Notes for Cryptography

Professor Brian Sittinger

2/22/16

1 Introduction

We will have our midterm in two weeks. For problem 2 of HW4, the basis should be fairly obvious, but we need to be clear why it works. The norm should serve to rule out almost everything. Number 3 is grizzly. The discriminant is not square free:

$$\Delta[1, \sqrt{2}, \sqrt{3}, \sqrt{6}] = 2^{10} \cdot 3^2$$

$$\alpha = (1/3)(a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}), a, b, c, d \in 0, 1, 2$$

Roughly 82 choices.

$$\sigma_1 : \sqrt{2} \to \sqrt{2}, \text{etc}$$

$a = 0$ which reduces this to 21 solutions. This is true since $T(a\alpha) \in \mathbb{Z}$. Then we find that $c = 0$ from

$$\alpha + \sqrt{2}(\alpha) = (1/3)(2c\sqrt{3})$$

being an algebraic integer of the form $\mathbb{Z}[\sqrt{3}]$. Furthermore we see that b and d are both 0 since

$$\alpha + \sigma_3(\alpha) = (1/3)2b\sqrt{2}$$

is an algebraic int in $\mathbb{Z}[\sqrt{2}]$. So we want

$$\alpha = \frac{d\sqrt{6}}{3}$$

is an algebraic integer (in $\mathbb{Z}[\sqrt{6}]$). Note that the $1/2$ case is an algebraic integer. New potential basis

$$\{1, 2, 3, (1/2)(\sqrt{2} + \sqrt{6})\}$$

Use MATLAB/python — we can use some hand waving this time only. We could have replaced $\sqrt{2}$ instead of $\sqrt{6}$ too. For number 7, they are essentially the Eisenstein integers, and we should have 6 of them. The new homework has been posted.

2 Quadratic/Cyclotomic Rings

Quadratic and cyclotomic rings are two sets with non-empty intersect. Some elements are

$$\mathbb{Z}[i], \mathbb{Z}\left[\frac{-1+\sqrt{-3}}{2}\right]$$

which are the Gaussian and Eisensteinian integers.

3 Chapter 4 — Factorization into Irreducibles

More about units and associates. We define u is a *unit* in ring R iff $u^{-1} \in R$ or $(\exists v \in R, uv = 1)$. Let x, y be two elements in R. Then x, y are *associates* iff

$$x = uy$$

for some unit $u \in R$. We denote the *group of units* in R as either $U(R)$ or R^*. For example

$$\mathbb{Z}^* = \{\pm 1\}$$
$$\mathbb{Z}[i]^* = \{\pm 1, \pm i$$
$$\mathbb{Z}\left[\frac{-1+\sqrt{-3}}{2}\right]^* = \{\pm 1, \pm\omega, \pm\omega^2\}$$
$$K^* = K \setminus \{0\}$$

Where K is a field.

Let D be an integral domain. Integral domains have the zero product property. Then

$$x \in D^* \equiv x|1$$

and x and y are associates iff $x|y$ and $y|x$. An associate of an irreducible element is also irreducible. An element is irreducible if factors are units or associates of itself. For example, in $\mathbb{Z}$, 7 is irreducible since it only has $\pm 7, \pm 1$ as factors.

3.1 Ideals

Let $x, y \in D$ be non-zero and D be an integral domain. Then "to contain is to divide."

$$\langle x \rangle \supseteq \langle y \rangle \Leftrightarrow x|y$$

We prove this below. Let $x|y$ Then $y = rx$ for some $r \in D$. Let $\langle a \rangle = \{ar | r \in R\}$. Thus $\langle x \rangle \supseteq \langle y \rangle$. Fortunately, all these steps are indeed reversible. Thus this proof is complete. For example, in $\mathbb{Z}$, consider 2 and 4. Then $2|4$ and $\langle 2 \rangle \supseteq \langle 4 \rangle$.

Now is x and y are associates, then

$$\langle x \rangle = \langle y \rangle$$

This flows directly from the definition of associates. Now $x \in D^*$ is equivalent to saying that $\langle x \rangle = D$. Furthermore iff x is irreducible, then $\langle x \rangle$ is maximal among proper principles ideals in D. An ideal is maximal if there is no ideal between it and the ring D. Check mathworld for details.

3.2 Norms

Theorem: Let $\mathcal{O}$ be the set of integers in K. Let $x, y \in \mathcal{O}$. Then

$$x \in \mathcal{O} \iff N(x) = \pm 1$$

$$x|y \implies N(x)|N(y)$$

The proof is something like this: $y = rx$ for some $r \in \mathcal{O}$. So, $\sigma_i(y) = \sigma_i(rx) = \sigma_i(r)\sigma_i(x)$ for all embeddings σ_i. Multiply through i to see that $N(y) = N(r)N(x)$. However, the converse to this theorem is untrue. Consider $\mathbb{Z}[i] : N(2 \pm i) = 5$. However, $(2+i) \nmid (2-i)$ and $N(2+i) \mid N(2-i)$.

If x, y are associates, then $N(x) = \pm N(y)$. This is again, unidirectional, and it flows from the definition of associates.

If $N(x)$ is prime, then x is irreducible. Primallity is defined in $\mathbb{Z}$. Suppose that $x = yz$ for some $y, z \in \mathcal{O}$. We then take the norm. Then

$$N(x) = N(y)N(z)$$

which is a contradiction unless $N(y)$ or $N(z)$ is ± 1. Thus one is a unit, and the other is an associate.

3.3 Existence of Factorizations into Irreducible Elements

For example, let $\alpha \in B \setminus (B^* \cup \{0\})$, where B is any algebraic integer over $\mathbb{Q}$. Since $\alpha = (\sqrt{\alpha})^2$, and $\sqrt{\alpha} \in B.$, α is not irreducible. So B has no irreducible elements. This is not the case in $\mathcal{O}$ for some number field K. We define an integral domain is *Noetherian* iff it satisfies the "ACC" that every ascending chain of ideals is terminates. This is equivalent to saying that every ideal is finitely generated. $\mathbb{Z}$ is Notherian, since all ideals are principle (1 generator). Consider $\langle 48 \rangle$. Then

$$\langle 48 \rangle \subset \langle 24 \rangle \subset \langle 12 \rangle \subset \langle 6 \rangle \subset \langle 2 \rangle \subset \langle 1 \rangle$$

A hint for the homework is "missisippi." An important note: Noetherian rings have factors into irreducible elements. We care about this because it turns out that $\mathcal{O}$ is Noetherian and relates in some way to Dedicand domains. But we will return to this later. We know that $\mathcal{O}$ is Noetherian because $(\mathcal{O}, +)$ has an integral basis of degree $n = [k : \mathbb{Q}]$ Therefore free Abelian group of rank n. So, any ideal $I \subseteq \mathcal{O}$ has an integral basis of at most n elements.

3.4 Primes vs Irreducible Elements

Let D be an integral domain. $x \in D_{\neq 0}$ is called *prime* iff

$$x|ab \implies x|a \text{ or } x|b$$

Note that Primes are irreducible. This is because if x is prime, and $x = ab$, then $x|ab$ and if $x|a$, $a = xc, c \in D$ then $x = ab = xcb$ and $1 = cb$ and

b is a unit, which makes x irreducible. The converse is false ($\mathbb{Z}[\sqrt{-5}]$). In an integral domain D where there exists factorization into irreducibles, this factorization is unique iff if each irreducible is prime. We show this by supposing that each irreducible is prime. We consider 2 factorizations are identical. Let $x = u_1 p_1 \dots p_m = u_2 q_1 \dots q_m$ where $u_1, u_2 \in D^*, p_1, \dots, p_m, q_1, \dots q_n$ are primes in D. This is trivially true for $m = 0$. We then prove this by induction. We may cancel out some prime factors. Ergo we see that $m = n$ and that the factorization is unique. Now we assume unique factorization into irreducibles, and show that each irreducible is prime. Suppose $p \in D$ is irreducible, suppose $p|ab$ and a, b is nonzero. So $ab - pc$ for some $c \in D$ Factor into irreducibles,

$$p(u_1, r_1 \dots r_s) = (u_2 p_1 \dots p_m)(u_3 q_1 \dots q_n)$$

At this point we apply the unique factorization as we assumed. Then p is an associate to one of p_i, q_j. Therefore, $p \mid a$ or $p \mid b$ respectively.

Consider this example (cultural note), how many quadratic number rings case with unique factorization: Gaussians, Eisensteinians, $d = -1, -2, -3, -7, -11, -19, -43, -67, -163$ and that's all! Gaussian is $d = -1$ and Eisensteinian is $d = -3$. In the Real numbers, this list is unknown. For example, all square free integers under 50 except 10, 15, 26, 30, 34, 35, 39, 42. The first positive prime d for which we lose factorization is 79. Moving onto the cyclotomics, the first root of unity for which we lose unique factorizations if 23.

We now consider Euclidean Domains, which is defined as an integral domain for which there exists ϕ such that

$$\phi : D_{\neq 0} \to \mathbb{N}$$

such that if $a|b$, $a, b \in D_{\neq 0}$, then $\phi(a) \leq \phi(b)$. Furthermore for $a, b \in D_{\neq 0}$ there exists $g, r \in D$ such that

$$a = bq + r$$

where $r = 0$ or $\phi(r) \leq \phi(b)$. For example, $\mathbb{Z}$ is Euclidean with $\phi(n) = |n|$. Also $k[x]$ is Euclidean with $\phi(p(x)) = \deg(p(x))$ where k is a field. Euclidean domains are principle ideal domains. That is, given two elements in the idea, we may use the Euclidean algorithm to find the principle generator. And so, as a principle ideal domain, we are also in a unique factorization domain. Consider the Imaginary Quadratic case. This is euclidean iff $d = -1, -2, -4, -7, -11$ with $\phi(\alpha) = N(\alpha)$. Corollary: If $d = -19, -43, -67, -163$, then $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ but is still a UFD. We show this by showing that ϕ satisfies some of the required properties. $a|b \implies N(a) < N(B)$ and that for any $\epsilon \in \mathbb{Q}(\sqrt{d})$, there exists $\kappa \in \mathcal{O}$ such that $N(\epsilon - \kappa) < 1$ which is equivalent to the second rule. Suppose $\epsilon = r + s\sqrt{d}$ where $d < 0, r, s \in \mathbb{Q}$. Case 1: $d \neq 1 \pmod 4$. For κ we take $x, y \in \mathbb{Z}$ as the integers closest to r, s respectively. $|x - r|, |y - s| \leq 1/2$. So we let $\kappa = x + y\sqrt{d}$. From this we calculate the norm, and see that

$$N(\kappa - \epsilon) = 3/4 < 1$$

as required. Case 2:

$$d = 1 \pmod 4$$

We let

$$\kappa = x + y\left(\frac{1+\sqrt{d}}{2}\right), x, y \in \mathbb{Z}$$

So we find

$$N(\kappa - \epsilon) = (r - x - y/2)^2 + |d|(s - y/2)^2$$

Pick y closest to $2s$, or $|2s-y| < 1/2$ and then find $x \in \mathbb{Z}$ such that $|r-x-y/2| < 1/2$. And so we see that

$$N(\kappa - \epsilon) < (1/2)^2 + \frac{11}{4}\left(\frac{1}{2}\right)^2 = 15/16 < 1$$

We now consider an example of factoring in $\mathbb{Z}[i]$. We factor $4 + 7i$. First we use the Norm, $N(4+7i) = 5 \cdot 13$. Note that 2 is no longer prime: $2 = (1+i)(1-i)$. Note that

$$p \equiv 3 \pmod 4$$

are still prime in $\mathbb{Z}[i], N(p) = p^2$. However

$$p \equiv 1 \pmod 4$$

can be factored. Primes with norm 5, $5 = (2+i)(2-i)$. We must try all factors (using trial and error) to find the one that works. Note that the factorization is not unique, but that is not important.

$$\frac{4+7i}{2+i} = 3 + 2i$$

$$N(5)N(13) \equiv 1 \pmod 4$$

so we know that that we have the prime factors $(2+i)(3+2i)$