Notes for Cryptography

Professor Brian Sittinger

3/28/16

1 Introduction

The tests were returned today. I got 98/100, having lost 2 points on a problem for not showing enough work. The professor's office hours are at noon tomorrow.

Homework questions: For the bonus question, we suppose that there are more than two roots of unities. The key is to use the tower law.

For the project, we should clearly explain what each person did. We should also email in our topics posthaste. Our paper should be at least 5 pages. The presentation should be 5-10 minutes long, approximately. The focus should be on the paper.

The strike should occur in 2-3 weeks. It may or may not happen, and we won't have any signs of compromise until the last minute.

2 Class Group/Number

Definition 1. Let $\mathcal{O}$ be a number ring. We Define the class group $H = \mathcal{F}/\mathcal{P} = \{\text{fractional ideals in}\mathcal{O}\}/\{\text{principle fractional ideals in } \mathcal{O}\}$. This is an ebelian group. Furthermore, this is finite. And the class number $h = |\mathfrak{H}|$ is the cardinality of the class group $\mathfrak{H}$. Without fractional ideals, we may let $\mathcal{F}$ be the set of ideal in $\mathcal{O}$ and define a an equivalence relation $\sim$ on ideals such that

$$\mathfrak{a} \sim \mathfrak{b}$$

iff there exist princple ideals $(\gamma), (\delta)$ such that

$$(\gamma)\mathfrak{a} = (\delta)\mathfrak{b}$$

And this is an equivalence relation. We can see transitivity by noting that

$$\mathfrak{a} \sim \mathfrak{b} \text{ and } \mathfrak{b} \sim \mathfrak{c}$$

so

$$(\alpha)\mathfrak{a} = (\beta)\mathfrak{b} \text{ and } (\gamma)\mathfrak{b} = (\delta)\mathfrak{c}$$

And so

$$(\alpha\gamma)\mathfrak{a} = (\beta\gamma)\mathfrak{b} \text{ and } (\beta\gamma)\mathfrak{b} = (\gamma\delta)\mathfrak{c}$$

so $\mathfrak{a} \sim \mathfrak{c}$.

So,

$$\mathfrak{H} = \{[\mathfrak{r}] \text{ with } [\mathfrak{r}][\mathfrak{s}] = [\mathfrak{r}\mathfrak{s}]\}$$

Theorem 2. *$\mathcal{O}$ has unique factorization into irreducibles iff $h = 1$*

A question: How do we compute $\mathfrak{H}$ and thus h? A fact: (the book gives two versions, this is the second one) Every equivalance class of the class group $\mathfrak{H}$ contains an ideal $\mathfrak{a}$ such that

$$\mathfrak{N}(\mathfrak{a}) \leq \left(\frac{4}{\pi}\right)^t \frac{n!}{n^n}\sqrt{|\Delta|}, n = s + 2t$$

Note that if the right side of the inequality is smaller, finding class groups is easier, since we have less "stuff to check."

Example 3. $\mathbb{Z}[\sqrt{-5}]$. We already know that $h > 1$ since this is not a unique factorization domain. Here, $n = 2$ since this is a quadratic extension, $s = 0, t = 1, \Delta = 4 \cdot -5 = -20$. So

$$\mathfrak{N}(\mathfrak{a}) \leq \left(\frac{4}{\pi}\right)^1 \frac{2!}{2^2}\sqrt{|20|}$$

So

$$\mathfrak{N}(\mathfrak{a}) = 1 \text{ or } 2$$

But $\mathfrak{N}(\mathfrak{a}) \neq 1$, since then $\frac{a}{=}\mathcal{O}$. So, $\mathfrak{N}(\mathfrak{a}) = 2$. Since $\mathfrak{a} \mid \langle 2\rangle$, $\mathfrak{a}$ is a factor of $\langle 2\rangle$. That is, the class group is generated by primes dividing $\langle 2\rangle$. Now we use Dedicand to factor $\langle 2\rangle$. The minimal polynomial of $\sqrt{-5}$ is x^2+5. So we reduce, $x^2 + 5 \pmod 2 \equiv x^2 - 1 \equiv (x + 1)^2$. So

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

so this is the only ideal with norm 2. So

$$\mathfrak{H} = \{[\mathcal{O}], [\langle 2, \sqrt{-5} + 1]\}$$

and $\mathfrak{H}$ is irreducible into fewer elements. So $h = |\mathfrak{H}| = 2$.

In the homework, we must finish up the list of 9 imaginary quadratic rings. We showed at least 3 or 4 of them earlier, but now we do the rest.

Example 4.

$$\mathbb{Z}[\frac{1 + \sqrt{-163}}{2}]$$

$n = 2, s = 0, t = 1, \Delta = -163 \equiv 1 \pmod 4$ So,

$$\mathfrak{N}(\mathfrak{a}) \leq (4\pi)\frac{2!}{2^2}\sqrt{163} \approx 8.1$$

We eliminate possible norms 1, 6, and 8. The minimum polynomial is

$$t^2 + t + (1 + 163)/4 = t^2 + t + 41$$

We first consider 2:

$$t^2 + t + 1 \mod 2$$

is irreducible. So,

$$\langle 2 \rangle = \langle 2, \alpha^2 + \alpha + 1 \rangle$$

where $\alpha = (1 + \sqrt{-163})/2$. This is intert, so in particular,

$$\langle 2 \rangle \sim \langle 1 \rangle$$

which is principal. This also eliminates 4 from our list.

We now check $\mod 3$. Now

$$t^2 + 2 + 2$$

is irreducible. So similarly,

$$\langle 3 \rangle = \langle 3, \alpha^2 + \alpha + 2 \rangle$$

for appropriate α. This also inert, so

$$\langle 3 \rangle \sim \langle 1 \rangle$$

Similarly for $\langle 5 \rangle$ and $\langle 7 \rangle$. Therefore

$$\mathfrak{H} = \langle \{[\mathcal{O}]\}, h = 1$$

Example 5. $\mathbb{Z}[\sqrt{-14}], s = 0, t = 1, \Delta = 4 \cdot -14 = -56$ since $14 \not\equiv 1 \pmod 4$. So,

$$\mathfrak{N}(\mathfrak{a}) \leq \left(\frac{4}{\pi}\right)^1 \frac{2!}{2^2}\sqrt{|56|} \approx 4.8$$

So, each ideal $\sim \mathfrak{a}$ with $\mathfrak{N}(\mathfrak{a}) < 4.8$, implies that the class group is generated by primes dividing $\langle 2 \rangle$ and $\langle 3 \rangle$.

p	$t^2 + 14$	$\langle p \rangle$ factors
2	t^2	$\langle 2, \sqrt{-14} \rangle^2$
3	$t^2 - 1$	$\langle 3, \sqrt{-14} - 1 \rangle \langle 3, \sqrt{-14} + 1 \rangle$

So, $\mathfrak{H}$ is generated by $[\mathcal{O}], \mathfrak{p}_2, \mathfrak{p}_3, \mathfrak{p}_3'$. Question, does this list reduce at all? We use lagrange to note that $h \leq 4$. First we check the orders: since $\mathfrak{p}_2^2 = \langle 2 \rangle$, and so $\mathfrak{p}^2 \sim \langle 1 \rangle$ ($\mathfrak{p}_2$ has order 2). Moreover $h \neq 1$, $\mathfrak{p}_2$ is not principle. $N(a + b\sqrt{-14}) = a^2 + 14b^2 = 1$ has no integer solutions. Morover,

$$\mathfrak{p}_3\mathfrak{p}_3' = \langle 3 \rangle \implies \mathfrak{p}_3\mathfrak{p}_3' \sim \langle 1 \rangle \implies \mathfrak{p}_3 \sim (\mathfrak{p}_3')^{-1}$$

Check

$$\mathfrak{p}_3^2 \sim \langle 1 \rangle \text{ and } \left(\mathfrak{p}_3'\right)^2 = \langle 1 \rangle$$

By mult.

$$\langle 3, 1 + \sqrt{-14} \rangle^2 = \langle 3^2, (1 + \sqrt{-14})^2, 3(1 + \sqrt{-14}) \rangle$$

A question: does there exist relations between $\mathfrak{p}_2$ and $\mathfrak{p}_3$? Answer: $N(2+\sqrt{-14}) = 18, 2 \cdot 3^2$ Since $2+\sqrt{-14}$ is not a multiple of 3,

$$\langle 2+\sqrt{-14}\rangle$$

is divisible by one of $\mathfrak{p}_3$ or $\mathfrak{p}_3'$. WLOG, let $\mathfrak{p}_3$ be the prime of the norm, an ddividing $\langle 2+\sqrt{-14}\rangle$ (principle!). Therefore,

$$\langle 2+\sqrt{-14}\rangle = \mathfrak{p}_2\mathfrak{p}_3^2 \implies \mathfrak{p}_2\mathfrak{p}_3^2 \sim \langle 1\rangle$$

And $\mathfrak{p}_2$ has order 2. Therfore,

$$\mathfrak{p}_3^2 \sim \mathfrak{p}_2[\mathfrak{H}]$$

which shows that

$$\mathfrak{H} = \langle[\mathfrak{p}_3]\rangle \cong \mathbb{Z}_4$$

We know that $\mathfrak{p}_3$ has order 4, since $2^2 = 4$. So, $h = 4$.

Theorem 6. *$\mathfrak{H}$ is finite. Proof: Let $[\mathfrak{a}]$ be an equivalence class of $\mathfrak{H}$. So*

$$\mathfrak{a} \sim \mathfrak{b}$$

Where $\mathfrak{N}(\frac{b}{\leq}\left(\frac{4}{\pi}\right)^t \frac{n!}{n^n}\sqrt{|\Delta|}$ which implies that there are finitely many chices for $\mathfrak{b}$, Therefore there are finitely many choices for $\mathfrak{a}$. QED.

Proposition, let $\mathcal{O}$ have class number h and $\mathfrak{a} \leq \mathcal{O}$. Then $\mathfrak{a}^h$ is principle and if $\gcd(q,h) = 1$ and $\mathfrak{a}^q$ is principle.

$$qx + hy = 1, x, y \in \mathbb{Z}$$

So,

$$\mathfrak{a} = a^{qx+hy} = (\mathfrak{a}^q)^x \cdot (\mathfrak{a}^h)^y$$

is prime.

Theorem 7. *Let $\mathcal{O}$ be a number ring. Suppose that for all primes $p \in \mathbb{N}$ such that*

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

that every prime ideal dividing $\langle p\rangle$ is principle.There, $h = 1$, ($\mathcal{O}$ is a UFD/PID). QED.