M E T U
Department of Mathematics

	Elementary Number Theory II FINAL	

Code : *Math 366* Acad. Year : *2018-2019* Semester : *Spring* Instructor : *Tolga Karayayla*	Last Name : First Name : Student ID : Department : Signature :
Date : *25.05.2019* Time : *9:30* Duration : *120 minutes*	7 Questions on 4 Pages SHOW DETAILED WORK!

1	2	3	4	5	6	7	

1. (8+12 pts.) a) Find two solutions of $x^2 - 18y^2 = 25$ in positive integers. (You can use $\sqrt{18} = [4, \overline{4, 8}]$).

Let (x_n, y_n) be a solution of $x^2 - 18y^2 = 1$, then $x_n^2 - 18y_n^2 = 1$

$25(x_n^2 - 18y_n^2) = 25$

$(5x_n)^2 - 18\cdot(5y_n)^2 = 25$

so $(5x_n, 5y_n)$ is a solution of $x^2 - 18y^2 = 25$.

Fundamental sol. of $x^2 - 18y^2 = 1$: (p_1, q_1)

n	-2	-1	0	1	2
a_n			4	4	8
p_n	0	1	4	17	
q_n	1	0	1	4	

$(x_1, y_1) = (17, 4)$ is the fundamental sol.

$(x_2 + y_2\sqrt{18}) = (17 + 4\sqrt{18})^2 = (289 + 16\cdot 18 + 136\sqrt{18}) = (579 + 136\sqrt{18})$

So $(579, 136)$ is a second sol. of $x^2 - 18y^2 = 1$

Then 2 sol. of $x^2 - 18y^2 = 25$ are $(5\cdot 17, 5\cdot 4) = (85, 20)$ and $(5\cdot 579, 5\cdot 136) = (2895, 680)$

b) What is the set of all solutions of $x^2 - 18y^2 = 25$?

We know that for the fundamental solution $(x_1, y_1) = (17, 4)$ of the Pell's Equation $x^2 - 18y^2 = 1$, all solutions of $x^2 - 18y^2 = 1$ in positive integers are (x_n, y_n) for $n \in \mathbb{Z}^+$ where $x_n + y_n\sqrt{18} = (x_1 + y_1\sqrt{18})^n = (17 + 4\sqrt{18})^n$

Then all sol. of $x^2 - 18y^2 = 1$ in integers is $\{(\mp 1, 0)\} \cup \{(\mp x_n, \mp y_n) \mid n \in \mathbb{Z}^+\}$

In part a above we showed that if (x, y) is a sol. of $x^2 - 18y^2 = 1$, then $(5x, 5y)$ is a sol. of $x^2 - 18y^2 = 25$. We now show that all sol. of $x^2 - 18y^2 = 25$ are of this form:

Let $x^2 - 18y^2 = 25$, then $x^2 - 3y^2 \equiv 0 \pmod 5$

$x^2 + 2y^2 \equiv 0 \pmod 5$ — x^2 and y^2 can be congruent to $0, 1$ or 4 modulo 5.

so $x^2 + 2y^2 \equiv 0 \pmod 5$ implies $x^2 \equiv y^2 \equiv 0 \pmod 5$

$5 \mid x^2 \Rightarrow 5 \mid x$

$5 \mid y^2 \Rightarrow 5 \mid y$

So $x = 5a$, $y = 5b$, and

$x^2 - 18y^2 = 25a^2 - 18\cdot 25b^2 = 25 \Rightarrow a^2 - 18b^2 = 1$

Therefore any solution (x, y) of $x^2 - 18y^2 = 25$ is of the form $(x, y) = (5a, 5b)$ where (a, b) is a sol. of $x^2 - 18y^2 = 1$.

Therefore: Solution set of $x^2 - 18y^2 = 25$ is:

$\{(\mp 5, 0)\} \cup \{(\mp 5x_n, \mp 5y_n) \mid n \in \mathbb{Z}^+\}$

x_n, y_n as written above.

2. (10 pts.) Solve the system of equations $x^2 + y^2 = z^2$, $x + y + z = 90$ in positive integers.

(x,y,z) is a solution $\Leftrightarrow$ (y,x,z) is a solution.

$x^2+y^2=z^2 \Rightarrow \begin{cases} x = k\cdot 2st,\ y=(s^2-t^2)\cdot k,\ z=(s^2+t^2)\cdot k \\ \text{or interchange } y \text{ and } x. \end{cases}$ for $k,s,t \in \mathbb{Z}^+$, $s>t$, $\gcd(s,t)=1$, $s \not\equiv t \pmod 2$

$x,y,z \in \mathbb{Z}^+$

Then

$x+y+z = k(2st+s^2-t^2+s^2+t^2) = k2s(s+t) = 90 \Rightarrow ks(s+t)=45$

$k=1 \Rightarrow s(s+t)=45$, $s=5, t=4 \Rightarrow (x,y,z)=(40,9,41)$ or $(9,40,41)$

$k=3 \Rightarrow s(s+t)=15$, $s=3, t=2 \Rightarrow (x,y,z)=(36,15,39)$ or $(15,36,39)$

$k=5 \Rightarrow s(s+t)=9$ no s,t exists.

$k=9 \Rightarrow s(s+t)=5$ " "

$k=15 \Rightarrow s(s+t)=3$ " " "

$k=45 \Rightarrow s(s+t)=1$ "

3. (5+10 pts.) a) Fill in the blanks with appropriate Gaussian integers (no explanation is necessary):
Let $\alpha \in \mathbb{Z}[i]$ be a Gaussian prime. If $N(\alpha)$ divides a power of 3, then α is an associate of $\underline{3}$.
If $N(\alpha)$ divides a power of 5, then α is an associate of either $\underline{2+i}$ or $\underline{2-i}$.
If $N(\alpha)$ divides a power of 13, then α is an associate of either $\underline{3+2i}$ or $\underline{3-2i}$.
b) How many distinct Gaussian integers β are there such that $N(\beta) = 3^2 \cdot 5 \cdot 13^2$? (Hint: Consider the factorization of β as a product of Gaussian primes. What can you say about the norms of these prime factors?) $\beta = \pi_1\pi_2\pi_3 \cdots \pi_k$ (prime factorization in $\mathbb{Z}[i]$, π_i: Gaussian primes)

$N(\beta) = 3^2\cdot 5 \cdot 13^2 = N(\pi_1)\cdot N(\pi_2) \cdots N(\pi_k)$

after reordering $\pi_1, \pi_2, \ldots, \pi_k$ if necessary), we get $N(\pi_1) \mid 3^2$, so π_1 is assoc. of 3, $N(\pi_1)=3^2$

Note that $N(\pi_i) = 2$, or p (where p is a prime, $p\equiv 1 \pmod 4$) or q^2 (where q is a prime, $q \equiv 3 \pmod 4$)

$N(\pi_2) \mid 5 \Rightarrow N(\pi_2)=5$, π_2 is an assoc. of $2+i$ or $2-i$

$N(\pi_3)=N(\pi_4)=13$ so π_3, π_4 are associates of $3+2i$ or $3-2i$.

Then, $\beta = \pi_1\pi_2\pi_3\pi_4$ and

β is an associate of $3\cdot(x)\cdot(y)$ where $x = 2\pm i$ (2 choices for x)

$y = (3+2i)^2$ or $(3-2i)^2$ or $(3+2i)(3-2i)$ (3 choices for y)

β is an associate of one of 6 choices for $3xy$.

(By unique factorization in $\mathbb{Z}[i]$, no 2 of these 6 different choices are associates of each other).

For a nonzero $\gamma \in \mathbb{Z}[i]$, it has 4 distinct associates: $\pm\gamma, \pm i\gamma$.

Therefore, we have $6\cdot 4 = 24$ distinct such β.

~~$(3+2i)^2$ and $(3-2i)^2$ are also associates.~~

Remark: $\beta = x+iy \Rightarrow N(\beta) = x^2+y^2 = 3^2\cdot 5 \cdot 13^2$

This question shows that $585 = 3^2\cdot 5\cdot 13$ can be written as a sum of 2 integers in 24 ways and as a sum of non-negative integers in 6 ways.

4. (10 pts.) Show that $I_{-21} = \mathbb{Z}[\sqrt{-21}]$ is not a UFD (Hint: Factorize 22 in I_{-21}).

$22 = 2 \cdot 11 = (1+\sqrt{-21})(1-\sqrt{-21})$

$N(x+y\sqrt{-21}) = x^2+21y^2 \geq 0$.

Claim: $2, 11, 1 \pm \sqrt{-21}$ are all irreducible in I_{-21}:

Proof of claim: If 2 is not irreducible $2 = a \cdot b$, a, b nonunits

$N(2) = N(a) \cdot N(b)$

$4 = N(a)N(b)$, $N(a) > 1$, $N(b) > 1$ since nonunits

so $N(a) = N(b) = 2$

Similarly, if 11 is not irreducible, then

$N(11) = 121 = N(a) \cdot N(b)$ for some nonunits a, b

$N(a) = N(b) = 11$

Similarly, if $1 \pm \sqrt{21}$ is not irreducible, $N(1 \pm \sqrt{-21}) = 22 = N(a) \cdot N(b)$ for nonunits a, b

$N(a) = 2$ or 11, $N(b) = 2$ or 11.

But $N(x+y\sqrt{21}) = x^2+y^2 \cdot 21 = 2$ or 11 has no solution x, y in $\mathbb{Z}$. Thus $2, 11, 1 \pm \sqrt{-21}$ are all irreducible in I_{-21}.

2 is not an associate of $1 \pm \sqrt{-21}$ since $|N(2)| = 4 \neq 22 = |N(1 \pm \sqrt{-21})|$

(For associate elements, abs. value of norms are equal)

So 22 is factorized in 2 different ways into product of irreducibles. I_{-21} is not a UFD.

5. (3×6 pts.) a) Factorize the principal ideal (5) as a product of prime ideals in $I_{10} = \mathbb{Z}[\sqrt{10}]$.

$Tr(\sqrt{10}) = 0$, $N(\sqrt{10}) = 10$, $f(x) = x^2 - Tr(\sqrt{10})x + N(\sqrt{10}) = x^2+10$

$f(x) = x^2+10 \equiv x^2$ in $\mathbb{Z}_5[x]$

$\equiv x \cdot x$

$p_1 = (5, \sqrt{10})$ $p_1 = p_2$

$p_2 = (5, \sqrt{10})$

Then by Dedekind's Thm, $(5) = (5, \sqrt{10})(5, \sqrt{10})$

$= p_1 \cdot p_2 = p_1^2$ (p_1 is a prime ideal)

b) Is the ideal $(5, \sqrt{10})$ a principal ideal in I_{10}?

From part a, $p_1 = (5, \sqrt{10})$ is prime and $N(5) = N(p_1^2) = (N(p_1))^2$

$25 = (N(p_1))^2 \Rightarrow N(p_1) = 5$

Assume $p_1 = (\alpha)$ for some $\alpha \in I_{10}$

Then $5 = N(p_1) = |N(\alpha)| \Rightarrow N(\alpha) = \pm 5$

$\alpha = x+y\sqrt{10} \Rightarrow N(\alpha) = x^2 - 10y^2 = \pm 5$

$x^2 - 10y^2 = \pm 5 \Rightarrow 5 \mid x^2 \Rightarrow 5 \mid x \Rightarrow x = 5z$

$25z^2 - 10y^2 = \pm 5 \Rightarrow 5z^2 - 2y^2 = \pm 1 \Rightarrow \pm 1 + 2y^2 = 5z^2$

$\pm 1 \pm 2y^2 \equiv 0 \pmod 5$ but $y^2 \equiv 0, 1$ or $4 \pmod 5$ so $\pm 1 \pm 2y^2 \not\equiv 0 \pmod 5$

Thus $x^2 - 10y^2 = \pm 5$ has no solution in $\mathbb{Z}^2$.

There is no α such that $|N(\alpha)| = 5$, thus p_1 is NOT a principal ideal.

c) Show that if n is odd, then the equation $x^2 - 10y^2 = 5^n$ has no solution $(x, y) \in \mathbb{Z}^2$.

$x^2 - 10y^2 = 5^n \Rightarrow N(x+y\sqrt{10}) = 5^n$

$(5) = p_1^2 \Rightarrow p_1$ is the only ideal of norm 5

$(N(B) = 5 \Rightarrow B \mid (5) = p_1^2 \Rightarrow B = p_1$ since P is also a prime ideal having norm $= 5$, an ordinary prime)

$n = 2k+1$, $k \in \mathbb{Z} \Rightarrow 5^n = 5^{2k+1}$

$= (N(p_1))^{2k+1} = N(p_1^{2k+1})$

If $N(x+y\sqrt{10}) = 5^{2k+1} = N(p_1^{2k+1})$, then $(x+y\sqrt{10}) = p_1^{2k+1}$ — since p_1^{2k+1} is the only ideal of norm 5^{2k+1} (because p_1 is the only ideal of norm 5)

So p_1^{2k+1} is principal if a solution of $x^2 - 10y^2 = 5^{2k+1}$ exists.

$p_1^2 = (5) \Rightarrow [p_1^2] = [I_d]$ — identity in the class group. So $[p_1^{2k+1}]$

$[p_1^{2k+1}]$

$= [p_1^2]^k \cdot [p_1]$

$= [I_d]^k \cdot [p_1] = [p_1]$

equals $[p_1^2]^k [p_1] = [I_d] \cdot [p_1] = [p_1] \neq [I_d]$

$[p_1] \neq [I_d]$ since p_1 is not principal. So p_1^{2k+1} is not principal.

6. (12 pts.) Show that $I_{-19} = \mathbb{Z}[\frac{1+\sqrt{-19}}{2}]$ is a UFD (Hint: Use the theorem on Minkowski constants).

$Tr(\frac{1+\sqrt{-19}}{2}) = 1$, $N(\frac{1+\sqrt{-19}}{2}) = 5$ $f = x^2 - Tr(\omega_{-19})x + N(\omega_{-19}) = x^2 - x + 5$ $\Delta = 1^2 - 4 \cdot 5 \cdot 1 = -19$

To show that I_{-19} is a UFD, it suffices to show that all ideals that divide (p) for primes $p \leq \frac{2}{\pi}\sqrt{|\Delta|}$ are principal

$p \leq \frac{2}{\pi}\sqrt{|-19|} = \frac{2}{\pi}\sqrt{19} < \frac{2}{\pi} \cdot \frac{9}{2} = \frac{9}{\pi} < 3$, so it suffices to consider $p = 2$.

$f = x^2 - x + 5 \equiv x^2 + x + 1 \pmod 2$

$x^2 + x + 1$ is irreducible in $\mathbb{Z}_2[x]$ (it has no roots in $\mathbb{Z}_2$), then (2) is prime by Dedekind's Thm.

$\alpha \neq I_{-19}$, $\alpha \mid (2) \Rightarrow (\alpha) = (2)$ since (2) is a prime ideal of I_{-19}

So $\alpha \mid (2) \Rightarrow \alpha$ is principal $(\alpha = (2))$

Therefore I_{-19} is a UFD.

7. (8+7 pts.) a) Let $p \in \mathbb{Z}$ be a prime. Show that if p does not divide d and d is a squarefree integer, then either the principal ideal (p) is a prime ideal or $(p) = \alpha\beta$ for two (not necessarily distinct) prime ideals α and β in the ring of integers I_d of the quadratic extension $Q(\sqrt{d})$.

$p \nmid d \Rightarrow p \neq d$ so $(p) \neq (0)$.

Thus, (p) factorizes as a product of prime ideals uniquely:

$(p) = \alpha_1 \cdot \alpha_2 \cdot \alpha_3 \cdots \alpha_k$ where α_i are all prime ideals.

$p^2 = N((p)) = N(\alpha_1) \cdot N(\alpha_2) \cdots N(\alpha_k)$ $\quad$ ~~$(N(\alpha_i) > 1$ since $N(\alpha_i) = |\frac{I_d}{\alpha_i}|$~~

p is prime in $\mathbb{Z}$, $N(\alpha_i) > 1$, $N(\alpha_i) \in \mathbb{Z}^+ \Rightarrow$ ~~$(k = 1 \wedge N(\alpha_1) = p^2$ and $\alpha_i \neq I_d$~~

or

$k = 2$, $N(\alpha_1) = N(\alpha_2) = p$

$k = 1 \Rightarrow (p) = \alpha_1$ (a prime ideal)

$k = 2 \Rightarrow (p) = \alpha_1 \cdot \alpha_2$, α_1 and α_2 are prime ideals, $N(\alpha_1) = N(\alpha_2) = p$

(Take $\alpha = \alpha_1$, $\beta = \alpha_2$, they may be equal or distinct)

b) Assume $(p) = \alpha\beta$ as in part (a) above and suppose $\alpha \neq \beta$ in I_d. How many ideals δ are there in I_d such that $N(\delta) = p^n$ where n is a positive integer, and what are these ideals δ?

$N(\alpha) = N(\beta) = p$ (as explained above)

Let $\delta = \omega_1 \cdot \omega_2 \cdots \omega_r$ where ω_r are prime ideals.

$N(\delta) = p^n = N(\omega_1) N(\omega_2) \cdots N(\omega_r) \Rightarrow N(\omega_j) = p^{m_j}$ for some $m_j \in \mathbb{Z}^+$

$N(\omega_j) \in \omega_j$, so $(N(\omega_j)) \subseteq \omega_j$

$\omega_j \mid (N(\omega_j)) = (p^{m_j})$

$\omega_j \mid (p)^{m_j} \Rightarrow \omega_j \mid (p)$ since ω_j is a prime ideal

Thus each ω_j is α or β, hence:

$\omega_j \mid \alpha \cdot \beta \Rightarrow \omega_j \mid \alpha \vee \omega_j \mid \beta$

$\omega_j = \alpha \vee \omega_j = \beta$

(since α and β are prime ideals)

$\delta = \alpha^s \cdot \beta^t$ $(s + t = r$

$N(\delta) = p^n = N(\alpha^s) \cdot N(\beta^t) = (N(\alpha))^s \cdot (N(\beta))^t = p^s \cdot p^t = p^{s+t}$

$n = s + t$

Therefore $\delta = \alpha^s \cdot \beta^{n-s}$ for some $s = 0, 1, 2, \ldots, n$

There are $n+1$ such ideals δ with norm p^n.