M E T U
Mathematics Department

Math 366 Elementary Number Theory II Spring 2017 FINAL					
Küçüksakallı **June 05, 2017** **9:30 – 11:45**	Name :		Student Number :		
	Last Name :		Signature :		
P.1 / 25	P.2 / 25	P.3 / 25	P.4 / 25	**SHOW YOUR ORGANIZED WORK**	**Total / 100**
				GOOD LUCK!	

Q.1) In this question, you are allowed to use the fact that $\mathbb{Z}[\sqrt{-2}\,]$ is a Euclidean domain. Let (x, y, z) be a solution of the Diophantine equation $x^2 + 2y^2 = z^2$ with $\gcd(x, y, z) = 1$.

a) Show that $\gcd(x + y\sqrt{-2}, x - y\sqrt{-2}) = 1$ in $\mathbb{Z}[\sqrt{-2}\,]$.

Solution: A greatest common divisor exists for each nonzero pair of elements in a Euclidean domain. Let δ be a greatest common divisor of $\alpha = x + y\sqrt{-2}$ and $\beta = x - y\sqrt{-2}$ in $\mathbb{Z}[\sqrt{-2}\,]$. We have $\delta | 2x = \alpha + \beta$ and $\delta | 2y\sqrt{-2} = \alpha - \beta$. Since $\gcd(x, y, z) = 1$ in $\mathbb{Z}$, we have $\gcd(x, y) = 1$ in $\mathbb{Z}$, too. Moreover $\gcd(x, y) = 1$ in $\mathbb{Z}[\sqrt{-2}\,]$ as well. It follows that $\delta | 2$ because $\mathbb{Z}[\sqrt{-2}\,]$ is a UFD. Assume that $\sqrt{-2} | \delta$. We will obtain a contradiction and this will finish the proof. If $\sqrt{-2} | \delta$ then $\sqrt{-2} | \alpha$ and therefore $\sqrt{-2} | x$ in $\mathbb{Z}[\sqrt{-2}\,]$. It follows that x must be an even integer. This implies that z is even since $x^2 + 2y^2 = z^2$. Finally, y is even too. Therefore $\gcd(x, y, z) = 2$, a contradiction.

b) Show that $x + y\sqrt{-2}$ is of the form $\pm\gamma^2$ for some $\gamma \in \mathbb{Z}[\sqrt{-2}\,]$.

Solution: If $\alpha = x + y\sqrt{-2}$ is a unit then $\alpha = \pm 1$ and we are done. Otherwise let π be an irreducible element of $\mathbb{Z}[\sqrt{-2}\,]$ dividing α. If $\pi | \alpha$, then $\pi | z^2 = \alpha\beta$. Since π is prime, we have $\pi | z$ (prime=irreducible in a UFD). It follows that $\pi^2 | z^2 = \alpha\beta$. In the previous part, we have seen that $\gcd(\alpha, \beta) = 1$. Thus $\pi^2 | \alpha$. Canceling π^2 from both sides of the equation $\alpha\beta = z^2$, we inductively see that α and β are both perfect squares up to units in $\mathbb{Z}[\sqrt{-2}]$.

c) Using the previous part, determine all solutions of $x^2 + 2y^2 = z^2$ with $\gcd(x, y, z) = 1$.

Solution: An arbitrary element $\gamma \in \mathbb{Z}[\sqrt{-2}\,]$ is of the form $a + b\sqrt{-2}$ for some integers a and b. We have

$$\gamma^2 = (a + b\sqrt{-2})^2 = \underbrace{a^2 - 2b^2}_{x} + \underbrace{2ab}_{y}\sqrt{-2}.$$

It follows that, each solution of $x^2 + 2y^2 = z^2$ with $\gcd(x, y, z) = 1$ must be of the form

$$(x, y, z) = \left(\pm(a^2 - 2b^2), \pm 2ab, \pm(a^2 + 2b^2)\right).$$

We have to put a further restriction, namely $\gcd(a, 2b) = 1$. Under this restriction $\gcd(x, y) = 1$ because a common divisor of x and y must divide $2a^2$ and $4b^2$. Finally $\gcd(x, y) = 1$ implies that $\gcd(x, y, z) = 1$ since $x^2 + 2y^2 = z^2$.

Q.2) Consider the ring $I_{-13} = \mathbb{Z}[\sqrt{-13}\,]$.

a) Show that I_{-13} is not a UFD.

Solution: We have $14 = 2 \cdot 7 = (1+\sqrt{-13}) \cdot (1-\sqrt{-13})$. The norm of an arbitrary element $x+y\sqrt{-13}$ in this ring is given by $x^2 + 13y^2$. This quantity is a positive integer and it is not equal to 2 or 7. It follows that the elements $2, 7, 1+\sqrt{-13}$ and $1-\sqrt{-13}$ are irreducible. Moreover $N(2) = 4 \neq 14 = N(1 \pm \sqrt{-13})$. The irreducible elements 2 and $1+\sqrt{-13}$ are not associates of each other. Similarly 2 and $1-\sqrt{-13}$ are not associates, either. We conclude that I_{-13} is not a UFD.

b) Let $\mathfrak{a} = (5, 15+\sqrt{-13})$. What is $N(\mathfrak{a})$? Is $\mathfrak{a}$ principal?

Solution: Note that $N(5) = 25$ and $N(15+\sqrt{-13}) = 2 \cdot 7 \cdot 17$ are relatively prime to each other. The ideal (5) remains prime in I_{-13}. On the other hand $(15+\sqrt{-13}) = \mathfrak{p}_2\mathfrak{p}_7\mathfrak{p}_{17}$ where $\mathfrak{p}_2, \mathfrak{p}_7$ and $\mathfrak{p}_{17}$ are prime ideals of indicated norms. We conclude that

$$\mathfrak{a} = (5) + (15+\sqrt{-13}) = \gcd((5), (15+\sqrt{-13})) = (1).$$

Thus $\mathfrak{a} = (1)$. We have $N(\mathfrak{a}) = 1$ and the ideal $\mathfrak{a}$ is principal.

Alternative Solution: Note that $-13 = (15+\sqrt{-13}-3\cdot 5)^2 \in \mathfrak{a}$. Moreover $\gcd(-13, 5) = 1 \in \mathfrak{a}$. We have $N(\mathfrak{a}) = 1$ and the ideal $\mathfrak{a}$ is principal.

c) Let $\mathfrak{b} = (7, 15+\sqrt{-13})$. What is $N(\mathfrak{b})$? Is $\mathfrak{b}$ principal?

Solution: Recall from the previous part that $(15+\sqrt{-13}) = \mathfrak{p}_2\mathfrak{p}_7\mathfrak{p}_{17}$. We have $(7) = \mathfrak{p}_7\mathfrak{p}_7'$ and

$$\mathfrak{a} = (7) + (15+\sqrt{-13}) = \gcd((7), (15+\sqrt{-13})) = \mathfrak{p}_7$$

where $\mathfrak{p}_7$ is an ideal of norm 7. It is either $(7, 1+\sqrt{-13})$, or $(7, 1-\sqrt{-13})$. We easily see that $\mathfrak{b} = (7, 1+\sqrt{-13})$. We have $N(\mathfrak{b}) = 7$. The ideal $\mathfrak{b}$ is not principal because there is no element in the ring I_{-13} of norm 7.

Alternative Solution: We have $(7) = \mathfrak{p}_7\mathfrak{p}_7'$ where $\mathfrak{p}_7 = (7, 1+\sqrt{-13})$ and $\mathfrak{p}_7' = (7, 1-\sqrt{-13})$. Note that $\mathfrak{b} = \mathfrak{p}_7$. We have $N(\mathfrak{b}) = 7$. The ideal $\mathfrak{b}$ is not principal because there is no element in the ring I_{-13} of norm 7.

d) Let $\mathfrak{c} = (17, 15+\sqrt{-13})$. What is $N(\mathfrak{c})$? Is $\mathfrak{c}$ principal?

Solution: Recall from the previous part that $(15+\sqrt{-13}) = \mathfrak{p}_2\mathfrak{p}_7\mathfrak{p}_{17}$. We have $(17) = \mathfrak{p}_{17}\mathfrak{p}_{17}'$ and

$$\mathfrak{a} = (17) + (15+\sqrt{-13}) = \gcd((17), (15+\sqrt{-13})) = \mathfrak{p}_{17}$$

where $\mathfrak{p}_{17}$ is an ideal of norm 17. It is either $(17, 2+\sqrt{-13})$, or $(17, 2-\sqrt{-13})$. We easily see that $\mathfrak{c} = (17, 2-\sqrt{-13})$. We have $N(\mathfrak{c}) = 17$. The ideal $\mathfrak{c}$ is principal because $\mathfrak{c} = (2-\sqrt{-13})$.

Alternative Solution: We have $\mathfrak{c} = (17, 15+\sqrt{-13}, 2-\sqrt{-13}) = (17, 2-\sqrt{-13}) = (2-\sqrt{-13})$. Thus $\mathfrak{c}$ is principal and its norm is given by $N(\mathfrak{c}) = |N(2-\sqrt{-13})| = 17$.

Q.3) Consider the ring $I_{-10} = \mathbb{Z}[\sqrt{-10}\,]$.

a) Show that $\mathrm{Cl}(-10) \cong \mathbb{Z}/2\mathbb{Z}$ (Minkowski's constant is slightly bigger than 4.).

Solution: We have $\mathrm{Cl}(-10) = \{[\mathfrak{a}] : N(\mathfrak{a}) \leq 4\}$. Note that $(2) = (2, \sqrt{-10})^2 = \mathfrak{p}_2^2$ and (3) remain inert. Thus $\mathrm{Cl}(-10) = \{[(1)], [\mathfrak{p}_2]\}$. There is no element of norm 2 in the ring I_{-10}. Thus $\mathfrak{p}_2$ is not principal. We conclude that $\mathrm{Cl}(-10) \cong \mathbb{Z}/2\mathbb{Z}$.

b) Find the number of solutions to the Diophantine equation $x^2 + 10y^2 = 2^{366}$.

Solution: There is only one ideal $\mathfrak{a} \subseteq I_{-10}$ with $N(\mathfrak{a}) = 2^{366}$. Namely, $\mathfrak{a} = \mathfrak{p}_2^{366}$. This ideal is principal since the exponent of $\mathfrak{p}_2$ is even. More precisely, we have $\mathfrak{a} = (\pm 2^{183})$. The equation $x^2 + 10y^2 = 2^{366}$ has only two solutions, namely $(2^{183}, 0)$ and $(-2^{183}, 0)$.

c) Find the number of solutions to the Diophantine equation $x^2 + 10y^2 = 7^{2017}$.

Solution: The prime 7 splits in I_{-10}, i.e. $(7) = \mathfrak{p}_7\mathfrak{p}_7'$ where $\mathfrak{p}_7 = (7, 2 + \sqrt{-10})$ and $\mathfrak{p}_7' = (7, 2 - \sqrt{-10})$. There is no element of norm 7 in the ring I_{-10}. Thus the ideals $\mathfrak{p}_7$ and $\mathfrak{p}_7'$ are not principal. An ideal $\mathfrak{a} \subseteq I_{-10}$ of norm 7^{2017} must be of the form $\mathfrak{a} = (\mathfrak{p}_7)^{2017-i} (\mathfrak{p}_7')^i$ where $i \in \{0, 1, 2, \ldots, 2017\}$. We have

$$[\mathfrak{a}] = \left[(\mathfrak{p}_7)^{2017-i}\right] \left[(\mathfrak{p}_7')^i\right] = [\mathfrak{p}_7] \neq [(1)].$$

Here, the second equality is obtained from the facts that

- one and only one of $2017 - i$ and i is odd,
- the ideal class group has order 2, and
- $[\mathfrak{p}_7] = [\mathfrak{p}_7']$.

We conclude that $\mathfrak{a}$ is never principal and there is no element of order 7^{2017} in I_{-10}. In other words, the Diophantine equation $x^2 + 10y^2 = 7^{2017}$ has no solution.

d) Find the number of solutions to the Diophantine equation $x^2 + 10y^2 = 13^{1000}$.

Solution: This part is similar to the first part except the exponent of the prime. The prime 13 splits in I_{-10} into a product of non-principal ideals. More precisely, $(13) = \mathfrak{p}_{13}\mathfrak{p}_{13}'$ where $\mathfrak{p}_{13} = (13, 4 + \sqrt{-10})$ and $\mathfrak{p}_{13}' = (13, 4 - \sqrt{-10})$. An ideal $\mathfrak{a} \subseteq I_{-10}$ of norm 13^{1000} must be of the form $\mathfrak{a} = (\mathfrak{p}_{13})^{1000-i} (\mathfrak{p}_{13}')^i$ where $i \in \{0, 1, 2, \ldots, 1000\}$. We have

$$[\mathfrak{a}] = \left[(\mathfrak{p}_{13})^{1000-i}\right] \left[(\mathfrak{p}_{13}')^i\right] = [(1)].$$

Here, the second equality is obtained from the facts that

- the exponents $1000 - i$ and i are both odd or both even,
- the ideal class group has order 2, and
- $[\mathfrak{p}_{13}] = [\mathfrak{p}_{13}']$.

We conclude that an ideal $\mathfrak{a} \subseteq I_{-10}$ of norm 13^{1000} is always principal. It follows that the Diophantine equation $x^2 + 10y^2 = 13^{1000}$ has 2 solutions for each choice of i. Thus there are 2002 solutions.

Q.4) Consider the ring $I_5 = \mathbb{Z}[w_5]$ where $w_5 = \dfrac{\sqrt{5}+1}{2}$.

a) Show that I_5 is a PID.

Solution: The Minkowski constant is $M_5 = \sqrt{5}/2 < 2$. We find that $\mathrm{Cl}(5) = \{[(1)]\}$. Thus I_5 is a PID.

b) Show that the Diophantine equation $x^2 + yx - y^2 = 1$ has infinitely many solutions.

Solution: We know that the Pell's equation $a^2 - 5b^2 = 1$ has infinitely many solutions. For each solution of this equation, there exists a unit $u = a + b\sqrt{5} \in I_5$. This unit u can also be expressed as $u = (a-b) + 2bw_5$. Set $x = a - b$ and $y = 2b$. Observe that $1 = N(u) = N(x + yw_5) = x^2 + yx - y^2$. Under the correspondence $x = a - b$ and $y = 2b$, each solution of the Pell's equation gives a different solution of $x^2 + yx - y^2 = 1$. Even though this correspondence is not one-to-one, this is not a problem since we do not attempt to find all solutions of $x^2 + yx - y^2 = 1$.

c) Show that the Diophantine equation $x^2 + yx - y^2 = 2017$ has no solution.

Solution: We use the quadratic reciprocity law to see that

$$\left(\frac{5}{2017}\right) = \left(\frac{2017}{5}\right) = \left(\frac{2}{5}\right) = -1.$$

It follows that 2017 remains prime in I_5 and as a result there is no ideal in I_5 of norm 2017. We conclude that there is no element in I_5 of norm 2017 and that the Diophantine equation $x^2 + yx - y^2 = 2017$ has no solution.

d) Show that the Diophantine equation $x^2 + yx - y^2 = 19$ has infinitely many solutions.

Solution: One can easily see that $(x, y) = (4, 1)$ is a solution. Set $\alpha = 4 + w_5$. The element $\varepsilon = 9 + 4\sqrt{5} \in I_5$ is a unit whose powers are distinct elements producing distinct solutions of the Pell's equation $x^2 - 5y^2 = 1$. As a result, the elements $\alpha\varepsilon^n$ are all distinct for $n = 1, 2, 3, \ldots$ and moreover $N(\alpha\varepsilon^n) = N(\alpha)N(\varepsilon)^n = 19 \cdot 1^n = 19$. We can express each such element using the basis $\{1, w_5\}$. More precisely,

$$\alpha\varepsilon^n = x_n + y_n w_5$$

for some integers x_n and y_n. Recall that $N(x_n + y_n w_5) = x_n^2 + y_n x_n - y_n^2$. We conclude that there are infinitely many solutions of the Diophantine equation $x^2 + yx - y^2 = 19$.