Math 104a: Number theory – Problem set 4

François Thilmany

due Friday 27 July 2018

Problem 1. Let R be a ring and $a, b \in R$. Check that the set $aR = \{ar \mid r \in R\}$ is an ideal. Prove that $aR \subset bR$ if and only if b divides a. (Any ideal which is of the form aR for some $a \in R$ is called a *principal ideal*, and a is called its generator, so that aR is called the (principal) ideal generated by a.)

Problem 2. Let R be a ring and $p \in R$. Show that the ideal $pR = \{pr \mid r \in R\}$ of R is a prime ideal if and only if p is a prime element.

Problem 3. Let D be a Euclidean domain and I an arbitrary ideal of D. Prove that there exists $a \in D$ such that $I = aD$. (In other words, any ideal of a Euclidean domain is principal.) In particular, every ideal of the ring $\mathbb{Z}$ is of the form $m\mathbb{Z}$ for some $m \in \mathbb{N}$.

Hint: If s denotes the Euclidean function of D and $I \neq \{0\}$, consider $a \in I - \{0\}$ with $s(a)$ minimal.

Problem 4. Let $\xi = \sqrt{-5}$, and recall the subring $\mathbb{Z}[\xi] = \{a + b\xi \mid a, b \in \mathbb{Z}\}$ of $\mathbb{C}$ from homework 3 problem 1. Prove that:

(a) $I = \{2\alpha + (1+\xi)\beta \mid \alpha, \beta \in \mathbb{Z}[\xi]\}$ is an ideal of $\mathbb{Z}[\xi]$.
(b) $\phi : \mathbb{Z}[\xi] \to \mathbb{Z}/2\mathbb{Z} : a + b\xi \mapsto a + b + 2\mathbb{Z}$ is a homomorphism of rings.
(c) $I = \ker \phi$.
(d) I is a maximal ideal, hence is also a prime ideal.

However, we have seen in homework 3 that neither 2 nor $1 + \xi$ is prime in $\mathbb{Z}[\xi]$.

Problem 5. Solve (i.e. give all solutions $x \in \mathbb{Z}$ to) the following congruences

(a) $9x \equiv 1 \mod 200$
(b) $9x \equiv 17 \mod 200$
(c) $4x \equiv 3 \mod 15$
(d) $2x \equiv 23 \mod 128$
(e) $4x \equiv 12 \mod 128$

Problem 6. Find all $x \in \mathbb{Z}_{35}$ which are solutions to the equation $x^3 - 5x^2 + 6x = 0$.

Hint: Factor the equation and use the fact that $\mathbb{Z}_5$ and $\mathbb{Z}_7$ are fields.

Problem 7. Find all solutions $x \in \mathbb{Z}$ of the system of congruences

$$\begin{cases} 3x \equiv 9 \mod 12 \\ 4x \equiv 5 \mod 35 \\ 6x \equiv 18 \mod 21 \end{cases}$$

Problem 8. Find all solutions $x \in \mathbb{Z}$ of the system of congruences

$$\begin{cases} x^2 \equiv 9 \mod 16 \\ 3x \equiv 1 \mod 40 \\ 4x \equiv 8 \mod 25 \end{cases}$$

Hint: First study the possible solutions of $x^2 = 9$ in $\mathbb{Z}_{16}$.

Problem 9. Let $a, b, c, d \in \mathbb{Z}$. Find all the solutions $x \in \mathbb{Z}$ (in terms of a, b, c, d) of the system of congruences

$$\begin{cases} x \equiv a \mod 2 \\ x \equiv b \mod 3 \\ x \equiv c \mod 5 \\ x \equiv d \mod 7 \end{cases}$$

Problem 10. Fix $k \in \mathbb{N}$. Prove that there exists an integer m such that there are no prime numbers among $m, m+1, \ldots, m+k$. Deduce that there are actually infinitely many such m's.

Hint: Use the Chinese remainder theorem.

Problem 11. Let $m \in \mathbb{N}$ and assume $m \neq 0, 1$. Solve the equation $(x+1)^2 = x^2$ in the ring $\mathbb{Z}_m$ (that is, give all possible solutions $x \in \mathbb{Z}_m$). The answer might depend on m.

Problem 12. Prove that if m divides n, then $\varphi(m)$ divides $\varphi(n)$. (Here and below, φ denotes Euler's totient function.)

Problem 13. Show that $\varphi(n)$ is even for any integer $n > 2$.