Notes for Cryptography

Professor Brian Sittinger

4/4/16

1 Homework Questions

Question 4D — Want principle $\mathfrak{a}, \mathfrak{b}$ such that

$$\mathfrak{a}\langle 2, \sqrt{-6}\rangle = \mathfrak{b}\langle 3, \sqrt{-6}\rangle$$

$$\langle 2(a+b\sqrt{-c}), -6b + a\sqrt{-6}\rangle = \langle 3(c+d\sqrt{-6}), -6d + c\sqrt{-6}\rangle$$
$$\langle 6 + 2\sqrt{-6}, -6 + 3\sqrt{-6}\rangle = \langle -6 + 3\sqrt{-6}, -6 - 2\sqrt{-6}\rangle$$

$$\mathfrak{a} = \langle 3 + \sqrt{-6}\rangle, \mathfrak{b} = \langle 2 - \sqrt{-6}\rangle$$

In part c, we found the class number is 2.

2 Applications to Diophantine Equations

The solution of Diophantine equations involves solutions to polynomials in the integers.

2.1 Pythagorean Triples

$$x^2 + y^2 = z^2, x, y, x \in \mathbb{N}^+$$

We want *Primitive Pythagorean Triples*, or $\gcd(x, y, z) = 1$. Without loss of generality we assume x is odd, and y is even (z is odd). If they were both even, they wouldn't be primitive. If they were both odd, then $\mod 4$, then $x^2 + y^2 = 2 \mod 4$, which is impossible since squares are in $\{0, 1\} \mod 4$. We will work in $\mathbb{Z}[i]$. Then

$$(x + iy)(x - iy) = z^2$$

Suppose $\pi \in \mathbb{Z}[i]$ is a prime such that,

$$\pi \mid (x + iy), \pi \mid (x - iy)$$

Then

$$\pi \mid (x + iy) + (x - iy) = 2x$$

$$\pi \mid (x+iy)-(x-iy)=2iy$$

Since z is odd and $N(1+i)=2$

$$\pi \neq 1+i$$

Take norms:

$$N(\pi) \mid x^2, N(\pi) \mid y^2$$

The norm of a Gaussian prime is p or p^2, p prime in $\mathbb{Z}$. p is the splitting case, and p^2 is the inert case. If the norm is p^2, then $\pi = p$. Therefore $p \mid x, p \mid y$ and so the $\gcd(x,y) \neq 1$. So we only concern ourselves with the p case. However, we still have this same contradiction. Therefore,

$$\gcd(x+iy, x-iy)=1$$

Now, if we use a prime factorization of z in $\mathbb{Z}[i]$ the Fundamental Theorem of Arithmetic in $\mathbb{Z}[i]$ implies that $x+iy=\mu\beta^2$ for some unit $\mu \in \mathbb{Z}[i]^*$ and $\beta \in \mathbb{Z}[i]$. And $x-iy=\Delta\gamma^2$. So

$$z=\nu\beta\gamma$$

for unit ν. We then take $\mu=1$ and write $\beta=a+bi, a,b \in \mathbb{Z}$. So, $x+iy=1\cdot(a+bi)^2=(a^2-b^2)+i(2ab)$. Therefore

$$x=a^2-b^2, y=2ab, z=a^2+b^2$$

So, for primitive Pythagorean triples,

$$(x,y,z)=(a^2-b^2, 2ab, a^2+b^2)$$

Where $a,b \in \mathbb{N}^+$, with $a>b$ and a and b have different parities (one even, one odd). In the homework, we are to find the primitive Pythagorean triples with hypotenuse less than or equal to 50. There should be around 7.

3 Mordell's Equation

See the handout.

$$y^2=x^3+d$$

Here, we assume $d<0$. So we rewrite to

$$x^3=y^2+\hat{d}$$

From this point, I refer to the handout ….

For problem 7, we should just list the 4 solutions. We don't need to show that no additional solutions exist.

Suppose the we don't know the class number. Suppose we find more than 2 solutions. Then the class number has to be divisible by 3.

4 Ramenujan-Nagell Equation

On page 98-100 from the current edition (96-98 from the old edition). The integer solutions of

$$x^2 + 7 = 2^n$$

are

$$(x, n) = (\pm 1, 3), (\pm 3, 4), (\pm 5, 5), (\pm 11, 7), (\pm 191, 15)$$

We prove this as follows. Let n be even. WLOG $x \geq 0$.

$$7 = 2^n - x^2 = (2^{n/2} + x)(2^{n/2} - x)$$

Therefore

$$\begin{aligned} 7 &= 2^{n/2} + x \\ 1 &= 2^{n/2} - x \end{aligned}$$

Add them, and we see that

$$2^3 = 2^{n/2+1}$$

and that $n = 4$.

We now assume that n is odd. WLOG $n > 3$, since $n = 1, 3$ has no solution. We're now going to work in $\mathcal{O}[\frac{1+\sqrt{-7}}{2}]$ is a UFD (notorious 9!). No class number issues. Since 2^n is even, x is odd, and so

$$4 \mid (x^2 + 7)$$

Thus, we can rewrite the Ramanujan-Nagell equation as

$$\frac{x^2+7}{4} = 2^{n-2}$$

Let $m = n - 2$.

$$\left(\frac{x+\sqrt{-7}}{2}\right)\left(\frac{x-\sqrt{-7}}{2}\right) = 2^m \in \mathbb{Z}[\frac{1+\sqrt{-7}}{2}]$$

$$\left(\frac{x+\sqrt{-7}}{2}\right)^m \cdot \left(\frac{x-\sqrt{-7}}{2}\right)^m$$

Now,

$$\frac{1 \pm \sqrt{-7}}{2}$$

are not common factors of

$$\frac{x \pm \sqrt{-7}}{2}$$

Thus

$$\frac{x \pm \sqrt{-7}}{2}$$

are relatively prime. Thus

$$\frac{x \pm \sqrt{-7}}{2} = (\pm 1) \cdot \left(\frac{1 \pm \sqrt{-7}}{2}\right)^m$$

We subtract

$$\pm\sqrt{-7} = \left(\frac{1+\sqrt{-7}}{2}\right)^m - \left(\frac{1-\sqrt{-7}}{2}\right)^m$$

Let

$$a = \left(\frac{1+\sqrt{-7}}{2}\right)^m, b = \left(\frac{1-\sqrt{-7}}{2}\right)^m$$

We claim that the + sign can't occur. If we assume that

$$a^m - b^m = \sqrt{-7}$$

Since

$$ab = 2, a^2 \equiv (1-b)^2 \equiv 1 \pmod{b^2}$$

So,

$$a^m \equiv a \cdot (a^2)^{\frac{m-1}{2}} \equiv a \pmod{b^2}$$

$$a \equiv a - b \pmod{b^2}$$

Which cannot be the case, so the sign must be negative.

So we break out the binomial theorem. That is

$$-\sqrt{-7} = a^m - b^m$$

$$-2^{m-1} = \binom{m}{1} - 7\binom{m}{3} + \ldots \pm \binom{m}{m} \cdot 7^{\frac{m-1}{2}}$$

So

$$-2^{m-1} \equiv m \pmod{7}$$

$$m = 3, 5, 13 \pmod{42}$$

By the Chinese Remainder Theorem and Fermat's little theorem. The question in the homework that asks what equation this resembles is probably like the Ramanujan-Nagell Equation.