M E T U
Department of Mathematics

Elementary Number Theory II Midterm 2	
Code : *Math 366* Acad. Year : *2015* Semester : *Spring* Instructor : *Küçüksakallı*	Last Name : Name : Student No. : Signature :
Date : *April 28, 2015* Time : *17:40* Duration : *120 minutes*	8 QUESTIONS ON 4 PAGES 100 TOTAL POINTS

1	2	3	4	5	6		

1. (12pts) Determine the fundamental solution of $x^2 - 101y^2 = 1$ using continued fractions.

Solution: Set $z_0 = \sqrt{101}$. We have $11 > z_0 > 10$. Thus $a_0 = 10$. Set $z_1 = \frac{1}{x_0 - a_0}$. Then

$$z_1 = \frac{1}{\sqrt{101} - 10} = \frac{\sqrt{101} + 10}{1}.$$

Since $21 > z_1 > 20$, we have $a_1 = 20$. Set $z_2 = \frac{1}{z_1 - a_1}$. Then

$$z_2 = \frac{1}{(\sqrt{101} + 10) - 20} = \frac{1}{\sqrt{101} - 10} = z_1.$$

It is obvious that this pattern continues forever and $\sqrt{101} = [10; \overline{20}]$. The continued fraction $[10; \overline{20}]$ has a period of length 1. Thus the fundamental solution is given by the first convergent $C_1 = 10 + \frac{1}{20} = \frac{201}{20}$. The fundamental solution is $(x_0, y_0) = (201, 20)$.

2. (12pts) Let R be an integral domain. Suppose that a and b are elements of R such that $\gcd(a, b) = ax + by$ for some $x, y \in R$. Show that the ideal $I = (a, b)$ is principal and generated by $\gcd(a, b)$.

Solution: Pick an element $i \in I$. Then $i = ar + bs$ for some $r, s \in R$. We have $a = \tilde{a} \gcd(a, b)$ and $b = \tilde{b} \gcd(a, b)$ for some $\tilde{a}, \tilde{b} \in R$. Thus $i = \gcd(a, b)(\tilde{a}r + \tilde{b}s)$. Since $\tilde{a}r + \tilde{b}s \in R$, we conclude that $i \in (\gcd(a, b))$.

Pick an element $j \in (\gcd(a, b))$. Then $j = r \gcd(a, b)$ for some $r \in R$. We are given that $\gcd(a, b) = ax + by$ for some $x, y \in R$. Thus $j = r(ax + by) = a(rx) + b(ry)$. Therefore $j \in (a, b)$.

3. (10pts) Show that there are infinitely many Pythagorean triples $a^2 + b^2 = c^2$ such that $|a - b| = 1$.

Solution: Suppose that $a = m^2 - n^2$ for some integers $m > n > 0$. Also set $b = 2mn$ and $c = m^2 + n^2$. The triple (a, b, c) is a Pythagorean triple. We want $a - b = 1$, i.e. $m^2 - n^2 - 2mn = 1$. Using the substitution $u = m - n$ and $v = n$, we obtain a Pell's equation $u^2 - 2v^2 = 1$ which has infinitely many solutions with $u, v > 0$. For each of these solutions $m = u + v$ and $n = v$ are distinct. Note that as v increases $c = m^2 + n^2$ increases too. As a result each solution of $u^2 - 2v^2 = 1$ would give a different Pythagorean triple (a, b, c) with $a - b = 1$.

4. (16pts) Let $\alpha = 15 + 3i$ and $\beta = 8 - i$ be Gaussian integers. Using the Euclidean algorithm, find Gaussian integers λ and η such that $\gcd(\alpha, \beta) = \alpha\lambda + \beta\eta$. Find a generator for the ideal $I = (\alpha, \beta)$ in the ring $\mathbb{Z}[i]$.

Solution: Applying the Euclidean algorithm, we obtain

$$\begin{aligned} 15 + 3i &= (8 - i)2 + (-1 + 5i) \\ 8 - i &= (-1 + 5i)(-i) + (3 - 2i) \\ -1 + 5i &= (3 - 2i)(-1 + i) + 0 \end{aligned}$$

Thus we conlude that $\gcd(\alpha, \beta) = 3 - 2i$. Applying the Euclidean algorithm in reverse, we find that

$$\begin{aligned} \gcd(\alpha, \beta) &= \beta + i(-1 + 5i) \\ &= \beta + i(\alpha - 2\beta) \\ &= (1 - 2i)\beta + i\alpha. \end{aligned}$$

We can choose $\lambda = 1 - 2i$ and $\eta = i$. A generator for the ideal $I = (\alpha, \beta)$ is $3 - 2i$ (or any associate). See Question 2.

5. (12pts) Show that the Diophantine equation $x^2 + 2y^2 = 3^k$ has $2(k+1)$ distinct solutions.

Solution: Consider $\alpha = x + y\sqrt{-2} \in \mathbb{Z}[\sqrt{-2}]$. Note that $N(\alpha) = 3^k$. The ring $\mathbb{Z}[\sqrt{-2}]$ is a Euclidean domain and there is a unique decomposition $\alpha = u\eta_1\eta_2\cdots\eta_s$ in terms of irreducible elements η_i. The element $\pi = 1 + \sqrt{-2}$ and its conjugate $\pi' = 1 - \sqrt{-2}$ are irreducible elements in $\mathbb{Z}[\sqrt{-2}]$. Moreover π and π' are not associates. Since $\pi\pi' = 3$ we must have $\eta_i = \pi$ or $\eta_i = \pi'$ for each i. Moreover 1 and -1 are the only units in I_{-2}. It follows that $\alpha = \pm\pi^{k-j}(\pi')^j$. There are $2(k+1)$ such elements and each one give a different solution of the Diophantine equation $x^2 + 2y^2 = 3^k$.

6. (12pts) Show that α is irreducible in I_d if $N(\alpha)$ is prime in **Z**. Give an example of an irreducible element $\beta \in I_d$ whose norm is not prime in **Z**.

Solution: Suppose that $N(\alpha) = p$ where p is prime in $\mathbb{Z}$. Let λ and γ be elements in I_d such that $\alpha = \lambda\gamma$. Then $N(\alpha) = p = N(\lambda)N(\gamma)$. Without loss of generality, assume that $N(\lambda) = 1$. Then $\lambda\lambda' = 1$ and therefore λ is a unit in I_d. Thus α is irreducible.

Consider $\beta = 1 + \sqrt{-5} \in I_{-5}$. If $\beta = \eta\nu$ for some $\eta, \nu \in I_{-5}$, then taking norms we obtain $6 = N(\eta)N(\nu)$. The norm of a generic element $a + b\sqrt{-5}$ in I_{-5} is equal to $a^2 + 5b^2$. It follows that there are no elements in I_{-5} of norm 2 or 3. Thus either $N(\eta) = 1$ or $N(\nu) = 1$ and therefore β is irreducible.

7. (10pts) Show that $(2, 1+\sqrt{-7})$ is a principal ideal in I_{-7}. Show that $(2, 1+\sqrt{-13})$ is not a principal ideal in I_{-13}.

Solution: The element $w = \frac{\sqrt{-7}+1}{2}$ belongs to I_{-7}. Note that $1+\sqrt{-7} = 2w$. Therefore the ideal $(2, 1+\sqrt{-7})$ is generated by 2, i.e. $(2, 1+\sqrt{-7}) = (2)$.

Assume that $(2, 1+\sqrt{-13})$ is principal in $I_{-13} = \mathbb{Z}[\sqrt{-13}]$. Then $(2, 1+\sqrt{-13}) = (\alpha)$ for some $\alpha \in I_{-13}$. We have $2 = \alpha\lambda$ and $1+\sqrt{-13} = \alpha\eta$ for some $\lambda, \eta \in I_{-13}$. Taking norms we obtain $4 = N(\alpha)N(\lambda)$ and $14 = N(\alpha)N(\eta)$. It follows that $N(\alpha)|2$. A generic element $a + b\sqrt{-13}$ in I_{-13} has norm $a^2 + 13b^2$ and it cannot be equal to 2. Thus α has norm 1 and it is a unit. Therefore $(\alpha) = I_{-13}$. However $1 \in I_{-13}$ but $1 \notin (2, 1+\sqrt{-13})$, a contradiction.

8. (16pts) If u is a unit in I_d, then show that $N(u) = \pm 1$. Determine the units in the ring I_{-11}.

Solution: Suppose that u is a unit in I_d. Then there exists $u \in I_d$ such that $uv = 1$. Since $u, v \in I_d$ we have $N(u), N(v) \in \mathbb{Z}$. Thus $N(u) = 1$ or $N(u) = -1$.

The element $w = \frac{\sqrt{-11}+1}{2}$ belongs to I_{-11}. Moreover $I_{-11} = \mathbb{Z}[w]$. A generic element $a + bw$ in I_{-11} has norm

$$N(a+bw) = (a+bw)(a+bw') = \left(a + \frac{b}{2}\right)^2 + 11\left(\frac{b}{2}\right)^2 = a^2 + ab + 3b^2.$$

The Diophantine equation

$$\left(a + \frac{b}{2}\right)^2 + 11\left(\frac{b}{2}\right)^2 = -1$$

has no solutions. On the other hand

$$\left(a + \frac{b}{2}\right)^2 + 11\left(\frac{b}{2}\right)^2 = 1$$

can only have solutions with $b = 0$. It follows that 1 and -1 are the only units in I_{-11}.