

UMASS AMHERST MATH 471 FALL 2006, F. HAJIR

SOLUTIONS FOR EXAM 1: 10/16/06

NAME: Solomon Soledad Soluz

Unless otherwise noted, all Greek letters denote elements of the set \mathbb{G} of Gaussian integers.

1. DEFINITIONS: DO ALL 7, 3 POINTS EACH

With your permission, I will leave these to you

- a. The set of *Gaussian integers* is $\mathbb{G} =$

- b. A Gaussian integer α is called a *unit* if

- c. We say α is an *associate* of β if

- d. We say α *divides* β ($\alpha|\beta$) if

- e. A Gaussian integer π is called a *Gaussian prime* if

- f. The *ideal* generated by α and β is defined to be $(\alpha, \beta) =$

- g. If π is a Gaussian prime and $\alpha \in \mathbb{G}$, then the π -*adic valuation* of α is $v_\pi(\alpha) =$

2. TRUE/FALSE: DO ALL FIVE, 2 POINTS EACH

You do not need to justify your answer.

- a. If α, β are non-zero Gaussian integers, then there exist $\kappa, \rho \in \mathbb{G}$ such that $\beta = \alpha\kappa + \rho$ with $N(\rho) < N(\alpha)$. TRUE
- b. If $\kappa \in \mathbb{G}$ then $(\alpha, \beta) = (\alpha, \beta - \kappa\alpha)$. TRUE
- c. If $N(\alpha) = p$ where p is a prime, then $(\alpha, \bar{\alpha}) = \mathbb{G}$. TRUE
- d. If $n \in \mathbb{Z}$, the equation $x^2 + y^2 = n$ has a solution with $x, y \in \mathbb{Z}$ if and only if there exists an element $\alpha \in \mathbb{G}$ with norm $N(\alpha) = n$. TRUE

e. For $\alpha, \beta \in \mathbb{G}$, if $N(\alpha) = N(\beta)$, then there exists a unit $\varepsilon \in \mathbb{G}$ such that $\alpha = \varepsilon\beta$.
FALSE: e.g. $2 + i, 2 - i$ have norm 5 but are not associates.

3. SHORT ANSWER: DO 4 OUT OF 6, 5 POINTS EACH

You do **not** need to justify your steps.

a. Determine a generator for the ideal (α, β) where $\alpha = 2 - i$ and $\beta = 3 - 4i$.

We apply the Euclidean algorithm and find $3 - 4i = (2 - i)^2$, so $(\alpha, \beta) = (2 - i)$.

b. When $8 + 7i$ is divided by $2 + i$, the quotient κ and remainder ρ are : $\kappa = 5 + I \quad \rho = -1$.

c. For the Gaussian prime $\pi = 1 - i$ and the Gaussian integer $\alpha = 8 + 8i$ compute the π -adic valuation $v_\pi(\alpha)$.

We recall that $1 - i$ is actually an associate of $1 + i$, and also we have $(1 - i)^2 = -2i$, cubing it we get $(1 - i)^6 = -8i^3 = 8i$. Thus $\alpha = 8(1 + i)$ is divisible by $(1 + i)^7$ but not by $(1 + i)^8$, giving $v_\pi(\alpha) = 7$.

d. It is a fact that $N(3333 + 1010i) = 12128989$; you don't need to check it. Given this fact, find integers $a, b \in \mathbb{Z}$ such that $a^2 + b^2 = 121289890$.

We have $N(1 + 3i) = 10$, if $\alpha = (1 + 3i)(3333 + 1010i)$, then $N(\alpha) = 121289890$. We compute $\alpha = 303 + 11009i$ so $a = 303, b = 11009$ will do. If we use $3 + i$ instead of $1 + 3i$, we'd get $a = 8989, b = 6363$ which is even cooler, maybe?

e. Suppose π_1, π_2, π_3 are distinct Gaussian primes and $\varepsilon_1, \varepsilon_2$ are units. Suppose $\alpha = \varepsilon_1\pi_1^{10}\pi_3^4$ and $\beta = \varepsilon_2\pi_1^3\pi_2^2\pi_3^{11}$. Find a generator γ for the ideal (α, β) .

We just have to take the greatest common divisor, and we can do that one prime at a time, so $\gamma = \pi_1^3\pi_3^4$ is a generator for (α, β) .

f. Suppose you know that α, β are non-zero elements of \mathbb{G} and that for every non-zero $\lambda \in (\alpha, \beta)$, $N(\lambda) > 12$. Suppose also that $471\alpha + 300\beta = 2 + 3i$. Find a generator γ for the ideal (α, β) .

Well, a generator for (α, β) is a least norm element of it, and $2 + 3i$ has norm 13 which is the smallest possible norm, we're told, so $2 + 3i$ must be a least-norm element of (α, β) hence a generator of it!

4. PROOFS: DO 4 OUT OF 6, 12 POINTS EACH

a. Suppose $n = 4k + 3$ for some integer $k \in \mathbb{Z}$. Show that the equation $x^2 + y^2 = n$ has no solutions with $x, y \in \mathbb{Z}$.

We have $x^2 \equiv 0^2, 1^2, 2^2, 3^2 \pmod{4}$ and the same goes for y^2 of course, so $x^2 + y^2 \equiv 0 + 0, 0 + 1, 1 + 0, 1 + 1 \pmod{4}$, thus $x^2 + y^2 \equiv 0, 1, 2 \pmod{4}$. Since $n \not\equiv 0, 1, 2 \pmod{4}$, $n \neq x^2 + y^2$.

b. Suppose p is an odd prime and $p = a^2 + b^2$ with $a, b \in \mathbb{Z}$. Prove that $\pi = a + bi$ is not an associate of $\bar{\pi} = a - bi$, i.e. there does not exist a unit $\varepsilon \in \mathbb{G}$ such that $\pi = \varepsilon\bar{\pi}$.

Suppose not. Then $a + bi = u(a - bi)$ where $u \in \{1, i, -i, -1\}$. We'll just rule these out one by one. If $u = 1$, then $b = 0$, so $p = a^2$ contradiction. If $u = i$, $a + bi = ai + b$ so $a = b$ so $p = 2a^2$ but p is odd, contradiction. If $u = -i$, $a + bi = -ai - b$ so $a = -b$ and again $p = 2a^2$, contradiction. Finally, if $u = -1$, $a + bi = -a + bi$ so $a = 0$, giving $p = b^2$, contradiction.

c. Suppose p is a prime number and $\alpha \in \mathbb{G}$ has norm $N(\alpha) = p$. Prove that α is a Gaussian prime.

If $\alpha = \beta\gamma$ with $\beta, \gamma \in \mathbb{G}$, then $p = N(\beta)N(\gamma)$ but p is prime so we must have $N(\beta) = 1$ or $N(\gamma) = 1$, i.e. we must have either $\beta \in \mathbb{G}^\times$ or $\gamma \in \mathbb{G}^\times$. Thus, α is a Gaussian prime.

d. Suppose $\alpha, \beta, \gamma \in \mathbb{G}$, and $(\gamma) = (\alpha, \beta)$. Suppose also that $1985\alpha + 2006\beta = 18$. Show that $\gamma = \varepsilon \cdot (1 + i)^m \cdot 3^n$ for some $\varepsilon \in \mathbb{G}^\times$ and some integers m, n in the range $0 \leq m, n \leq 2$.

We have $18 \in (\alpha, \beta) = (\gamma)$, thus $18 = \gamma\kappa$ for some $\kappa \in \mathbb{G}$, i.e. $\gamma|18$. Now 18 factors into Gaussian primes as $18 = (-i) \cdot 3^2 \cdot (1 + i)^2$ so γ is a unit times $(1 + i)^m 3^n$ where m is 0, 1, or 2 and n is 0, 1, or 2.

e. Prove that if $\alpha, \beta \in \mathbb{G}$ satisfy $\gcd(N(\alpha), N(\beta)) = 1$, then $(\alpha, \beta) = \mathbb{G}$.

We know that there exists γ such that $(\gamma) = (\alpha, \beta)$. Thus, $\gamma|\alpha$ and $\gamma|\beta$. By the multiplicativity of the norm, $N(\gamma)$ is then a common divisor of $N(\alpha)$ and $N(\beta)$. But these numbers being coprime, that means $N(\gamma) = 1$, so $(\alpha, \beta) = \mathbb{G}$.

f. For $\alpha, \beta \in \mathbb{G}$, let us say that α and β are **related** if $\alpha|\beta$ and $\beta|\alpha$. Prove that α and β are related if and only if there exists a unit $\varepsilon \in \mathbb{G}^\times$ such that $\alpha = \beta\varepsilon$.

First note that α and β must be non-zero, otherwise, $\alpha|\beta$ etc. makes no sense. If α and β are related, then $\alpha = \beta\alpha'$ and $\beta = \alpha\beta' = (\beta\alpha')\beta'$. Subtracting, we get $\beta - \beta\alpha'\beta' = \beta(1 - \alpha'\beta') = 0$. Since $\beta \neq 0$, we must have $1 - \alpha'\beta' = 0$ i.e. $\alpha'\beta' = 1$ so α' and β' are both units which shows that α, β are associates, as desired. The other direction, clearly if $\alpha = \beta\varepsilon$, then $\beta|\alpha$. But ε is a unit, so $\beta = \alpha\delta$ where $\delta = \varepsilon^{-1} \in \mathbb{G}$, so $\alpha|\beta$ also.