcal{O}$ that contain p.

Solution (sketch).

Let $K = \mathbb{Q}(\theta)$ be a number field given by an algebraic integer θ as root of its minimal monic polynomial F of degree n. We assume that an order $\mathcal{O}$ has been given by a basis $\omega_1, \ldots, \omega_n$ and that $\mathcal{O}$ that contains $\mathbb{Z}[\theta]$.

Given a prime number $p \in \mathbb{Z}$, the following (*sketch* of an) algorithm computes the primes $\mathfrak{p}_i \in \mathrm{Spec}(\mathcal{O})$ lying over p, i.e., the maximal ideals $\mathfrak{p}_i$ of $\mathcal{O}$ that contain p. Each of the following steps can be carried out very efficiently using little more than linear algebra over $\mathbb{F}_p$. The details are in [1, §6.2.5].

1. [Check if easy] If $p \nmid \mathrm{disc}(\mathbb{Z}[\theta])/\mathrm{disc}(\mathcal{O})$ then by a slight modification of Theorem 2.1, we easily factor $p\mathcal{O}$.

2. [Compute radical] Using linear algebra over the finite field $\mathbb{F}_p$, compute a basis for $I/p\mathcal{O}$, where I is the radical of $p\mathcal{O}$. (The *radical* of $p\mathcal{O}$ is the ideal of elements $x \in \mathcal{O}$ such that $x^m \in p\mathcal{O}$ for some positive integer m.)

3. [Compute quotient] Compute an $\mathbb{F}_p$ basis of
$$A = \mathcal{O}/I = (\mathcal{O}/p\mathcal{O})/(I/p\mathcal{O}).$$

4. [Decompose] Decompose A as a product $A \cong \prod \mathbb{F}_p[x]/g_i(x)$ of fields.

5. [Compute the maximal ideals] Each maximal ideal $\mathfrak{p}_i$ lying over p is the kernel of $\mathcal{O} \to A \to F_p[x]/g_i(x)$.

4 Essential Discriminant Divisors

Definition 4.1. A prime p is an *essential discriminant divisor* if $p \mid [\mathcal{O}_K : \mathbb{Z}[\alpha]]$ for *every* $\alpha \in \mathcal{O}_K$.

Example 4.2 *(Dedekind).* Let $K = \mathbb{Q}(\theta)$ be the cubic field defined by the polynomial $f = x^3 + x^2 - 2x + 8$. We will use MAGMA, which implements the algorithm described in the previous section, to show that 2 is an essential discriminant divisor for K.

```
> K := NumberField(x^3 + x^2 - 2*x + 8);
> OK := MaximalOrder(K);
> Factorization(2*OK);
[
<Prime Ideal of OK
Basis:
[2 0 0]
[0 1 0]
[0 0 1], 1>,
<Prime Ideal of OK
Basis:
[1 0 1]
[0 1 0]
[0 0 2], 1>,
<Prime Ideal of OK
Basis:
[1 0 1]
[0 1 1]
[0 0 2], 1>
]
```

Thus $2\mathcal{O}_K = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3$ with the $\mathfrak{p}_i$ distinct and $\mathcal{O}_K/\mathfrak{p}_i \cong \mathbb{F}_2$. If $\mathcal{O}_K = \mathbb{Z}[\alpha]$ for some $\alpha \in \mathcal{O}_K$ with minimal polynomial g, then $\overline{g}(x) \in \mathbb{F}_2[x]$ must be a product of three *distinct* linear factors, which is impossible.

References

[1] H. Cohen, *A course in computational algebraic number theory*, Springer-Verlag, Berlin, 1993.

[2] D. Eisenbud and J. Harris, *The geometry of schemes*, Springer-Verlag, New York, 2000.

[3] A. K. Lenstra and H. W. Lenstra, Jr. (eds.), *The development of the number field sieve*, Springer-Verlag, Berlin, 1993.