ALGEBRA: HOMEWORK 1

Problem 1. *Prove that* $15x^2 - 7y^2 = 9$ *has no solutions in* $\mathbb{Z}$.

Sketch of proof: if there exist solutions in $\mathbb{Z}$, consider this equation in $\mathbb{Z}/5\mathbb{Z}$:

$$-7y^2 = 9 = 3^2 \pmod 5,$$

but $-7 = 3 \pmod 5$ is a QNR (quadratic nonresidue), contradiction.

Problem 2. *Prove that an integer of the form* $8n + 7$ *cannot be written as a sum of three integer squares.*

Sketch of proof: By enumeration we know that QRs in $\mathbb{Z}/8\mathbb{Z}$ are $\{0, 1, 4\}$, and then the sum of three integer squares in $\mathbb{Z}/8\mathbb{Z}$ is in $\{0, 1, 2, 3, 4, 5, 6\}$.

Problem 3. *Show that if* $x^2 = a \pmod p$ *is solvable then* $x^2 = a \pmod{p^n}$ *is also solvable, for all positive integers* n.

Sketch of proof: Clearly, this holds for $a = 0$ or $a = 1$. Now assume that p is odd $a \neq 0$. By induction, it suffices to prove that if $x^2 = a\ (p^n)$, then there exists x' of form $x' = x + lp^n$ such that $x'^2 = a\ (p^{n+1})$.

Assume $x^2 - a = kp^n$, and we need to solve $(x + lp^n)^2 = x'^2 = a = x^2 - kp^n\ (p^{n+1})$, i.e., $2xlp^n = kp^n\ (p^{n+1})$, i.e., $2xl = -k\ (p)$. Since $p \nmid 2$ and $p \nmid x$, then there exists l such that $2xl = -k\ (p)$.

Problem 4. *Show that* $(2, 3, 7)$ *is the only triple of integers* > 1 *such that*

$$c \mid (ab + 1), \quad b \mid (ac + 1), \text{ and } \quad a \mid (bc + 1).$$

Sketch of proof: It is easy to see that a, b, c are pairwise co-prime. We have

$$abc \mid (ab + 1)(bc + 1)(ca + 1).$$

Since

$$(ab + 1)(bc + 1)(ac + 1) = abc(abc + a + b + c) + ab + bc + ca + 1,$$

we have $abc \mid ab + bc + ca + 1$. and thus $abc \leq ab + bc + ca + 1$, i.e.,

$$\frac{1}{a} + \frac{1}{b} + \frac{1}{c} + \frac{1}{abc} \geq 1.$$

Without loss of generality, we may assume $a < b < c$ and enumerate the finite cases satisfying the above inequality. (Actually there are only 2 cases (2,3,5), (2,3,7) satisfying the inequality and pairwise co-prime condition.)

Problem 5. *Let* $f : \mathbb{N} \to \mathbb{C}$ *be given by*

$$\sum_{d \mid n} f(d) = \phi(n), \text{ (the Euler function)},$$

for all $n \in \mathbb{N}$. *Find all such* f.

Sketch of proof: Such f is uniquely defined by the inductive identity

$$f(n) = \phi(n) - \sum_{d|n, d\neq n} f(d).$$

Thus it exists and is unique. Now we compute this f. First

$$\begin{aligned} f(p^n) &= \sum_{d|p^n} f(d) - \sum_{d|p^{n-1}} f(d) = \phi(p^n) - \phi(p^{n-1}) \\ &= \begin{cases} 1 & n = 0 \\ (p-1) - 1 = p - 2 & n = 1 \\ p^{n-1}(p-1) - p^{n-2}(p-1) = p^{n-2}(p-1)^2 & n \geq 2 \end{cases}. \end{aligned}$$

Now for $n = p_1^{a_1}...p_k^{a_k}$, we claim that

$$f(n) = f(p_1^{a_1})...f(p_k^{a_k})$$

is a desired f.

For $n = p_1^{a_1}...p_k^{a_k}$, we have

$$\begin{aligned} \sum_{d|n} f(d) &= \sum_{d_1|p_1^{a_1}} ... \sum_{d_k|p_k^{a_k}} f(d_1...d_k) \\ &= \sum_{d_1|p_1^{a_1}} ... \sum_{d_k|p_k^{a_k}} f(d_1)...f(d_k) \\ &= \sum_{d_1|p_1^{a_1}} f(d_1) ... \sum_{d_k|p_k^{a_k}} f(d_k) \\ &= \phi(p_1^{a_1})...\phi(p_k^{a_k}) = \phi(n). \end{aligned}$$