

UMASS AMHERST MATH 471 FALL 2006, F. HAJIR

SOLUTIONS FOR HOMEWORK 2: GAUSSIAN INTEGERS II

1. Recall that for integers m, a with $a \neq 0$, $\text{Rem}(m \div a)$ is the unique integer $r \in [0, |a|)$ such that $m = qa + r$ for some $q \in \mathbb{Z}$; i.e. it is the remainder when you divide m by a .

Suppose a is a positive integer, m, n are integers and $r = \text{Rem}(m \div a)$, $s = \text{Rem}(n \div a)$ are their remainders upon division by a .

(a) Suppose $r + s < a$. Show that $\text{Rem}((m + n) \div a) = r + s$.

Recall what it means for a number say t to be $\text{Rem}((m + n) \div a)$. It means that we can write $m + n = qa + t$ for some integer q and that $0 \leq t < a$. Now, let us write $m = ax + r$, $n = ay + s$ with $x, y \in \mathbb{Z}$. Then $m + n = a(x + y) + (r + s)$. Since $0 \leq r + s < a$, we have written $m + n$ in the form $aq + (r + s)$ with $q \in \mathbb{Z}$ so $(r + s)$ must be the remainder of $m + n \div a$.

(b) More generally, show that $\text{Rem}((m + n) \div a) = \text{Rem}((r + s) \div a)$.

With the same notation as above, we have $m + n = aq + (r + s)$. Now if we write $r + s = aq' + t$ with $q' \in \mathbb{Z}$ and $0 \leq t < a$, then $t = \text{Rem}((r + s) \div a)$ of course. We compute $m + n = aq + aq' + t$, so $m + n = aq'' + t$ with $q'' \in \mathbb{Z}$ and t is in the right range ($0 \leq t < a$) hence by the same principle as above, $t = \text{Rem}((m + n) \div a)$.

2. Suppose an integer t is of the form $t = 4k + 3$ with $k \in \mathbb{Z}$. Show that t cannot be expressed as $t = x^2 + y^2$ with $x, y \in \mathbb{Z}$.

Hint: proceed by contradiction and divide by 4.

Suppose the statement is false. Then there exists integers k, t, x, y with $t = 4k + 3 = x^2 + y^2$. We will derive a contradiction from this, and then we'll be done. Since $4k + 3$ is odd, x, y cannot both be even, nor both odd. So, without loss of generality, let us assume x is odd and y is even. Then we'll write $x = 2m + 1$ and $y = 2n$ with integers m, n . We compute

$$4k + 3 = (2m + 1)^2 + (2n)^2 = 4m^2 + 4m + 1 + 4n^2 = 4(m^2 + m + n^2) + 1.$$

Subtracting $4k + 1$ from both sides, we find $2 = 4q$ for some integer q . This is clearly impossible, because dividing by 2, we find $1 = 2q$ for an integer q , which is absurd. Thus, integers that give remainder 3 when divided by 4 cannot be sums of two squares.

3. Show that if p is a prime of the form $4k + 3$ with $k \in \mathbb{Z}$, then p is a Gaussian prime.

Suppose p is NOT a Gaussian prime. Then there exist non-zero non-units $\alpha, \beta \in \mathbb{G}$ such that $p = \alpha\beta$. Taking norms, we find $p^2 = N(\alpha)N(\beta)$. Since α and β are *not* units, they cannot have norm 1. Since they are not 1 and they multiply together to give p^2 , they must

both equal p : there is no other way to factor p^2 as a product of integers! Thus, we must have $N(\alpha) = N(\beta) = p$. By the lemma proved in HW1, since α has prime norm p , it is a Gaussian prime.

4. Given that $167^2 + 32^2 = 28913$, find integers a, b such that $28913000 = a^2 + b^2$.
Hint: $1000 = 100 + 900$.

Say we have $x^2 + y^2 = n$. That means $N(x + iy) = n$. Now, $1000 = 10^2 + 30^2$ so $N(10 + 30i) = 1000$. Recalling that the norm N is multiplicative, we then have $N((x + iy)(10 + 30i)) = 1000n$, in other words, $N((x + iy)(10 + 30i)) = 1000n$. Using this idea, then we compute

$$(167 + 32i)(10 + 30i) = 1670 - 32 \cdot 30 + 167 \cdot 30i + 320i = 710 + 5330i,$$

which gives $710^2 + 5330^2 = 28913000$.

5. Compute the Gaussian Prime Factorization of $\gamma = 1527 - 199i$.
Hint: $2371330 = 2 \cdot 5 \cdot 13 \cdot 17 \cdot 29 \cdot 37$.

We simply try to find elements of norm $2, 5, 13, 17, 29, 37$ that go into γ . So to start: $\gamma_1 = \gamma/(1 + i) = 664 - 863i$. Next, $\gamma_2 = \gamma_1/(2 + i) = 93 - 478i$. Now $\gamma_2/(3 + 2i) = -677/13 - 1620/13i$ is not integral so we try instead $\gamma_3 = \gamma_2/(2 + 3i) = -96 - 95i$. Keepin' on truckin', we get $\gamma_4 = \gamma_3/(1 + 4i) = -28 + 17i$, and $\gamma_5 = \gamma_4/(2 + 5i) = 1 + 6i$ and $\gamma_6 = \gamma_5/(1 + 6i) = 1$.

The upshot is that

$$\gamma = (1 + i)(2 + i)(2 + 3i)(1 + 4i)(2 + 5i)(1 + 6i)$$

is a factorization of γ into Gaussian primes.

6. Recall that we say $\beta \div \alpha$ has quotient $\kappa \in \mathbb{G}$ and remainder $\rho \in \mathbb{G}$ if $\beta = \kappa\alpha + \rho$ and $|\rho|^2 < |\alpha|^2$.

Calculate “the” quotient κ and “the” remainder ρ for $\beta \div \alpha$; explain in each case if the quotient and remainder are unique or not.

- (a) $\alpha = 2 + i$ and $\beta = 14 + i$.

We divide

$$\frac{\beta}{\alpha} = \frac{(14 + i)(2 - i)}{5} = \frac{29 - 12i}{5}.$$

We round this to $\kappa = 6 - 2i$. This is the unique closest Gaussian integer to β/α , because there is no ambiguity in rounding $29/5$ or $12/5$ to the closest integer. To compute the remainder, we write $14 + i = (2 + i)(6 - 2i) + \rho$ and compute $\rho = 14 + i - (14 + 2i) = -i$, so $N(\rho) = 1 < N(2 + i) = 5$ as desired. The quotient and remainder are unique in this case.

- (b) $\alpha = 1 + i$ and $\beta = 1 + 2i$.

This time $\beta/\alpha = 1.5 + 0.5i$ so it can be rounded to 4 Gaussian integers: there are 4 Gaussian integers all having an equal claim on being “the” closest to β/α , namely $1, 1 + i, 2,$ and $2 + i$. If we say the quotient is $\kappa = 2 + i$, say, then the remainder is $\rho = (1 + 2i) - (1 + i)(2 + i) = -i$ has norm 1.

7. Recall that for $\alpha \in \mathbb{G}$, $(\alpha) = \{\alpha\lambda \mid \lambda \in \mathbb{G}\}$ is called the “ideal” generated by α . Similarly, for $\alpha, \beta \in \mathbb{G}$, we define

$$(\alpha, \beta) = \{\alpha\lambda + \beta\mu \mid \lambda, \mu \in \mathbb{G}\}$$

and call this the ideal generated by α and β .

(a) Prove that if $\gamma \in (\alpha, \beta)$, then $\gamma\delta \in (\alpha, \beta)$ for all $\delta \in \mathbb{G}$.

If $\gamma \in (\alpha, \beta)$, then $\gamma = \alpha\lambda_1 + \beta\lambda_2$ for some $\lambda_i \in \mathbb{G}$. If κ is any element of \mathbb{G} , then multiplying the previous equality by it we get $\gamma\kappa = \alpha\lambda_1\kappa + \beta\lambda_2\kappa$ which certifies that $\gamma\kappa$ is a \mathbb{G} -linear combination of α and β , so $\gamma\kappa \in (\alpha, \beta)$.

(b) Prove that $(\alpha, \beta) = \mathbb{G}$ if and only if $1 \in (\alpha, \beta)$.

Clearly, if $(\alpha, \beta) = \mathbb{G}$, then since $1 \in \mathbb{G}$ we get $1 \in (\alpha, \beta)$. Conversely, if $1 \in (\alpha, \beta)$, then for all $\kappa \in \mathbb{G}$, by part (a) of this problem $1\kappa = \kappa \in (\alpha, \beta)$. Hence $\mathbb{G} \subseteq (\alpha, \beta)$. But by definition $(\alpha, \beta) \subseteq \mathbb{G}$ giving us $\mathbb{G} = (\alpha, \beta)$.

(c) Prove that $(\alpha, \beta) = \mathbb{G}$ if and only if $(\alpha, \beta) \cap \mathbb{G}^\times$ is not empty.

If $(\alpha, \beta) = \mathbb{G}$ then $(\alpha, \beta) \cap \mathbb{G}^\times = \mathbb{G} \cap \mathbb{G}^\times = \mathbb{G}^\times \neq \emptyset$ so that direction is easy. Now suppose $(\alpha, \beta) \cap \mathbb{G}^\times$ is non-empty so it contains some element ε say. Clearly $\varepsilon \in \mathbb{G}^\times$, so there exists $\theta \in \mathbb{G}$ such that $\varepsilon\theta = 1$. By (a), since $\varepsilon \in (\alpha, \beta)$, $\varepsilon\theta \in (\alpha, \beta)$ also. Thus, $1 \in (\alpha, \beta)$, so by (b), $(\alpha, \beta) = \mathbb{G}$. Done.

8. Show that $(6 + i, 19 - 7i) = \mathbb{G}$.

We could show this directly by finding a linear combination giving 1, or we could be sneaky. Namely, $N(6 + i) = 37$ and $N(19 - 7i) = 410$. Now it's easy to see that 37 does not divide 410 and 37 being prime we conclude that $\gcd(37, 410) = 1$. (Why?) Now suppose $(6 + i, 19 - 7i) = (\gamma)$. We showed in class such a γ always exist (and it can be taken to be an element of smallest positive norm in the ideal). Since $6 + i$ and $19 - 7i$ belong to (γ) , they are both divisible by γ , so $6 + i = \gamma\alpha_1$ and $19 - 7i = \gamma\alpha_2$. Then taking norms and remembering that the norm is multiplicative, we get $37 = N(\gamma)N(\alpha_1)$ and $410 = N(\gamma)N(\alpha_2)$. Thus, $N(\gamma)$ is a common divisor of 37 and 410. But $\gcd(37, 410) = 1$ so that must mean $N(\gamma) = 1$ so γ is a unit, so we're done by (c) of previous problem.

But now let's use honest elbow grease. Dividing, we find

$$19 - 7i = (6 + i)(3 - 2i) + (-1 + 2i)$$

so $-1 + 2i$ is in $(6 + i, 19 - 7i)$. Now let's try to find a “smaller” linear combination of $-1 + 2i$ and $6 + i$, i.e. we divide $6 + i \div -1 + 2i$ and find

$$(6 + i) = (-1 + 2i)(-1 - 3i) + 1$$

. Thus, 1 is a linear combination of $6 + i$ and $-1 + 2i$ which are both in the ideal $(6 + i, 19 - 7i)$ so $1 \in (6 + i, 19 - 7i)$ so $(6 + i, 19 - 7i) = \mathbb{G}$. An actual linear combination of the original two numbers which gives on is

$$(8 + 7i)(6 + i) + (-1 - 3i)(19 - 7i) = 1.$$

9. For each $r \in \mathbb{N}$, let $B_r = \{\alpha \in \mathbb{G} \mid |\alpha|^2 \leq r\}$ be the set of those Gaussian integers which are of norm at most r (i.e. those Gaussian integers whose distance from the origin is at most \sqrt{r} : these are the grid points inside the circle of radius r around the origin).

(a) Draw a picture of the set $B_{20} \cap (1 + 3i, 3 + i)$, which are those grid points within the circle of radius 20 that are in the ideal $(1 + 3i, 3 + i)$.

This turns out to be all the \mathbb{G} -multiples of $1 + i$.

(b) What are the elements of smallest norm in the ideal $(1 + 3i, 3 + i)$? Are these all associates of one another?

They are $1 + i, -1 + i, -1 - i, 1 - i$.

(c) Now draw a picture of the set $B_{20} \cap (1 + i)$.

It's the same picture!

(d) Can you make a conjecture about the ideals $(1 + i)$ and $(1 + 3i, 3 + i)$ based on (a) and (b)? Can you prove that conjecture?

They are the same. Why? Because $1 + i$ is the element of smallest positive norm in $(1 + 3i, 3 + i)$ and as we proved in class, the element of smallest positive norm in an ideal is a generator of it!

10. Recall that for $\alpha, \gamma \in \mathbb{G}$ we write $\alpha|\gamma$ (read: α divides γ) if there exists $\lambda \in \mathbb{G}$ such that $\gamma = \alpha\lambda$.

(a) Suppose $\alpha, \beta, \gamma \in \mathbb{G}$ and $(\alpha, \beta) = \mathbb{G}$. Show that if $\alpha|\gamma$ and $\beta|\gamma$, then $\alpha\beta|\gamma$.

Since $(\alpha, \beta) = \mathbb{G}$, we can find $\lambda, \mu \in \mathbb{G}$ such that $\alpha\lambda + \beta\mu = 1$. We also know that $\alpha\alpha' = \gamma$ and $\beta\beta' = \gamma$ for some $\alpha', \beta' \in \mathbb{G}$. Multiplying the previous equation by γ we get

$$\gamma = \gamma\alpha\lambda + \gamma\beta\mu.$$

Let's divide! We get

$$\frac{\gamma}{\alpha\beta} = \frac{\gamma\lambda}{\beta} + \frac{\gamma\mu}{\alpha} = \beta'\lambda + \alpha'\mu \in \mathbb{G}.$$

We divided γ by $\alpha\beta$ and got something in \mathbb{G} so $\alpha\beta|\gamma$ as desired.

(b) Show via an example that in (a) we cannot dispense with the assumption $(\alpha, \beta) = \mathbb{G}$.

That's easy. If $\alpha = \beta = (1 + i)$, then α and β both divide $(1 + i)$ but $(1 + i)$ is not divisible by $\alpha\beta(1 + i)^2 = 2i$ because $(1 + i)/(2i) = 1/2 - i/2$.

Extra Credit.

A. Find integers a, b such that $p = a^2 + b^2$ where p is the prime

$$p = 2938741902873409187309487102983740198723094871902387717.$$

A little advice: there is only one pair (a, b) of positive integers that solves this and a and b are each greater than 10^{24} , so I think that rules out trial and error.