M E T U
Department of Mathematics

Elementary Number Theory II Final	
Code : *Math 366* Acad. Year : *2015* Semester : *Spring* Instructor : *Küçüksakallı* Date : *June 5, 2015* Time : *13:30* Duration : *135 minutes*	Last Name : Name : Student No. : Signature : 8 QUESTIONS ON 4 PAGES 100 TOTAL POINTS

1	2	3	4	5	6	7	8		

1. (12pts) Let R be an integral domain and let A and B be two nonzero ideals of R. Suppose that AB is principal and it is generated by a_0b_0 with $a_0 \in A$ and $b_0 \in B$. Show that A is principal and generated by a_0.

Solution: Let a be an element of A. Then $ab_0 \in AB$ and there exists $r \in R$ such that $ab_0 = ra_0b_0$. It follows that $b_0(a - ra_0) = 0$. The ideal AB is nonzero and therefore the element b_0 is not zero. Using the fact that R is an integral domain we can cancel b_0 from the equation $b_0(a - ra_0) = 0$ and obtain $a = ra_0$ for some $r \in R$.

2. (12pts) Prove that the Diophantine equation $y^2 = x^3 - x$ has only the trivial solutions with $y = 0$.

Solution: Note that the right hand side of the Diophantine equation $y^2 = x^3 - x$ can be factored as $(x-1)(x)(x+1)$. Assume that x is not equal to $1, 0$ or -1. If the integers $x-1, x$ and $x+1$ are pairwise coprime then each one must be a perfect square (up to ± 1) since their product is a perfect square ($\mathbb{Z}$ is a UFD). If the integers $x-1, x$ and $x+1$ are not pairwise coprime then we must have $\gcd(x-1, x+1) = 2$. Write $x = 2k+1$. Then the Diophantine equation becomes $y^2 = 2k(2k+1)(2k+2)$. It is obvious that y is even. Set $y = 2\ell$. Then $\ell^2 = k(2k+1)(k+1)$. The integers $k, 2k+1$ and $k+1$ are pairwise coprime and their product is a perfect square. It follows that k and $k+1$ are perfect squares. However this is a contradiction to the assumption x is not equal to $1, 0$ or -1.

3. (12pts) For each of the following ideals in $I_{-5} = \mathbb{Z}[\sqrt{-5}]$, determine its norm and explain briefly how you find it.

- $\mathfrak{a}_1 = (1, 1+\sqrt{-5})$.

  Solution: We have $N(\mathfrak{a}_1) = 1$ since $\mathfrak{a}_1$ contains the unit 1.

- $\mathfrak{a}_2 = (2, 1+\sqrt{-5})$.

  Solution: The ideal prime decomposition of (2) in I_{-5} is given by $(2) = \mathfrak{a}_2^2$. It follows that $N(\mathfrak{a}_2) = 2$.

- $\mathfrak{a}_3 = (3, 1+\sqrt{-5})$.

  Solution: The ideal prime decomposition of (3) in I_{-5} is given by $(3) = \mathfrak{a}_3\mathfrak{a}_3'$. It follows that $N(\mathfrak{a}_3) = 3$.

- $\mathfrak{a}_4 = (4, 1+\sqrt{-5})$.

  Solution: Note that $\mathfrak{a}_4 = (4, 1+\sqrt{-5}, 6) = (2, 1+\sqrt{-5})$. Therefore $N(\mathfrak{a}_4) = 2$.

- $\mathfrak{a}_5 = (5, 1+\sqrt{-5})$.

  Solution: The ideal $\mathfrak{a}_5$ contains the unit $1 = (1+\sqrt{-5})(1-\sqrt{-5}) - 5$. Thus we have $N(\mathfrak{a}_5) = 1$.

- $\mathfrak{a}_6 = (6, 1+\sqrt{-5})$.

  Solution: We have $\mathfrak{a}_6 = (1+\sqrt{-5})$. Therefore $N(\mathfrak{a}_6) = |N(1+\sqrt{-5})| = 6$.

4. (12pts) Find the number of ideals in $I_{-14} = \mathbf{Z}[\sqrt{-14}]$ containing the element 30.

Solution: Suppose that $\mathfrak{a}$ is an ideal containing the element 30. It follows that $\mathfrak{a} \supseteq (30)$ and therefore $\mathfrak{a}|(30)$. The ideal prime decomposition of (30) is given by

$$(30) = \mathfrak{p}_2^2\mathfrak{p}_3\mathfrak{p}_3'\mathfrak{p}_5\mathfrak{p}_5'.$$

where $\mathfrak{p}_2 = (2, \sqrt{-14}), \mathfrak{p}_3 = (3, 1+\sqrt{-15}), \mathfrak{p}_3' = (3, 1-\sqrt{-15}), \mathfrak{p}_5 = (5, 1+\sqrt{-15})$ and $\mathfrak{p}_5' = (5, 1-\sqrt{-15})$. Therefore there are $48 = 3 \cdot 2 \cdot 2 \cdot 2 \cdot 2$ ideals of I_{-14} containing the element 30.

5. (12pts) Show that $I_{-5} = \mathbf{Z}[\sqrt{-5}\,]$ is not a Euclidean domain under the norm map $a + b\sqrt{-5} \mapsto a^2 + 5b^2$ without using the fact that E.D. $\Longrightarrow$ P.I.D. $\Longrightarrow$ U.F.D..

Solution: Assume that I_{-5} is a Euclidean domain. Set $\alpha = 1 + \sqrt{-5}$ and $\beta = 2$. There exist $\gamma, \delta \in \mathbf{Z}[\sqrt{-5}\,]$ such that $\alpha = \beta\gamma + \delta$ where $\delta = 0$ or $N(\delta) < 4$. Since $N(\beta) \nmid N(\alpha)$, the element δ cannot be zero. If $N(\delta) = 1$, then $(2, 1 + \sqrt{-5}) = (\delta) = \mathbf{Z}[\sqrt{-5}\,]$. However this is not possible since $(2, 1 + \sqrt{-5})^2 = (2)$. Observe that there are no elements in $\mathbf{Z}[\sqrt{-5}\,]$ of norm 2 or 3. We conclude that $\mathbf{Z}[\sqrt{-5}\,]$ is not a Euclidean domain under the norm map $a + b\sqrt{-5} \mapsto a^2 + 5b^2$.

6. (12pts) Show that $I_{-10} = \mathbb{Z}[\sqrt{-10}\,]$ is not a unique factorization domain by factoring $14 \in I_{-10}$ in two different ways.

Solution: Note that $14 = 2 \cdot 7 = (2 + \sqrt{-10})(2 - \sqrt{-10})$. The norm of an arbitrary element $\alpha = a + b\sqrt{-10} \in I_{-10}$ is given by $N(\alpha) = a^2 + 10b^2$. Note that $N(\alpha)$ cannot be equal to 2 or 7. It follows that the elements $2, 7, 2 + \sqrt{-10}$ and $2 - \sqrt{-10}$ are irreducible. We also observe that these elements are not associates of each other since they don't differ by ± 1 which are the only units in the ring I_{-10}. We conlude that I_{-10} is not a unique factorization domain.

7. (16pts) Show that $\mathrm{Cl}(-6) \cong \mathbb{Z}/2\mathbb{Z}$ (Minkowski's constant is slightly bigger than 3.).

Solution: We start with finding prime ideal decomposition of (2) and (3) in $I_{-6} = \mathbf{Z}[\sqrt{-6}]$. Set $\mathfrak{p}_2 = (2, \sqrt{-6})$ and $\mathfrak{p}_2 = (3, \sqrt{-6})$ We have $(2) = \mathfrak{p}_2^2$ and $(3) = \mathfrak{p}_3^2$. The class group of I_{-6} is given by

$$\mathrm{Cl}(-6) = \{[\mathfrak{a}] : N(\mathfrak{a}) \leq 3\} = \{[(1)], [\mathfrak{p}_2], [\mathfrak{p}_3]\}.$$

The group $\mathrm{Cl}(-6)$ cannot be $\mathbb{Z}/3\mathbb{Z}$ since there is no element of order 3. The ideal $\mathfrak{p}_2$ is not principal because there is no element in I_{-6} of norm 2. Thus $\mathrm{Cl}(-6)$ is not trivial, either. We conclude that the group $\mathrm{Cl}(-6)$ must be isomorphic to $\mathbb{Z}/2\mathbb{Z}$.

8. (12pts) Find the number of solutions to the Diophantine equation $x^2 + 6y^2 = 5^{366}$.

Solution: There is a one-to-one correspondence between the the solutions of this Diophantine equation and the generators of principal ideals of I_{-6} of norm 5^{366}. An ideal $\mathfrak{a} \subseteq I_{-6}$ of norm 5^{366} must be of the following form

$$\mathfrak{a} = (\mathfrak{p}_5)^i (\mathfrak{p}_5')^{366-i}, \qquad i \in \{0, 1, 2, \ldots, 366\}$$

where $\mathfrak{p}_5 = (5, 2 + \sqrt{6})$ and $\mathfrak{p}_5' = (5, 2 - \sqrt{6})$. The ideal $\mathfrak{a}$ is principal for each i since

$$[\mathfrak{a}] = [(\mathfrak{p}_5)^i (\mathfrak{p}_5')^{366-i}] = [(\mathfrak{p}_5)^i (\mathfrak{p}_5)^{366-i}] = [(\mathfrak{p}_5)^{366}] = [(1)].$$

The last equality follows from the fact that $\mathrm{Cl}(-6) \cong \mathbb{Z}/2\mathbb{Z}$, see the previous question. There are 367 ideals of I_{-6} of prescribed norm. There are two units in I_{-6}, namely 1 and -1. It follows that there are $734 = 2 \cdot 367$ elements in I_{-6} of norm 5^{366}. We conlude that the Diophantine equation $x^2 + 6y^2 = 5^{366}$ has 734 distinct solutions.