Math 104a: Number theory – Problem set 2

François Thilmany

due Friday 13 July 2018

Problem 1. Solve (i.e. find all integral solutions to) the following linear diophantine equations:

(a) $4x + 5y = 0$
(b) $4x + 5y = -2$
(c) $49x - 35y = 14$
(d) $15x + 27y = 35$

Problem 2. Alice owes Bob \$107, but only has banknotes worth \$5 and \$7 (Alice and Bob live in Fiji). How should Alice proceed in the following situations? (Provide all solutions and justify them properly.)

(a) Alice would like to pay back Bob (the exact amount) with as few bills as possible.
(b) Out of spite, Alice would like to return the exact amount to Bob using as many bills as possible.
(c) Bob actually has change: he has \$5 notes and is willing to give Alice change back if she overpays. Together, they would like to minimize the total number of bills that get exchanged.

Problem 3. How many ways are there to make \$100 from 1000 coins, using only quarters (\$0.25), dimes (\$0.10) or nickels (\$0.05)?

For the problems below, you will need some definitions that we will cover on Monday 9th. At the end of this document, I included these definitions and some examples. I encourage you to read ahead and start working on the problems.

Problem 4. Let G be a group and $g \in G$. For any $n \in \mathbb{Z}$, denote by g^n the n-fold product $g \cdot g \cdot \cdots \cdot g$ if $n > 0$. Otherwise, if $n < 0$, denote by g^n the $|n|$-fold product $g^{-1} \cdot g^{-1} \cdot \cdots \cdot g^{-1}$. If $n = 0$, we set $g^0 = e$, the neutral element of G.

Show that the set $\{\dots, g^{-2}, g^{-1}, g^0, g^1, g^2, \dots\}$ of all the "powers" of g is a group with the same multiplication as G. It is called the *subgroup generated by* g.

Problem 5. Let G be a set endowed with a binary operation $\cdot : G \times G \to G$ such that G satisfies all the axiom of a group except perhaps for the existence of inverses:

(A) $\cdot$ is associative, i.e. $(g \cdot h) \cdot k = g \cdot (h \cdot k)$ for all $g, h, k \in G$

(N) There is an element $e \in G$ such that $g \cdot e = g = e \cdot g$ for all $g \in G$.

Fix an element $g \in G$, and let l_g denote the map "left multiplication by g", defined by

$$l_g : G \to G : h \mapsto l_g(h) = gh.$$

Prove that the existence of an inverse for g is equivalent to the fact that l_g is bijective. Deduce that if G is a group, then l_g is always bijective.

Hint: If g has an inverse g^{-1}, show that l_g and $l_{g^{-1}}$ are inverses (as maps $G \to G$), so that l_g is a bijection. For the converse, first use that l_g is surjective to find a right inverse h for g, then use injectivity to show that h is also a left inverse.

Problem 6. (a) Let $\xi = \frac{1+\sqrt{5}}{2}$ and let $\mathbb{Z}[\xi]$ denote the subset $\{a + b\xi \mid a, b \in \mathbb{Z}\}$ of $\mathbb{R}$. Show that $\mathbb{Z}[\xi]$, endowed with the usual addition and product of real numbers, is an integral domain.

Hint: Show that $\xi^2 = \xi + 1$, and use it to check that multiplication $\mathbb{Z}[\xi] \times \mathbb{Z}[\xi] \to \mathbb{Z}[\xi]$ is well defined. Think about which axioms you need to check, and which ones are automatically true because they hold in $\mathbb{R}$.

(b) Let $\chi = \frac{\sqrt{5}}{2}$ and let $\mathbb{Z}[\chi]$ denote the subset $\{a + b\chi \mid a, b \in \mathbb{Z}\}$ of $\mathbb{R}$. Show that $\mathbb{Z}[\chi]$, if endowed with the usual multiplication and addition of real numbers, is *not* a ring.
Hint: You may use that $\sqrt{5} \notin \mathbb{Q}$.

Problem 7. Let D be an integral domain and let $a, b \in D$. If d and d' are gcd's of a and b, prove that there exists a unit $u \in D^\times$ such that $d' = ud$. Conversely, prove that if $u \in D^\times$ and d is a gcd of a and b, then ud is also a gcd of a and b.

(This shows that the gcd is unique *up to multiplication by a unit*.)

Problem 8. Show that $\mathbb{C}[x]$, the ring of polynomials with coefficients in $\mathbb{C}$, is a Euclidean domain with Euclidean function the degree, $\deg : \mathbb{C}[x] - \{0\} \to \mathbb{N} : P \mapsto \deg P$.

Hint: To show that $\mathbb{C}[x]$ is a domain, use the degree function. To prove that deg is an acceptable Euclidean function, use long division of polynomials.

Problem 9. Let D be a Euclidean domain with Euclidean function $s : D - \{0\} \to \mathbb{N}$. Show that if a divides b and $s(a) = s(b)$, then a and b are associates. Give an example to show that the hypothesis "a divides b" is necessary.

Hint: Write the Euclidean division of a by b, say with remainder r. What can you say about $s(r)$?

Problem 10. Let D be a Euclidean domain. Using Bézout's identity, prove Euclid's lemma: if $p \in D$ is irreducible, then p is prime.

Hint: Adapt the proof we have seen for $D = \mathbb{Z}$.

Problem 11. Show that $1+i$ is a prime in the Euclidean domain $\mathbb{Z}[i] = \{a+bi \mid a, b \in \mathbb{Z}\} \subset \mathbb{C}$. Is 2 a prime in $\mathbb{Z}[i]$? What about 7?

Definitions for problems 4-11

Definition. Let S be a set. A binary operation on S is a map $S \times S \to S$. Binary operations are often denoted with the common symbols $*$, $\cdot$, $+$, $\circ$, etc. If, say, $*$ denotes a binary operation $* : S \times S \to S$, then the image of a couple $(a, b) \in S$ will be denoted $a * b$.

Definition. A *group* is a set G endowed with a binary operation $* : G \times G \to G$ ($*$ is often called the *product* of G) with the following three properties:

(A) $*$ is associative: for any $a, b, c \in G$, $(a * b) * c = a * (b * c)$

(N) $*$ has a neutral element e (called *identity*): there exists $e \in G$ such that $g * e = g = e * g$ holds for any $g \in G$.

(I) every element has an inverse for $*$: for any $g \in G$, there exists $h \in G$ such that $h * g = e = g * h$.

If in addition, a group G satisfies the commutativity property below, then G is called *commutative* or *abelian*.

(Com) $*$ is commutative: For any $g, h \in G$, we have $h * g = g * h$.

Example. In lectures, we will briefly explain why the following sets with binary operations are commutative groups. (Can you identify the neutral element in each case?)

(i) $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ with the usual addition $+$

(ii) $\{1, -1\}$ with usual multiplication $\cdot$

(iii) $\{1, i, -1, -i\}$ with multiplication $\cdot$ of complex numbers.

(iv) The set $\mathbb{Q}^\times = \mathbb{Q} - \{0\}$ of non-zero rational numbers with usual multiplication $\cdot$

(v) The set $\mathbb{R}^\times$ of non-zero real numbers with usual multiplication $\cdot$

(vi) The set $\mathbb{C}^\times$ of non-zero complex numbers with usual multiplication $\cdot$

Definition. A ring is a set R with two binary operations: *addition* "+" and *multiplication* "$\cdot$", that satisfy the following properties:

- R is a commutative group with $+$, i.e.
  - (A) $+$ is associative
  - (N) $+$ has a neutral element denoted 0
  - (I) every element $a \in R$ has an inverse for $+$, called the *opposite* and denoted $-a$.
  - (Com) $+$ is commutative
- Multiplication $\cdot : R \times R \to R$ satisfies
  - (A) $\cdot$ is associative
  - (N) $\cdot$ has a neutral element denoted 1
  - (Com) $\cdot$ is commutative
- $+$ and $\cdot$ are compatible via the distribution law:
  - (D) for any $a, b, c \in R$, we have $a \cdot (b + c) = a \cdot b + a \cdot c$.

Example. In lectures, we will briefly explain why the following sets with operations are rings. In this homework, you may use this fact without proof, but indicate where you use it.

(i) $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ are rings with the usual addition and usual multiplication.

(*ii*) The set $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\} \subset \mathbb{C}$ with addition and multiplication of complex numbers.

(*iii*) $\mathbb{C}[x]$, the set of polynomials with coefficients in $\mathbb{C}$, is a ring with addition and multiplications of polynomials.

Definition. Let D be a ring. If D satisfies the cancellation law

(C) for any $a \in D - \{0\}$ and $b, c \in D$, if $ab = ac$ then $b = c$

and if $D \neq \{0\}$ (equivalently, $1 \neq 0$ in D), then D is called an *integral domain* (or *domain* for short). By convention, the one-element ring $R = \{0\}$ is not a domain.

Example. The examples of rings $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}[i]$ and $\mathbb{C}[x]$ above are all integral domains. We will see examples of rings that are not domains in class.

Definition. An integral domain D is called Euclidean if there is a Euclidean function $s : D - \{0\} \to \mathbb{N}$. A Euclidean function is a function $s : D - \{0\} \to \mathbb{N}$ which satisfies the two properties:

(*i*) If $a, b \in D - \{0\}$ are such that a divides b, then $s(a) \leq s(b)$.

(*ii*) For any $a, b \in D - \{0\}$, there are $q, r \in D$ such that

$$a = bq + r \quad \text{and either } r = 0 \text{ or } s(r) < s(b).$$

Property (*ii*) says we can do Euclidean division in D using s.

Example. (*i*) We have proved in class that $\mathbb{Z}$ is a Euclidean domain with the Euclidean function $s(a) = |a|$.

(*ii*) We will prove that $\mathbb{Z}[i]$ is a Euclidean domain with the Euclidean function N defined by $N(a + bi) = a^2 + b^2$.