

UMASS AMHERST MATH 471 FALL 2006, F. HAJIR

SOLUTIONS FOR HOMEWORK 3: GAUSSIAN INTEGERS III

1. Determine a generator for the ideal $(\alpha_1, \alpha_2, \alpha_3)$ where $\alpha_1 = -1 + 3i$, $\alpha_2 = -4 + 7i$, and $\alpha_3 = -3 + 4i$.

As a first step, we can determine a generator γ for the ideal (α_1, α_2) . We do this by the Euclidean algorithm. First we divide α_2 by α_1 . Thus, $\alpha_2 = \alpha_1(3 + i) + (2 - i)$, so $(\alpha_1, \alpha_2) = (\alpha_2, \alpha_1) = (\alpha_1, 2 - i)$. Now divide α_1 by $2 - i$ and this time there is no remainder! So $(\alpha_1, \alpha_2) = (2 - i)$.

Therefore, $(\alpha_1, \alpha_2, \alpha_3) = (2 - i, \alpha_3)$. Now divide $\alpha_3/(2 - i) = (-2 + i)$ and again there is no remainder, so $(\alpha_1, \alpha_2, \alpha_3) = (2 - i, \alpha_3) = (2 - i)$.

2. (a) Using the Euclidean algorithm, compute a generator γ for the ideal $(-4 + 7i, -3 + 4i)$ and find $\lambda, \mu \in \mathbb{G}$ such that $\gamma = \lambda(-4 + 7i) + \mu(-3 + 4i)$.

Same thing, but we do more book-keeping. We check that $-3 + 4i$ goes into $-4 + 7i$ 2 times with remainder $2 - i$, so we start our table

$$\left| \begin{array}{c|c|c|c} & -4 + 7i & 1 & 0 \\ & -3 + 4i & 0 & 1 \\ -2 + i & 2 - i & 1 & -2 \\ & 0 & 2 - i & -3 + 2i \end{array} \right|$$

Thus, $\gamma = 2 - i$ is a generator, and $2 - i = 1(-4 + 7i) - 2(-3 + 4i)$.

(b) Using the Euclidean algorithm, compute a generator γ for the ideal $(-11 + 49i, -33 + 56i)$ and find $\lambda, \mu \in \mathbb{G}$ such that $\gamma = \lambda(-11 + 49i) + \mu(-33 + 56i)$.

Same algorithm; $-11 + 49i$ goes into $-33 + 56i$ 1 time, with remainder $-22 + 7i$ is how we start, and then we divide $(-11 + 49i)/(-22 + 7i)$ etc.

$$\left| \begin{array}{c|c|c|c} & -33 + 56i & 1 & 0 \\ & -11 + 49i & 0 & 1 \\ 1 - 2i & -22 + 7i & 1 & -1 \\ 4 - 5i & -3 - 2i & -1 + 2i & 2 - 2i \\ & 0 & -5 - 13i & 1 + 18i \end{array} \right|$$

Thus, $\gamma = -3 - 2i$, $\lambda = -1 + 2i$, $\mu = 2 - 2i$.

3. Suppose $\alpha, \beta \in \mathbb{G}$ and $\gcd(|\alpha|^2, |\beta|^2) = 1$. Prove that $(\alpha, \beta) = \mathbb{G}$.

We know that every ideal in \mathbb{G} has a generator, so let us write $(\gamma) = (\alpha, \beta)$. Then α and β are multiples of γ so there exist $\alpha', \beta' \in \mathbb{G}$ such that $\gamma\alpha' = \alpha$ and $\gamma\beta' = \beta$. Taking norms, we have $g\alpha' = a$ and $g\beta' = b$ where $g = N(\gamma)$, $a = N(\alpha)$, etc. Thus, g divides a and b . But by assumption, $\gcd(a, b) = 1$, and so $g = 1$. That means γ is a unit, so $(\gamma) = (1) = \mathbb{G}$.

4. Prove or disprove: Whenever $\alpha, \beta, \gamma \in \mathbb{G}$ where $(\gamma) = (\alpha, \beta)$, then $|\gamma|^2$ divides $\gcd(|\alpha|^2, |\beta|^2)$.

This is true, because we just proved it in the previous solution.

5. Suppose $\alpha, \beta, \pi \in \mathbb{G}$ and π is a Gaussian prime. Show that if $(\alpha, \beta) = \mathbb{G}$ and $\pi|\alpha\beta$ (i.e. there exists $\delta \in \mathbb{G}$ such that $\pi\delta = \alpha\beta$), then either $\pi|\alpha$ or $\pi|\beta$.

We proved this in class. But let's go through it again. If $\pi|\alpha$, we are done. Now suppose π does not divide α . Then $(\pi, \alpha) = \mathbb{G}$, because if $(\pi, \alpha) = (\gamma)$, then γ divides π and α . Since π is a Gaussian prime, its only divisors are either units or associates of π . Now if $\gamma = u\pi$ for some unit $u \in \mathbb{G}^\times$, then γ divides α implies that π divides α but we have assumed π does not divide α . Thus, γ must be a unit, so $(\pi, \alpha) = \mathbb{G}$. Thus, there exist $\theta, \eta \in \mathbb{G}$ such that $\pi\theta + \alpha\eta = 1$. Multiplying by β we have $\beta = \beta\pi\theta + \beta\alpha\eta$. Now we can easily factor a π out of the right hand side:

$$\beta = \pi(\beta\theta + \delta\eta).$$

Thus, $\pi|\beta$ as desired.

6. For $\alpha, \beta, \gamma \in \mathbb{G}$ show that if $(\alpha, \beta) = \mathbb{G}$, then $(\gamma\alpha, \gamma\beta) = (\gamma)$.

Since $(\alpha, \beta) = \mathbb{G}$, we can find $\lambda, \mu \in \mathbb{G}$ such that $1 = \alpha\lambda + \beta\mu$. Multiplying by γ , we have $\gamma = \gamma\alpha\lambda + \gamma\beta\mu$, giving γ as a linear combination of $\gamma\alpha$ and $\gamma\beta$. Therefore, every multiple of γ is also such a linear combination (just multiply both sides!) We have shown that $(\gamma) \subseteq (\gamma\alpha, \gamma\beta)$. But clearly $(\gamma\alpha, \gamma\beta) \subseteq (\gamma)$ because

$$\gamma\alpha\theta + \gamma\beta\eta = \gamma(\alpha\theta + \beta\eta).$$

This completes the proof.

7. (a) Show that for $a, b \in \mathbb{Z}$, if $\gcd(a, b) = 1$ then $\gcd(a + b, a - b)$ is either 1 or 2.

Suppose $g|(a+b)$ and $g|(a-b)$. Then $g|[(a+b)+(a-b)]$ so $g|2a$. Similarly, $g|[(a+b)-(a-b)]$ so $g|2b$. Now we have that g is a common divisor of $2a$ and $2b$. I claim that this implies that g divides $\gcd(2a, 2b)$.

CLAIM. If x, y, g are integers and $g|x$ and $g|y$, then $g|\gcd(x, y)$.

Proof. By Bézout's theorem, we can find integers m, n such that $xm + yn = \gcd(x, y)$. Then

$$\gcd(x, y) = g\left(\frac{x}{g}m + \frac{y}{g}n\right)$$

is clearly an integer multiple of g , i.e. $g|\gcd(x, y)$.

Using the claim, we get $g|\gcd(2a, 2b)$. Now I have another claim.

ANOTHER CLAIM. $\gcd(ma, mb) = m\gcd(a, b)$.

Proof. Suppose g divides a and b . Then mg divides ma and mb . Thus, $m \gcd(a, b)$ divides both ma and mb so by the previous claim, $m \gcd(a, b) \mid \gcd(ma, mb)$. On the other hand, letting $h = \gcd(ma, mb)$, since $m \mid ma$ and $m \mid mb$, by the previous claim again, $m \mid h$, so let's write $h = mh'$. Then $mh' \mid ma$ and $mh' \mid mb$ which just means $h' \mid a$ and $h' \mid b$. By a third application of the previous claim, we have $h' \mid \gcd(a, b)$. Multiplying by m , we have $mh' \mid m \gcd(a, b)$ or $\gcd(ma, mb) \mid m \gcd(a, b)$. Since $m \gcd(a, b) \mid \gcd(ma, mb)$ and $\gcd(ma, mb) \mid m \gcd(a, b)$, we must have $\gcd(ma, mb) = \pm m \gcd(a, b)$ but since they are both positive, the $+$ sign must hold.

So now we have $\gcd(a + b, a - b) \mid \gcd(2a, 2b) = 2 \gcd(a, b) = 2$. Thus, $\gcd(a + b, a - b)$ is either 1 or 2.

(b) For $\alpha, \beta \in \mathbb{G}$ such that $(\alpha, \beta) = \mathbb{G}$, what values can $\gcd(\alpha + \beta, \alpha - \beta)$ take? Prove that your answer is correct.

If $(\alpha, \beta) = \mathbb{G}$, then $\gcd(\alpha + \beta, \alpha - \beta) \mid 2$ so it is in the set

$$\{\pm 1, \pm i, \pm(1 + i), \pm i(1 + i), \pm 2, \pm 2i\}.$$

Proving the second half of the above statement is easy because the set is just the set of divisors of $2 = -i(1 + i)^2$. To prove the first half, we just follow the same proof as above. if $(\gamma) = (\alpha + \beta, \alpha - \beta)$, then $\gamma \mid 2\alpha$ and $\gamma \mid 2\beta$. Then $2\alpha \in (\gamma)$ and $2\beta \in (\gamma)$ so $(2\alpha, 2\beta) \subseteq (\gamma)$. But $(2\alpha, 2\beta) = 2(\alpha, \beta) = 2(1) = (2)$, so $(2) \subseteq (\gamma)$ i.e. $\gamma \mid 2$ as desired.

8. Suppose $(\alpha, \beta) = (\gamma)$. Thus, γ divides α and β , so we can write $\gamma\alpha' = \alpha$ and $\gamma\beta' = \beta$ for some $\alpha', \beta' \in \mathbb{G}$. Prove that $(\alpha', \beta') = \mathbb{G}$.

Hint: One option is to use proof by contradiction.

Another option is to just do it. We have $\gamma = \lambda\alpha + \mu\beta$ for some $\lambda, \mu \in \mathbb{G}$. Divide by γ to get $1 = \lambda\alpha' + \mu\beta'$. Thus, $1 \in (\alpha', \beta')$ so $(\alpha', \beta') = \mathbb{G}$.

9. Suppose $\alpha, \beta, \gamma \in \mathbb{G}$, such that $(\alpha, \beta) = \mathbb{G}$ and $\alpha\beta = \gamma^2$. Show that there exist $\lambda, \mu \in \mathbb{G}$ such that $\alpha \sim \lambda^2, \beta \sim \mu^2$. Recall that $\theta \sim \eta$ means that $\theta = \varepsilon\eta$ for some $\varepsilon \in \mathbb{G}^\times$.

Hint: Use the fact that \mathbb{G} is a unique factorization domain.

Note that the statement was first given on the homework (with $\alpha = \lambda^2$ and $\beta = \mu^2$) was not correct: for example, with $\alpha = i, \beta = -i, \alpha\beta = 1$ is a square but i and $-i$ are not squares in \mathbb{G} .

Let us write $\gamma = \pi_1^{a_1} \pi_2^{a_2} \dots \pi_r^{a_r}$, where π_1, \dots, π_r are the distinct Gaussian primes that divide γ . Then for each $j, 1 \leq j \leq r, v_{\pi_j}(\alpha\beta)$ is an even integer because

$$v_{\pi_j}(\alpha\beta) = v_{\pi_j}(\gamma^2) = v_{\pi_j}(\gamma\gamma) = v_{\pi_j}(\gamma) + v_{\pi_j}(\gamma) = 2v_{\pi_j}(\gamma).$$

But $v_{\pi_j}(\alpha\beta) = v_{\pi_j}(\alpha) + v_{\pi_j}(\beta)$. Now, if $v_{\pi_j}(\alpha) > 0$, i.e. if π_j divides α , then because $(\alpha, \beta) = (1)$, π_j cannot divide β so $v_{\pi_j}(\beta) = 0$. Thus, if π_j divides α , then $v_{\pi_j}(\alpha) + v_{\pi_j}(\beta) = v_{\pi_j}(\alpha) + 0 = v_{\pi_j}(\alpha) = 2v_{\pi_j}(\gamma)$ is even.

The upshot is that if π is a Gaussian prime that divides α , then $\pi \mid \gamma^2$ so $\pi \mid \gamma$ (remember if π divides $\alpha\beta$, then π divides either α or β) so $\pi \in \{\pi_1, \dots, \pi_r\}$, so $v_{\pi}(\alpha)$ is even. Therefore,

there exists a unit ε and some $\alpha_1 \in \mathbb{G}$ such that $\alpha = \varepsilon\alpha_1^2$. By symmetry we get the same for β .

Extra Credit

A. Prove that given $\alpha, \beta \in \mathbb{G}$, there exist $\lambda \in \mathbb{G}$ (unique up to multiplication by a unit) such that $(\alpha) \cap (\beta) = (\gamma)$. Explain why γ should be called a *lowest common multiple* for α and β .

B. With α, β, λ as in A, and $(\alpha, \beta) = (\gamma)$ prove that $\alpha\beta = \gamma\lambda\varepsilon$ for some unit $\varepsilon \in \mathbb{G}^\times$.