# Notes for Cryptography

Professor Brian Sittinger

4/11/16

## 1 Introduction

A MIDTERM was given out today. It is due next week. We also have a progress report on our final project due the weekend after that, two weeks from today.

From the midterm, 1 puts everything together. What do quadratic number rings look like. Look into positive and negative, mod 4, etc. Keep things organized. For number 2, don't do proof by mathematica or maple. Factor using norms, or other stuff. Number 3, we can use the fact that there are infinitely many prime in $\mathbb{Z}$. Number 4 is open ended. This can be quadratic-ish or not. Number 5 and 6 are based on recent homework, or notes. It is actually dooable by hand. The degree of the extension of the 7th root of unity is 6. In part b, show the work from dedicand's theorm. Use the hint for part c! It could give it away. Number 6 gives an example of a class number of 3. For part b, list the equivalences. List use the factors. The hint for part c, lagrange's theorem, cuts through a lot of the work. You can't have something of order 3 in a group of order 4 or 5. The unit structure for the 5th cyclotomic field involves a bunch of one line answers. Problem, the fundamental unit in this cyclotomic should look suspiciously familar to a pell-like equation. Work on this on Wednesday.

From the homework, due today, we had the following questions. When finding the order of the class group, we are interested in finding the number of non-principle ideals, which generate classes, which spike the number up. Principle ideals are equavalent to $\mathcal{O}$. Non-principle ideals may be more nuanced. Just look at the prime ideals, since the other ideals just factor futher. For question 3d, for HW9: since since $p|(y^2+1)$

$$y \equiv -1 \pmod{p}$$

contradicts because of

$$-\frac{1}{p} = -1$$

if $p \equiv 3 \pmod{4}$. Due to the fact

$$y^2 \equiv -1 \pmod{p}$$

implies that $p \not\equiv 3 \pmod{4}$

2b from hw8. 2 is a square mod p implies that

$$\frac{2}{p} = +1 = (-1)\frac{p^2-1}{8}$$

is equivalent to

$$p \equiv \pm 1 \mod 8$$

quadratic residue. For problem 5. Let $\mathfrak{a} = \langle 1 \rangle = \mathcal{O}$. The norm of $\langle 1 \rangle$ is 1. So

$$1 \leq \left(\frac{4}{\pi}\right)^t \cdot \left(\frac{n!}{n^n}\right) \cdot \sqrt{|\Delta|}$$

$$n = s + t$$

Sq

$$1 \leq \left(\frac{4}{\pi}\right)^{2t} \left(\frac{n!}{n^n}\right)^2 |\Delta| \leq \left(\frac{4}{\pi}\right)^{n=s+2t} \left(\frac{n!}{n^n}\right)^2 |\Delta|$$

The norm of a non-tribal ideal is greater than equal to 1.

On hw8 Number 3. In mod 5 for square root of -19, don't you get something that factors? It is worked out in detail in the textbook.

$$t^2 - t + 5$$

Mod 5

$$t^2 - t$$

$$\mathbb{Z}[\frac{1+\sqrt{-19}}{2}]$$

$$\langle 5 \rangle = \langle 5, \frac{1+\sqrt{-19}}{2} \rangle \langle 5, \frac{-1+\sqrt{-19}}{2} \rangle$$

## 2 More About Prime Decompositions

Not in the textbook! We operate over $\mathbb{Q}$ as usual. Recall that a any rational prime decomposes uniquely.

$$\langle p \rangle = \mathfrak{p}_1^{e_1} \dots \mathfrak{p}_g^{e_g}$$

for prime ideals $\mathfrak{p}_i$ and positive integers $e_i$ $1 \leq i \leq g$. A note:

$$\mathfrak{p}_k \cap \mathbb{Z} = \langle p \rangle$$

for each $k, 1 \leq k \leq g$. Note that the name of the $e$s are "ramification indecies" of $\mathfrak{p}_k$ over $q$. Furthermore, $f_k$ is an intertial degree iff

$$f_k = [\mathcal{O}/\mathfrak{p}_k : \mathbb{Z}/p\mathbb{Z}]$$

We then define the following theorem.

$$\sum_{k=1}^{q} = e_k f_k = [k : \mathbb{Q}] = n$$

Example: A quadratic field $n = 2$. There are 3 types of behaviour for $\langle p \rangle$.

If they are inert $\langle p \rangle$ still prime in $\mathcal{O}$. So $e = 1$. Therefore $f = 2$. This is the case because $e_1 = 1$ which implies that $f_1 = 2$ by the previous theorem. We can double check this easil

$$\mathfrak{N}(\langle p \rangle) = p^2$$

$$|\mathcal{O}/\langle p \rangle|$$

$$g = 1$$

If they are split,

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

$$g = 2$$

So,

$$e_1 = e_2 = 1$$

Therefore

$$f_1 = 1 = f_2$$

Since $[k : \mathbb{Q}] = e_1 f_1 + e_2 f_2$ So, we double check

$$\mathfrak{N}(\mathfrak{p}_k) = p, k = 1, 2$$

Without loss of generality

$$\mathfrak{N}(\langle p \rangle) = \mathfrak{N}(\mathfrak{p}_1 \mathfrak{p}_2)$$

$$p^2 = \mathfrak{N}(\mathfrak{p}_1)\mathfrak{N}(\mathfrak{p}_2)$$

No we look into the ramify case:

$$\langle p \rangle = \mathfrak{p}^2$$

$$g = 1$$

$$e_1 = 1$$

$$f = 1$$

As in the split case,

$$\mathfrak{N}(\mathfrak{p}) = p$$

$$\mathcal{O}/\mathfrak{p} = \{0, \dots, p - 1\}$$

We must now define some new terminology. $\langle p \rangle$ "splits completely" if $g = [k : \mathbb{Q}]$ and all

$$e_k = f_k = 1$$

$$\mathfrak{p} = \mathfrak{p}_1 \dots \mathfrak{p}_{[k:\mathbb{Q}]}$$

$\langle p\rangle$ is ramified if at least one $e_k > 1$. Furthermore, if $g = 1$ then $\langle p\rangle$ ramifies completely.

Finally, we note that $\langle p\rangle$ is inert if $g = 1$ and $e = 1, (f = n)$.

Example, from Hule. In $\mathbb{Z}[\sqrt[3]{2}], \langle 7\rangle$ is inert. $e_1 = 1, f_1 = 3$.

$$\langle 29\rangle = \mathfrak{p}\mathfrak{q}$$

$$e_1, e_2 = 1, f_1, f_2 = \{1, 2\}$$

$$\langle 31\rangle = \mathfrak{p}\mathfrak{q}\mathfrak{r}$$

$$e_1 = e_2 = e_3 = 1$$

and so

$$f_1 = f_2 = f_3 = 1$$

$n = 3$. This is not a Galois extension.

Look at $\mathbb{Q}(\alpha)$ where $\alpha^3 - \alpha - 1 = 0$.

$$[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$$

In

$$\mathcal{O}_{\zeta(n)}$$

$$\langle 23\rangle = \langle 23, \alpha - 10\rangle^{10}\langle 23, \alpha - 3\rangle = \mathfrak{p}^2 - \mathfrak{q}$$

$$e_1 = 2, f_1 = 1, e_2 = 1, f_2 = 1$$

Via dedicand's theorem.

Fact: If $K$ is a Galois extension over $\mathbb{Q}$ the Galois Group $[\mathrm{Gal}(k/\mathbb{Q})]$ permutes the prime ideals of $\mathcal{O}_k$ transitively! If $\mathfrak{p}_1, \mathfrak{p}_2$ are prime ideals above $\langle p\rangle$ then $\mathfrak{p}_2 = \sigma(\mathfrak{p}_1)$ for some $\sigma \in \mathrm{Gal}(k/\mathbb{Q})$. A corroloary of this is that if $K$ is Galois over $\mathbb{Q}$ then all prime ideals have the same ramification index and inertic degree or,

$$efg = n = [k : \mathbb{Q}]$$

Example of "nice" number fields whicha re Galois. Quadratic number fields! Cyclotomic number fields at least with $p$th root of unity $\zeta_p = e^{2\pi/p}$.

Lets look into $\mathbb{Q}(\zeta_5)$. $n = 5 - 1 = 4$. What are the possibilities?

$$\langle p\rangle = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_4$$

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

$$\langle p\rangle = \mathfrak{p}_1^4$$

Example $\mathbb{Q}(\zeta_7)$. $n = 7 - 1 = 6$. What are the possibilities?

$$\langle p\rangle = \mathfrak{p}_1^6$$

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

$$\langle p\rangle = \mathfrak{p}_1^2\mathfrak{p}_2^2\mathfrak{p}_3^2$$

$$\langle p\rangle = \mathfrak{p}_1\mathfrak{p}_2\mathfrak{p}_3\mathfrak{p}_4\mathfrak{p}_5\mathfrak{p}_6$$

Galois Cubic extension: (irreducible cubic whos discriminent is a square).

$$\mathbb{Q}(\alpha), \alpha^3 - 3\alpha - 1 = 0$$

We now do synthetic division: and see that $\alpha$ is indeed a root. Then

$$x^3 - 3x - 1 = (x-\alpha)(x^2 + \alpha x + \alpha^2 - 3)$$

This is straight off of wikipedia. We can then apply the quadratic equation, and get

$$x = \frac{-\alpha \pm \sqrt{12 - 3\alpha^2}}{2}$$

We turned to wolfram alpha, and failed. This is supposed to turn to

$$x^3 - 3x - 1 = (x-\alpha)(x - (\alpha^2 - \alpha - 2))(x - (-\alpha^2 + 2))$$

So, $\mathbb{Q}(\alpha)$ is the splittinf field of $x^3 - 3x - 1 = 0$ Therefore $\mathbb{Q}(\alpha)$ is Galois over $\mathbb{Q}$. The Prime behavior in $\mathcal{O}_{\mathbb{Q}(\alpha)}$.

$$\langle p\rangle = \mathfrak{p}^3, g = 1, e = 3, f = 1$$

or

$$\langle p\rangle = \mathfrak{p}\mathfrak{q}\mathfrak{r}, g = 3, e = f = 1$$