

Prof. Valentin Blomer

University of Toronto
Department of Mathematics

Algebra

Problem Set 9 (due Nov 28, 2006)

9.1. a) Find a generator for the principal ideal $(47 - 13i, 53 + 56i) \in \mathbb{Z}[i]$.

b) Let R be a commutative ring with unity, $a, b \in R \setminus \{0\}$. Give a reasonable definition for a least common multiple of a and b . If R is factorial, show that a least common multiple always exists and give an explicit expression in terms of the prime factorization of a and b . If R is a principal ideal domain, give an expression in terms of the ideals (a) and (b) .

9.2. Let $\mathfrak{a} = (\alpha) \in \mathbb{Z}[i]$ be an ideal. We define the norm $N\mathfrak{a}$ of \mathfrak{a} to be the cardinality of $\mathbb{Z}[i]/\mathfrak{a}$. Show that $N\mathfrak{a}$ is finite and equals $N(\alpha) = |\alpha|^2$. Conclude again that in $\mathbb{Z}[i]$ every prime ideal is maximal.

Suggestion: If you like, you can proceed as follows:

a) Prove the claim for α a Gaussian prime. If $\alpha \mid p$ for some $p \equiv 1 \pmod{4}$, use the Chinese remainder theorem (check the hypotheses!)

b) Prove the claim for $\alpha = \pi^j$ a power of a Gaussian prime using the isomorphism $\mathbb{Z}[i]/(\pi) = (\pi^{j-1})/(\pi^j)$.

c) Conclude the claim for any α using the Chinese remainder theorem.

9.3. Let $R = \mathbb{Z}[\sqrt{-5}]$, and $\mathfrak{a} := (2, 1 + \sqrt{-5})$, $\mathfrak{b} := (3, 2 + \sqrt{-5})$, $\mathfrak{c} := (3, 2 - \sqrt{-5})$.

a) Pick your favourite ideal out of $\mathfrak{a}, \mathfrak{b}, \mathfrak{c}$, and show that it is prime. *Hint:* You could count the order of the quotient.

b) Show that $(6) = \mathfrak{a}^2\mathfrak{b}\mathfrak{c}$ is a decomposition of (6) (into prime ideals).

9.4. Find all pairs (x, y) of integers satisfying $x^2 + 2 = y^3$. *Hint:* You can use that $\mathbb{Z}[\sqrt{-2}]$ is factorial. It might also be useful to show first that x must be odd.

9.5. (*voluntarily*) Let $r(n) := \{(a, b) \in \mathbb{Z}^2 \mid n = a^2 + b^2\}$ be the number of representations of n as a sum of two squares. Since $\#\mathbb{Z}[i]^* = 4$, we have $\tilde{r}(n) := \frac{1}{4}r(n) = \#\{\mathfrak{a} \in \mathbb{Z}[i] \mid N\mathfrak{a} = n\}$. Let $\chi(n) = 1$ if $n \equiv 1 \pmod{4}$, $\chi(n) = -1$ if $n \equiv -1 \pmod{4}$, and $\chi(n) = 0$ if n is even.

For $\Re s > 1$ let $\zeta(s)$ be the Riemann ζ function, let $L(s, \chi) := \sum_n \chi(n)n^{-s}$ be the L -function attached to χ , and let

$$Z(s) := \sum_{\substack{\{0\} \neq \mathfrak{a} \subseteq \mathbb{Z}[i] \\ \mathfrak{a} \text{ ideal}}} \frac{1}{(N\mathfrak{a})^s} = \sum_{n=1}^{\infty} \frac{\tilde{r}(n)}{n^s}$$

be the Zeta-function attached to the Gaussian integers.

a) Show that $r(n) = 4 \sum_{d|n} \chi(d)$

b) Conclude (one line) that $Z(s)$ factors as $\zeta(s)L(s, \chi)$.

c) Show (one line) that every interval $[x, x + 10x^{1/4}]$, $x > 1$, contains an integer n that is the norm of an ideal in $\mathbb{Z}[i]$, or equivalently, that can be written as a sum of two squares. *Hint:* Be greedy.

Suggestion: In order to show the first part, you could proceed as follows: A function $f : \mathbb{N} \rightarrow \mathbb{C}$ is called multiplicative, if $f(ab) = f(a)f(b)$ whenever $(a, b) = 1$.

a) Show that $\frac{1}{4}r(n)$ is multiplicative (where do you use $(a, b) = 1$?).

b) Clearly χ is multiplicative. If f is multiplicative, then $\sum_{d|n} f(d)$ is multiplicative (where do you use $(a, b) = 1$?).

c) By a) and b) it is enough to prove the claim for $n = p^k$ a prime power. Distinguish the cases $p = 2$, $p \equiv 1 \pmod{4}$ and $p \equiv 3 \pmod{4}$.

Remarks: a) One can show that if K/\mathbb{Q} is any abelian extension of degree d and discriminant D , then there are $d - 1$ periodic, multiplicative functions χ_j of period dividing $|D|$ such that the zeta-function attached to K factors as $\zeta(s) \prod_j L(s, \chi_j)$. The above problem corresponds to simplest non-trivial extension $K = \mathbb{Q}(i)$ of degree 2 and discriminant -4.

b) Conjecturally, for any $\varepsilon > 0$ there is a constant $c(\varepsilon)$ such that every interval $[x, x + c(\varepsilon)x^\varepsilon]$, $x > 1$, contains a sum of two squares. Proving (or disproving) this for any $0 < \varepsilon < 1/4$ is worth a PhD.