Notes for Cryptography

Professor Brian Sittinger

3/7/16

1 Introduction

The midterm was released today. Attach all code files. For problem 1, give the polynomial. One direction is easier. This is over $\mathbb{Q}$. For Part b, don't do a proof by induction. Just show the relevant facts.

For Problem 2, we need to show that the polynomial is minimal. For Part d, part c might have something to do with it. Part d should have actual cube roots or something. If you have one unit, you can find the other one for "free." If you get truly desperate, you can search with a computer.

For question 3, don't work harder than you need to.

For question 4, no prime ideals or extra stuff.

For Number 5, you can use multiplicitivity of norms. For part c, use something similar. The primes of the form n^2 is a good reference for this.

For question 7, you may want to use the sum of finite geometric series. This exam is due next Monday at 7pm sharp.

The Homework

Problem 3, use the LCM GCD theorem. Lemma 5.8 in the textbook. Problem 6,

$$[K : \mathbb{Q}] = n$$

$$m \in \mathbb{Z}$$

So, $\langle m \rangle \subseteq \mathcal{O}[ideal]$, so show that

$$\mathfrak{N}(\langle m \rangle) = |m|^n$$

Let $\{\omega_1, \ldots, \omega_n\}$ be an integer basis for K, Then $\{mw_1, \ldots, m\omega_n\}$ is a $\mathbb{Z}$ basis for $\langle m \rangle$ So, $\Delta[m\omega_1, \ldots, m\omega_n] = (m^n)^2 \Delta[\omega_1, \ldots, \omega_n]$. So,

$$\mathfrak{N}(\langle m \rangle) = \left(\frac{\Delta[\omega_1, \ldots, \omega_n]}{\Delta_k} \right)^{1/2} = |m|^n$$

A relevant aside: regarding, $\langle 2, 1 + \sqrt{-5} \rangle$ having norm 2, in $\mathbb{Z}[\sqrt{-5}]$. We claim that $\{2, 1 + \sqrt{-5}\}$ is a $\mathbb{Z}$ basis for $\mathfrak{p}$. $\langle 2, 1 + \sqrt{-5} \rangle$ is created from linear

combinations from $\mathbb{Z}$. We write $\alpha = a + b\sqrt{-5},\ \beta = c + d\sqrt{-5}, a, b, c, d \in \mathbb{Z}$.
Then

$$2\alpha+(1+\sqrt{-5})\beta = (2a+2b\sqrt{-5})+[(c-5d)+(c+d)\sqrt{-5}] = (a-3d-b)\cdot 2+(2b+c+d)(1+\sqrt{-5})$$

Then

$$\Delta[2, 1+\sqrt{-5}] = \begin{vmatrix} 2 & 1+\sqrt{-5} \\ 2 & 1-\sqrt{-5} \end{vmatrix}^2$$

The field discriminent, $\Delta_k = 5 \cdot (-5)$ since $-5 \not\equiv 1 \pmod 4$. Therefore

$$\mathfrak{N}(\mathfrak{p}) = \left(\frac{\Delta[2, 1+\sqrt{-5}]}{\Delta_k} \right)^{1/2} = 2$$

Alternatively,

$$\mathfrak{N}(\mathfrak{p}) = \left|\mathbb{Z}[\sqrt{-5}]/\mathfrak{p}\right| = \left|\mathbb{Z}[\sqrt{-5}]/\langle 2, 1+\sqrt{-5}\rangle\right| =^{\text{isomorphic}} \left|\mathbb{Z}_2[\sqrt{-5}]/\langle 1+\sqrt{-5}\rangle\right| = |\{0,1\}| = 2$$

Also, for one problem on the HW, we should note that

$$\mathfrak{N}(\mathfrak{p}_1, \ldots, \mathfrak{p}_r) = 2 \cdot 3\dot{c}5^2$$

Therefore

$$\mathbb{Z}[\sqrt{-2}] \text{ is a UFD, and so PID}$$

For any $\mathfrak{p} \subset \mathbb{Z}[\sqrt{-2}], \mathfrak{p} = \langle a + b\sqrt{-2}\rangle, a, b \in \mathbb{Z}$, therefore $N(\mathfrak{p}) = a^2 + 2b^2$.

$$a^2 + 2b^2 = 2 \implies a = 0, b = \pm 1$$

$$a^2 + 2b^2 = 3 \implies a = \pm 1, b = \pm 1$$

$$a^2 + 2b^2 = 5 \implies a = \pm 5, b = 0 \implies \langle 5\rangle$$

so these are the only possible ideals for primailty?

2 Summary

If $\mathcal{O}$ has unique factorsization into irreducible elements, then these are all primes. And, factorization of elmeents is roughly equivalent to factorization of principle ideals. On the other hand, if $\mathcal{O}$ lacks unique factorization, of elements, then some irreducible of elements, then some irreducible elements are not prime. Any non-prime irreducible generates a principle ideal which properly factors into non-principle ideals (with two generators).

This begets the following questions: Are primes in $\mathbb{Z}$ still primes in $\mathcal{O}$? What do the prime ideals look like. With this in mind, we now turn to

Theorem 10.1 (Dedikind): Let $[K : \mathbb{Q}] = n$ with $\mathcal{O} = \mathbb{Z}[\theta]$ for some $\theta \in \mathcal{O}$. Given, a rational prime p, suppose that the minimal polynomail f of θ over $\mathbb{Q}$ factors in $\mathbb{Z}_p$ as follows. $\bar{f} = \bar{f}_1^{e_1} f_2^{e_2} \ldots f_r^{e_r} \pmod p, \bar{f}_1, \ldots, \bar{f}_r$ are monic and irreducible in $\mathbb{Z}_p[x]$. Note that our book forgot to state monic here. Then $\langle p\rangle = \mathfrak{p}_1^{e_1} \ldots \mathfrak{p}_r^{e_r}$. Where $\mathfrak{p}_k = \langle p, f_k(\theta)\rangle$ prime in $\mathcal{O}$.

Lets look at some examples. Lets look at $\mathbb{Z}[\sqrt{-5}]$, with $\mathcal{O} = \mathbb{Z}[\sqrt{-5}]$. Minimal polynomial for $\sqrt{-5}$ is $x^2 + 5$. Now let us look at

$$\langle 2 \rangle$$

Thus, I factor the minimum polynomial mod 2, and see that

$$x^2 + 5 \equiv x^2 + 2x + 1 \pmod{2}$$

We can see that $x = 1$ is a zero, so $x - 1$ is a factor. The other factor is $x + 1$ is a factor too. This can be factored easily. By Dedicand, we see that $\langle 2 \rangle = \mathfrak{p}\mathfrak{p} = \mathfrak{p}^2, \mathfrak{p} = \langle 2, \sqrt{-5} + 1 \rangle$

Time for a new example, $\langle 3 \rangle$. This has the minimal polynomial mod 3 is

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

So

$$\langle 3 \rangle = \mathfrak{p}_1\mathfrak{p}_2$$

Where $\mathfrak{p} = \langle 3, \sqrt{-5} - 1 \rangle = \langle 3, 1 - \sqrt{-5} \rangle$.

Yet another example: $\langle 5 \rangle$. The minimum polynomial is

$$x^2 + 5 \equiv x^2 \pmod{5}$$

so

$$\langle 5 \rangle = \mathfrak{p}^2 = \langle 5, \sqrt{-5} \rangle = \langle \sqrt{-5} \rangle$$

Now we try 7, so

$$x^2 + 5 \equiv (x - 3)(x + 3) \mod 7$$

So

$$\langle 7 \rangle = \langle 7, \sqrt{-5} + 3 \rangle \langle 7, \sqrt{-5} - 3 \rangle$$

Now lets consider

$$x^2 + 5 \pmod{11}$$

which is irreducible, since none of $0, \pm 1, \pm 2, \pm 3, \pm 4, \pm 5$ are roots. So 11 is still prime! Thus 11 is a prime that is *inert*.

Note that the field discriminant is -20, so 2 and 5 are special cases. The discriminant says something about ramification.

Example,

$$K = \mathbb{Q}, \mathcal{O} = \mathbb{Z}[i]$$

with minimum polynomial $x^2 + 1$, so if $p = 2$,

$$x^2 + 1 \equiv x^2 - 1 \pmod{2}$$

so $\langle 2 \rangle = \langle 1 + i \rangle^2$ since $2 = (1 - i)(1 - i)$.

Let p be odd, then the minimum polynomial mod p is

$$x^2 + 1 \pmod{p}$$

This factors iff $x^2 = -1 \pmod{p} \iff p = 1 \pmod{4}$. We prove this by contraposition. Thus $x^2 + y^2 = p$ has no integer solution. Suppose that $p \equiv 1 \pmod{4}$ so $p = 4n + 1, n \in \mathbb{N}$, so we claim that $x = (2n)! \mod p$ is a solution. Note that

$$-1 \equiv (p-1)! \equiv (4n)! \mod p$$

by Wilson's theorem. And thus

$$\equiv (2n)!(p-1)(p-2)\dots(p-2n) \equiv (2n)!(4n-1)\dots(2n+1) \equiv (2n)![(-1)^{2n}(2n)! \equiv [(2n)!]^2 \mod p$$

So,

$$\langle p \rangle = \langle p, i^2 + 1 \rangle \text{ if } p \equiv 3 \pmod{4}$$
$$\langle p \rangle = \langle p, \mathfrak{p}_1\mathfrak{p}_2 \rangle \text{ if } p \equiv 1 \pmod{4}$$

Where $\mathfrak{p}_1\mathfrak{p}_2 = \langle p, i \pm \lambda \rangle$ where

$$x^2 + 1 - (x - \lambda)(x + \lambda) \pmod{p}$$

Note that $\mathbb{Z}[i]$ being PID implies that $\mathfrak{p}_1\mathfrak{p}_2$ are actually principle ideals.

The result of all this is Legendre's symbol. Suppose that $p \nmid d$

$$\left(\frac{d}{p}\right) \equiv +1 \text{ if } x^2 \equiv d \pmod{p} \text{is solvable}$$

$$\left(\frac{d}{p}\right) \equiv -1 \text{ if } x^2 \equiv d \pmod{p} \text{is not solvable}$$

Let p be an odd prime. $\Delta =$ discrim of $\mathcal{O}(\sqrt{d})$, suppose if $p|\Delta$ then $\langle p \rangle = \mathfrak{p}^2$ for some prime ideal $\mathfrak{p} \subseteq \mathcal{O}$. If $p \nmid \Delta$ and $\left(\frac{d}{p}\right) = -1$ then $\langle p \rangle$ is still prime in $\mathcal{O}$. If $p \nmid \Delta$ and $\left(\frac{d}{p}\right) = 1$, then $\langle p \rangle = \mathfrak{p}_1\mathfrak{p}_2$ for some distinct prime ideals $\mathfrak{p}_1 p_2 \in \mathcal{O}$. Proposition: int he $p = 2$ case, for $\mathbb{Q}(\sqrt{d})$, d is square free. If $2 \mid \Delta$, then $\langle 2 \rangle = \mathfrak{p}^2$ for some prime $\mathfrak{p} \subseteq \mathcal{O}$.

If $2 \nmid \Delta$ and $d \equiv 5 \pmod{8}$ then $\langle 2 \rangle$ is prime in $\mathcal{O}$. If $2 \nmid \Delta$ and $d \equiv 1 \pmod{8}$ then

$$\langle 2 \rangle = \mathfrak{p}_1\mathfrak{p}_2$$

for some distinct primes $\mathfrak{p}_1, \mathfrak{p}_2 \subseteq \mathcal{O}$.

Reminder: $d \not\equiv 1 \pmod{4}$ then it has a minimum poly of $x^2 - d$. If $d \equiv 1 \pmod{4}$ then the min poly is

$$x^2 - x + \frac{1-d}{4} = \frac{(2x-1)^2 - d}{4}$$

This is one of the few "nice" ways of doing this. The prime cyclotomics are also reasonable, and may be in the book.

2.1 Proof

We now proceed to the pr