Algebraic number theory Assignment 1

N'Dah Jean KOUAGOU

January 12, 2019

1.

1.1 Five integral solutions of $x^2 - 6y^2 = 1$.

Let's find five integral solutions $x, y > 0$ of Pell equation $x^2 - 6y^2 = 1$.
We consider the ring $\mathbb{Z}[\sqrt{6}]$ and we define the norm N by :
$\forall\ \alpha = x + y\sqrt{6} \in \mathbb{Z}[\sqrt{6}], N(\alpha) = x^2 - 6y^2$. Then the set of solutions of Pell equation $x^2 - 6y^2 = 1$ is

$$S = \left\{(x, y) \in \mathbb{Z}^2 : x + y\sqrt{6} \in \mathbb{Z}[\sqrt{6}]^* \text{ and } N(x + y\sqrt{6}) = 1\right\},$$

where $\mathbb{Z}[\sqrt{6}]^*$ is the unit group of $\mathbb{Z}[\sqrt{6}]$.
$(5, 2)$ is a solution of the equation since $5^2 - 6 \times 2^2 = 1$.
$5 + 2\sqrt{6}$ is even the smallest solution with $x, y > 0$.
We can now find other solutions by taking the powers of $\epsilon = 5+\sqrt{6}$: $(5+2\sqrt{6})^2 = 49+20\sqrt{6}$; $(5+2\sqrt{6})^3 = 485+198\sqrt{6}$; $(5+2\sqrt{6})^4 = 4801+1960\sqrt{6}$; $(5+2\sqrt{6})^5 = 47525 + 19402\sqrt{6}$.
So we find the following five solutions for $x^2 - 6y^2 = 1$:

$$\left\{(5, 2), (49, 20), (485, 198), (4801, 1960), (47525, 19402)\right\}.$$

1.2 Five integral solutions of $x^2 - 6y^2 = 19$.

$(5, 1)$ is a solution of $x^2 - 6y^2 = 19$.
Let $\epsilon' = 5 + \sqrt{6}$.
Since $N(\alpha\beta) = N(\alpha)N(\beta)\ \forall\ \alpha, \beta \in \mathbb{Z}[\sqrt{6}]$ then if α is a solution of $x^2 - +y^2 = 1$ and β is a solution of $x^2 - 6y^2 = 19$ then $\alpha\beta$ is a solution of $x^2 - 6y^2 = 19$.
So we can find five solutions of $x^2 - 6y^2 = 19$ by multiplying the solutions we got above for $x^2 - 6y^2 = 1$ by $\epsilon' = 5 + \sqrt{6}$:
$(5 + \sqrt{6})(5 + 2\sqrt{6}) = 37 + 15\sqrt{6}$; $(5 + \sqrt{6})(49 + 20\sqrt{6}) = 365 + 149\sqrt{6}$;
$(5 + \sqrt{6})(485 + 198\sqrt{6}) = 3613 + 1475\sqrt{6}$; $(5 + \sqrt{6})(4801 + 1960\sqrt{6}) = 35765 + 14601\sqrt{6}$.
Therefore we have the following five solutions for $x^2 - 6y^2 = 19$**:**

$$\left\{(5, 1), (37, 15), (365, 149), (3613, 1475), (35765, 14601)\right\}.$$

2.

We define $\begin{cases} u_0 = u_1 = 1, \\ u_{k+1} = 2u_k + u_{k-1} \text{ for } k \geq 1 \end{cases}$ and $\begin{cases} v_0 = 0, v_1 = 1, \\ v_{k+1} = 2v_k + v_{k-1} \text{ for } k \geq 1. \end{cases}$

(a) Computation of u_k and v_k for $0 \leq k \leq 10$

We have using the SageMath code

```
u0 = 1
u1 = 1
for i in range(9) :
    u = 2 * u1 + u0
    u0 = u1
    u1 = u
    show(u)
```

```
v0 = 0
v1 = 1
for i in range(9) :
     = 2 * v1 + v0
    v0 = v1
    v1 = v
    show(v)
```

$u_0 = 1,\ u_1 = 1,\ u_2 = 3,\ u_3 = 7,\ u_4 = 17,\ u_5 = 41,\ u_6 = 99,\ u_7 = 239,\ u_8 = 577,\ u_9 = 1393,\ u_{10} = 3363$

and

$v_0 = 0,\ v_1 = 1,\ v_2 = 2,\ v_3 = 5,\ v_4 = 12,\ v_5 = 29,\ v_6 = 70,\ v_7 = 169,\ v_8 = 408,\ v_9 = 985,\ v_{10} = 2378.$

(b) Proof of $(1+\sqrt{2})^k = u_k + v_k\sqrt{2}$ and $u_k^2 - 2v_k^2 = (-1)^k \ \forall\ k \geq 0$.

* $(1+\sqrt{2})^k = u_k + v_k\sqrt{2}$
We have $(1+\sqrt{2})^0 = 1 = 1+0\times\sqrt{2} = u_0 + v_0\sqrt{2}$. So the formula is true for $k = 0$.
It is also true for $k = 1$ because $(1+\sqrt{2})^1 = 1+\sqrt{2} = 1+1\times\sqrt{2} = u_1 + v_1\sqrt{2}$.
Let's show the formula by induction.
Let $K \geq 1$ be an integer. Suppose we have $(1+\sqrt{2})^k = u_k + v_k\sqrt{2}$ for all integer $k : 0 \leq k \leq K$.

We have:

$$\begin{aligned}
u_{K+1} + v_{K+1}\sqrt{2} &= 2u_K + u_{K-1} + 2v_K\sqrt{2} + v_{K-1}\sqrt{2} \\
&= u_{K-1} + v_{K-1}\sqrt{2} + 2u_K + 2v_K\sqrt{2} \\
&= u_{K-1} + v_{K-1}\sqrt{2} + 2(u_K + v_K\sqrt{2}) \\
&= (1+\sqrt{2})^{K-1} + 2(1+\sqrt{2})^K \text{ because } K \geq 1 \text{ and the formula is true for all } 0 \leq k \leq K \\
&= \frac{(1+\sqrt{2})^K}{1+\sqrt{2}} + 2(1+\sqrt{2})^K \\
&= (1+\sqrt{2})^K \left(\frac{1}{1+\sqrt{2}} + 2\right) \\
&= (1+\sqrt{2})^K \left(\frac{1+2\sqrt{2}+2}{1+\sqrt{2}}\right) \\
&= (1+\sqrt{2})^K \left(\frac{(1+\sqrt{2})^2}{1+\sqrt{2}}\right) \\
&= (1+\sqrt{2})^K \left(1+\sqrt{2}\right) \\
&= (1+\sqrt{2})^{K+1}
\end{aligned}$$

As a result, we have $(1+\sqrt{2})^k = u_k + v_k\sqrt{2}$ for all integer $k \geq 0$.

* $u_k^2 - 2v_k^2 = (-1)^k$
We have $u_k^2 - 2v_k^2 = (u_k - v_k\sqrt{2})(u_k + v_k\sqrt{2}) = (1+\sqrt{2})^k(u_k - v_k\sqrt{2})$ for all integer $k \geq 0$ (using our previous proof).
So, it is sufficient to show that $u_k - v_k\sqrt{2} = (1-\sqrt{2})^k$ for all $k \geq 0$.
Just as we did above, we have $(1-\sqrt{2})^0 = 1 = 1 - 0 \times \sqrt{2} = u_0 - v_0\sqrt{2}$. So the formula is true for $k = 0$. It is also true for $k = 1$ because $(1-\sqrt{2})^1 = 1-\sqrt{2} = 1 - 1 \times \sqrt{2} = u_1 - v_1\sqrt{2}$.
Let's show the formula by induction.
Let $K \geq 1$ be an integer. Suppose we have $(1+\sqrt{2})^k = u_k + v_k\sqrt{2}$ for all integer $k : 0 \leq k \leq K$.

We have:

$$\begin{aligned}
u_{K+1} - v_{K+1}\sqrt{2} &= 2u_K + u_{K-1} - 2v_K\sqrt{2} - v_{K-1}\sqrt{2} \\
&= u_{K-1} - v_{K-1}\sqrt{2} + 2u_K - 2v_K\sqrt{2} \\
&= u_{K-1} - v_{K-1}\sqrt{2} + 2(u_K - v_K\sqrt{2}) \\
&= (1-\sqrt{2})^{K-1} + 2(1-\sqrt{2})^K \text{ because } K \geq 1 \text{ and the formula is true for all } 0 \leq k \leq K \\
&= \frac{(1-\sqrt{2})^K}{1-\sqrt{2}} + 2(1-\sqrt{2})^K \\
&= (1-\sqrt{2})^K \left(\frac{1}{1-\sqrt{2}} + 2\right) \\
&= (1-\sqrt{2})^K \left(\frac{1-2\sqrt{2}+2}{1-\sqrt{2}}\right) \\
&= (1-\sqrt{2})^K \left(\frac{(1-\sqrt{2})^2}{1-\sqrt{2}}\right) \\
&= (1-\sqrt{2})^K \left(1-\sqrt{2}\right) \\
&= (1-\sqrt{2})^{K+1}
\end{aligned}$$

Therefore we have $u_k - v_k\sqrt{2} = (1-\sqrt{2})^k$ for all integer $k \geq 0$.
It follows that for all integer $k \geq 0$,

$$\begin{aligned}
u_k^2 - 2v_k^2 &= (u_k + v_k\sqrt{2})(u_k - v_k\sqrt{2})^k \\
&= (1+\sqrt{2})^k(u_k - v_k\sqrt{2}) \\
&= (1+\sqrt{2})^k(1-\sqrt{2})^k \\
&= \left((1+\sqrt{2})(1-\sqrt{2})\right)^k \\
&= (-1)^k
\end{aligned}$$

We conclude that $u_k^2 - 2v_k^2 = (-1)^k$ for all integer $k \geq 0$.

(c) Proof of "v_k is divisible by 3 if and only if $k \equiv 0 (mod\ 4)$ "

Let $r \in \mathbb{N}$.

We have $v_{r+2} = 2v_{r+1} + v_r$

$$\begin{aligned} v_{r+3} &= 2v_{r+2} + v_{r+1} \\ &= 5v_{r+1} + 2v_r \\ v_{r+4} &= 2v_{r+3} + v_{r+2} \\ &= 12v_{r+1} + 5v_r \end{aligned}$$

Since $12v_{r+1} \in 3\mathbb{Z}$ and 5 is a prime number, then we have:
$v_{r+4} \in 3\mathbb{Z} \Leftrightarrow v_r \in 3\mathbb{Z}$.
Since r is arbitrary in $\mathbb{N}$, then we have the following:
For all $p \in \mathbb{N}$,

$$\begin{aligned} v_p \in 3\mathbb{Z} &\Leftrightarrow v_{p+4} \in 3\mathbb{Z} \\ &\Leftrightarrow v_{p+4+4} \in 3\mathbb{Z} \\ &\Leftrightarrow v_{p+4+4+4} \in 3\mathbb{Z} \\ &\quad\vdots \\ &\Leftrightarrow v_{4k+p} \in 3\mathbb{Z} \ \forall \ k \in \mathbb{N}. \end{aligned}$$

So $\forall p \in \mathbb{N}, v_p \in 3\mathbb{Z} \Leftrightarrow v_{4k+p} \in 3\mathbb{Z} \ \forall \ k \in \mathbb{N}$. **(*)**

Now we have: $v_0 = 0 \in 3\mathbb{Z}, v_1 = 1 \notin 3\mathbb{Z}, v_2 = 2 \notin 3\mathbb{Z}$ and $v_3 = 5 \notin 3\mathbb{Z}$.
Taking successively $p = 0,\ p = 1,\ p = 2$ and $p = 3$ and using **(*)**, we have for all $k \in \mathbb{N},\ v_{4k} \in 3\mathbb{Z},\ v_{4k+1} \notin 3\mathbb{Z},\ v_{4k+2} \notin 3\mathbb{Z}$ and $v_{4k+3} \notin 3\mathbb{Z}$.
We conclude that for all $n \in \mathbb{N}$, v_n is divisible by 3 if and only if $n \equiv 0(mod\ 4)$

(d) Deduction : $x^2 - 2y^2 = 1$ and $x^2 - 18y^2 = 1$ have infinitely many integral solutions.

The two sequences have integral terms and are strictly increasing (from the second term on), by their definition. So we have infinitely many terms for each sequence. Moreover, we have $u_k^2 - 2v_k^2 = (-1)^k$ for all integer $k \geq 0$.
* So $u_{2k}^2 - 2v_{2k}^2 = 1$ for all integer $k \geq 0$.
Therefore, the equation $x^2 - 2y^2 = 1$ has infinitely many integral solutions.
* We have shown that $v_{4k} \in 3\mathbb{Z}$ for all $k \geq 0$. So for all $k \in \mathbb{N}$, there exists $l_k \in \mathbb{N}$ such that $v_{4k} = 3l_k$.
Hence $u_{4k}^2 - 2v_{4k}^2 = u_{4k}^2 - 2(3l_k)^2 = u_{4k}^2 - 18l_k^2 = 1$ for all integer $k \geq 0$.
We therefore conclude that the equation $x^2 - 18y^2 = 1$ has infinitely many integral solutions.

3.

Let $d > 0$ be an integer that is not a square. Let $A = \left\{a + b\sqrt{d} : a, b \in \mathbb{Z}\right\}$.

(a) Showing that A is a subring of $\mathbb{R}$.

We have $A \subseteq \mathbb{R}$ and $0 = 0 + 0 \times \sqrt{d}$ and $1 = 1 + 0 \times \sqrt{d}$. So $0, 1 \in A$.
Let $x = a_1 + b_1\sqrt{d}, y = a_2 + b_2\sqrt{d}$ be two elements of A.
We have:

- $$\begin{aligned} x - y &= a_1 + b_1\sqrt{d} - (a_2 + b_2\sqrt{d}) \\ &= a_1 - a_2 + (b_1 - b_2)\sqrt{d} \in A \text{ because } a_1 - a_2, b_1 - b_2 \in \mathbb{Z}. \end{aligned}$$
- $$\begin{aligned} xy &= (a_1 + b_1\sqrt{d})(a_2 + b_2\sqrt{d}) \\ &= a_1a_2 + b_1b_2d + (a_1b_2 + a_2b_1)\sqrt{d} \in A \text{ because } a, b, d \in \mathbb{Z}. \end{aligned}$$

We conclude that A is a subring of $\mathbb{R}$.

(b) Showing that $A \cong \mathbb{Z}[X]/(X^2 - d)$.

For all $P(X) \in \mathbb{Z}[X]$, we have $P(\sqrt{d}) \in A$, by definition of A.
Consider the map $\varphi : \mathbb{Z}[X] \to A$
$P(X) \mapsto P(\sqrt{d})$
φ is well defined.
We shall show that φ is a ring homomorphism.
Let $P_1(X), P_2(X) \in \mathbb{Z}[X]$.
We have:

- $$\begin{aligned} \varphi(P_1(X) + P_2(X)) &= \Big(P_1(X) + P_2(X)\Big)(\sqrt{d}) \\ &= P_1(\sqrt{d}) + P_2(\sqrt{d}) \\ &= \varphi(P_1(X)) + \varphi(P_2(X)) \end{aligned}$$
- $$\begin{aligned} \varphi(P_1(X)P_2(X)) &= \Big(P_1(X)P_2(X)\Big)(\sqrt{d}) \\ &= P_1(\sqrt{d})P_2(\sqrt{d}) \\ &= \varphi(P_1(X))\varphi(P_2(X)) \end{aligned}$$
- $$\begin{aligned} \varphi(0_{\mathbb{Z}[X]}) &= 0_{\mathbb{Z}[X]}(\sqrt{d}) \\ &= 0 \end{aligned}$$
- $$\begin{aligned} \varphi(1_{\mathbb{Z}[X]}) &= 1_{\mathbb{Z}[X]}(\sqrt{d}) \\ &= 1 \end{aligned}$$

So φ is a ring homomorphism.

Now we find the kernel and the range of φ.
• $ker(\varphi)$
We have $\varphi(X^2 - d) = (\sqrt{d})^2 - d = 0$.
So $X^2 - d \in ker(\varphi)$ and it follows that $(X^2 - d)\mathbb{Z}[X] = (X^2 - d) \subseteq ker(\varphi)$ since φ is a ring homomorphism.

Let's show that $ker(\varphi) \subseteq (X^2 - d)$.
Let $Q(X) \in ker(\varphi)$. Then $Q(\sqrt{d}) = 0$. Since the integer $d > 0$ is not a square, then $\sqrt{d} \notin \mathbb{Q}$ and the irreducible polynomial of $\sqrt{d}$ in $\mathbb{Q}[X]$ is $X^2 - d \in \mathbb{Z}[X]$. It follows that $X^2 - d$ divides $Q(X)$. So $Q \in (X^2 - d)$. Thus $ker(\varphi) = (X^2 - d)$.
• $rg(\varphi)$
Now we show that φ is surjective.
Let $x = a + b\sqrt{d} \in A$. We have $a + bX \in \mathbb{Z}[X]$ and $\varphi(a + bX) = a + b\sqrt{d}$.
So φ is surjective and we have $rg(\varphi) = A$.
• Using the first isomorphism theorem, we have $\mathbb{Z}[X]/ker(\varphi) \cong rg(\varphi)$, that is,

$$\mathbb{Z}[X]/(X^2 - d) \cong A.$$

4.

Let's factor $\alpha = 63 + 75i$ and $\beta = 217 - 35i$ into primes in $\mathbb{Z}[i]$ and compute $gcd(\alpha, \beta)$
• α
We have $\alpha\bar{\alpha} = 63^2 + 75^2 = 9594 = 2 \times 3^2 \times 13 \times 41$ and:
$2 = 1^2 + 1^2 = (1 - i)(1 + i)$
$13 = 2^2 + 3^2 = (2 - 3i)(2 + 3i)$
$41 = 4^2 + 5^2 = (4 - 5i)(4 + 5i)$
3 is irreducible in $\mathbb{Z}[i]$.
So $\alpha\bar{\alpha} = 9(1 + i)(1 - i)(2 - 3i)(2 + 3i)(4 - 5i)(4 + 5i)$.

We have

- $$\begin{aligned}\frac{\alpha}{1+i} &= \frac{(63+75i)(1-i)}{(1+i)(1-i)}\\ &= \frac{(63+75i)(1-i)}{2}\\ &= \frac{63+75+75i-63i}{2}\\ &= 69+6i \in \mathbb{Z}[i]\end{aligned}$$

- $\dfrac{\alpha}{1-i} = -6+69i \in \mathbb{Z}[i]$

- $$\begin{aligned}\frac{\alpha}{3-2i} &= \frac{(63+75i)(3+2i)}{(3-2i)(3+2i)}\\ &= \frac{189-150+225i+126i}{13}\\ &= 3+27i \in \mathbb{Z}[i]\end{aligned}$$

- $\dfrac{\alpha}{3+2i} = \dfrac{339}{13} + \dfrac{99}{13}i \notin \mathbb{Z}[i],$ so this factor does not divide α

- $$\begin{aligned}\frac{\alpha}{4-5i} &= \frac{(63+75i)(4+5i)}{(4-5i)(4+5i)}\\ &= \frac{252-375+315i+300i}{41}\\ &= -3+15i \in \mathbb{Z}[i]\end{aligned}$$

- $\dfrac{\alpha}{4+5i} = \dfrac{627}{41} - \dfrac{15}{41}i \notin \mathbb{Z}[i],$ so this factor does not divide α

- $\dfrac{\alpha}{3} = 21+25i \in \mathbb{Z}[i]$

$$\begin{aligned}\text{We have } 3(1+i)(3-2i)(4-5i) &= 3(3-2i+3i+2)(4-5i)\\ &= 3(5+i)(4-5i)\\ &= 3(20+5-25i+4i)\\ &= 3(25-21i)\\ &= 75-63i\\ &= i\alpha\end{aligned}$$

So $\boxed{\alpha = -3i(1+i)(3-2i)(4-5i)}$ **(**)**

- β

We have $\beta\bar{\beta} = 217^2 + 35^2 = 48314 = 2 \times 7^2 \times 17 \times 29$ and:

$2 = 1^2 + 1^2 = (1-i)(1+i)$
$17 = 1^2 + 4^2 = (4-i)(4+i)$
$29 = 5^2 + 2^2 = (5-2i)(5+2i)$
7 is irreducible in $\mathbb{Z}[i]$.
We have

- $$\begin{aligned}\frac{\beta}{1+i} &= \frac{(217-35i)(1-i)}{(1+i)(1-i)} \\ &= \frac{217-35-35i-217i}{2} \\ &= 91-126i \in \mathbb{Z}[i]\end{aligned}$$

- $$\frac{\beta}{1-i} = 126+91i \in \mathbb{Z}[i]$$

- $$\begin{aligned}\frac{\beta}{4+i} &= \frac{(217-35i)(4-i)}{(4+i)(4-i)} \\ &= \frac{868-140i+217i+35}{17} \\ &= 49-21i \in \mathbb{Z}[i]\end{aligned}$$

- $$\begin{aligned}\frac{\beta}{4-i} &= \frac{(217-35i)(4+i)}{(4+i)(4-i)} \\ &= \frac{903}{17} + \frac{77}{17} \notin \mathbb{Z}[i]\end{aligned}$$

- $$\begin{aligned}\frac{\beta}{5+2i} &= \frac{(217-35i)(5-2i)}{(5+2i)(5-2i)} \\ &= \frac{1085+70-175i+434i}{29} \\ &= 35-21i \in \mathbb{Z}[i]\end{aligned}$$

- $$\begin{aligned}\frac{\beta}{5-2i} &= \frac{(217-35i)(5+2i)}{(5+2i)(5-2i)} \\ &= \frac{1155}{29} + \frac{259}{29} \notin \mathbb{Z}[i]\end{aligned}$$

- $$\frac{\beta}{7} = 31-5i \in \mathbb{Z}[i]$$

$$\begin{aligned}\text{We have } 7(1+i)(5+2i)(4+i) & \\ &= 7(1+i)(5+2i)(4+i) \\ &= 35+217i \\ &= i\beta\end{aligned}$$

So $\boxed{\beta = -7i(1+i)(5+2i)(4+i)}$ **(***)**

Using **(**) and (***)** we conclude that $gcd(\alpha, \beta) = 1 + i$.