Math 104a: Number theory – Problem set 3

François Thilmany

due Friday 20 July 2018

Problem 1. Let $\xi = \sqrt{-5}$, and consider the subset $\mathbb{Z}[\xi] = \{a + b\xi \mid a, b \in \mathbb{Z}\}$ of $\mathbb{C}$. Prove that:

(a) $\mathbb{Z}[\xi]$ is an integral domain.
(b) The units of $\mathbb{Z}[\xi]$ are 1 and -1
(c) The elements 2, 3, $1+\xi$ and $1-\xi$ are irreducible in $\mathbb{Z}[\xi]$.
(d) No two distinct elements among 2, 3, $1+\xi$ and $1-\xi$ are associate in $\mathbb{Z}[\xi]$.
(e) None of 2, 3, $1+\xi$ and $1-\xi$ are prime in $\mathbb{Z}[\xi]$.
(f) $2(1+\xi)$ and 6 do not have a greatest common divisor.

Does $\mathbb{Z}[\xi]$ satisfy unique factorization? Is it a Euclidean domain?

Hint: The restriction of the complex norm gives a function

$$N : \mathbb{Z}[\xi] \to \mathbb{N} : a + b\xi \mapsto a^2 + 5b^2.$$

Use that N is multiplicative.

Problem 2. Let $p \in \mathbb{Z}$ be a prime number. If p can be represented as a sum of squares, say $p = a^2 + b^2$ for $a, b \in \mathbb{Z}$, then this representation is unique (i.e. the squares a^2 and b^2 are unique).

Hint: Factor p in $\mathbb{Z}[i]$.

Problem 3. Let (a, b, c) be a primitive Pythagorean triple, i.e. $a^2 + b^2 = c^2$ and the only common divisors of a, b and c are ± 1. Show that exactly one of a, b, c is divisible by 5. Can it be a? Can it be c?

Problem 4. Let $a > 0$ be an integer which is divisible by 4. Show that there exist $b, c \in \mathbb{N}$ such that (a, b, c) is a primitive Pythagorean triple.

Problem 5. Let $I = (3 + 2i)\mathbb{Z}[i]$ be the ideal of $\mathbb{Z}[i]$ consisting of the multiples of $3 + 2i$. Show that the quotient $\mathbb{Z}[i]/I$ can be identified with the finite ring $\mathbb{Z}_{13}$.

Hint: First show that for any $\alpha \in \mathbb{Z}[i]$, you can find $\beta \in \mathbb{Z}$ such that $\alpha - \beta \in I$. Then show $13 \in I$. Finally, show that $(3 + 2i)$ does not divide any of the integers between 1 and 12.

Problem 6. Compute

(a) 5^{2018} in $\mathbb{Z}_7$
(b) 6^{2018} in $\mathbb{Z}_{256}$
(c) 5^{2m} in $\mathbb{Z}_{17}$, in terms of $m \in \mathbb{N}$
(d) 2^{3m} in $\mathbb{Z}_{17}$, in terms of $m \in \mathbb{N}$
(e) $3 \cdot 5^{2m+1} + 2^{3m+1}$ in $\mathbb{Z}_{17}$, in term of m.

Problem 7. Let G be a group and $g \in G$. The order of g is defined to be

$$\operatorname{ord} g := \min\{n \in \mathbb{N} - \{0\} \mid g^n = e\}.$$

When R is a ring, the order of 1 in the additive group $(R, +)$,

$$\operatorname{ord} 1 = \min\{n \in \mathbb{N} - \{0\} \mid \underbrace{1 + 1 + \cdots + 1}_{n \text{ times}} = 0\},$$

is called the characteristic of the ring R *if it is finite*. If 1 has infinite order in $(R, +)$, then R is said to have characteristic 0.

Prove that if R is a domain, then the characteristic of R must be either 0, 1, or a prime number. Show that for any integer $m > 0$, the characteristic of $\mathbb{Z}_m$ is m. Deduce that $\mathbb{Z}_m$ is never a domain when m is a composite integer (i.e. m is not a prime nor a unit).

Problem 8. Let $m \in \mathbb{N}$ and assume $m \neq 0, 1$. Find all the units of the ring $\mathbb{Z}_m$. Deduce that the following are equivalent: (i) $\mathbb{Z}_m$ is a field; (ii) $\mathbb{Z}_m$ is a domain; (iii) m is prime.

Hint: Which elements in $\mathbb{Z}_m (= \mathbb{Z}/m\mathbb{Z})$ have no chance of being invertible? For the others, use Bézout's identity.

Problem 9. For the purpose of this problem, let ζ be an abstract symbol. Endow the nine-element set

$$\mathbb{F}_9 := \{a + b\zeta \mid a, b \in \mathbb{Z}_3\} = \{0, 1, 2, \zeta, 1 + \zeta, 2 + \zeta, 2\zeta, 1 + 2\zeta, 2 + 2\zeta\}$$

with the ring structure given by the following addition and multiplication: $(a, b, c, d \in \mathbb{Z}_3)$

$$(a + b\zeta) + (c + d\zeta) := (a + c) + (b + d)\zeta$$
$$(a + b\zeta) \cdot (c + d\zeta) := (ac - bd) + (bc + ad)\zeta.$$

(In the right hand side, all the operations inside the parentheses are carried out in $\mathbb{Z}_3$. You may assume that these operations do define a valid ring structure on $\mathbb{F}_9$.)

(a) Find the neutral elements in $\mathbb{F}_9$ for this addition and multiplication. Compute ζ^2. Show that $1 + \zeta$ is a unit, and find its (multiplicative) inverse.
(b) What is the characteristic of the ring $\mathbb{F}_9$?
(c) Let $I = 3\mathbb{Z}[i]$ be the ideal of $\mathbb{Z}[i]$ consisting of all the multiples of 3 in $\mathbb{Z}[i]$. Show that you can identify the elements of the quotient ring $\mathbb{Z}[i]/I$ with the elements of $\mathbb{F}_9$ (bijectively) in such a way the addition and multiplication of $\mathbb{Z}[i]/I$ correspond to the addition and multiplication of $\mathbb{F}_9$ defined above. (In other words, show that $\mathbb{Z}[i]/I$ and $\mathbb{F}_9$ are isomorphic rings.)

(d) Show that you cannot do the same with the ring $\mathbb{Z}_9$, i.e. that $\mathbb{Z}[i]/I$ and $\mathbb{Z}_9$ are non-isomorphic rings. (Thus $\mathbb{Z}[i]/I$ is an example of a ring of residues which is not one of the usual $\mathbb{Z}_m$'s.)

Problem 10. Let $a, b \in \mathbb{Z}$ be odd. Prove that

(a) $ab - 1 = (a-1) + (b-1) \mod 4$

(b) $a^2 = 1 \mod 8$

(c) $(ab)^2 - 1 = (a^2 - 1) + (b^2 - 1) \mod 64$.

Problem 11. (a) Prove that $10^n = 1 \mod 9$ for any $n \in \mathbb{N}$. Deduce the familiar criterion for divisibility by 9: the residue modulo 9 of a number written $a_n a_{n-1} \dots a_1 a_0$ in decimal expansion (with digits $a_i \in \{0, 1, \dots, 9\}$) is equal to the residue of the sum $\sum_{i=0}^n a_i$ modulo 9.

Use this to show that the residue modulo 9 of an integer is invariant under any permutation of its decimal digits.

(b) Prove that $10^n = (-1)^n \mod 11$. Deduce the following criterion for divisibility by 11: the residue modulo 11 of a number written $a_n a_{n-1} \dots a_1 a_0$ in decimal expansion (with digits $a_i \in \{0, 1, \dots, 9\}$) is equal to the residue modulo 11 of the alternating sum $\sum_{i=0}^n (-1)^i a_i$.

Use this criterion to show that a palindromic number with an even number of digits is always divisible by 11. (A number is called *palindromic* if its decimal expansion reads the same from left to right as in reverse, from right to left. For example, 1234554321 is palindromic.)

Problem 12. Find all triples of prime numbers which are of the form $(n, n+2, n+4)$ for some $n \in \mathbb{Z}$.

Problem 13. Let f be a polynomial with integers coefficients, say $f = a_n x^n + a_{n-1} x^{n-1} + \dots + a_0$ with $a_i \in \mathbb{Z}$, and fix an integer $r \geq 2$. Assume that there are r consecutive integer values $f(m_0)$, $f(m_0 + 1)$, $\dots$, $f(m_0 + r - 1)$ of f that are divisible by r. Prove that this implies that $f(m)$ is divisible by r for every integer m. Give an example of a polynomial f with coprime coefficients and an integer $r \geq 2$ which realize the assumption.

Hint: Apply the ring homomorphism from $\mathbb{Z}$ to $\mathbb{Z}_r$.

Problem 14. Show that $(0, 0)$ is the only pair of integers that is solution to the equation $x^2 + 6xy + y^2 = 0$.

Hint: Look at the equation in $\mathbb{Z}_5$.

Problem 15. Use the Euclidean algorithm and Bézout's identity to compute the inverses of

(a) 4 in $\mathbb{Z}_{15}$

(b) 9 in $\mathbb{Z}_{200}$

(c) 3 in $\mathbb{Z}_{200}$

(d) 7 in $\mathbb{Z}_{330}$.