2 Second assignment

1. Let p be a prime number.

   (a) Let $\alpha \in \mathbb{Z}_p^*$ and define $\alpha_n := \alpha^{p^n}$ for $n = 0, 1, 2, \ldots$. Prove that $\alpha_n \equiv \alpha_{n-1} (\text{mod } p^n)$ for $n = 1, 2, \ldots$. (Hint: first look at $\alpha \in \mathbb{Z}$, not divisible by p.)

   (b) Prove that α_n converges to a limit $\xi \in \mathbb{Z}_p$ and that $\xi^{p-1} = 1$.

   (c) Given $\alpha \in \mathbb{Z}_p^*$, prove that there is $\xi \in \mathbb{Z}_p$ with $\xi^{p-1} = 1$ such that $\alpha \equiv \xi (\text{mod } p)$. Prove that $X^{p-1} = 1$ has precisely $p - 1$ solutions in $\mathbb{Z}_p$.

   (d) Let $T = \{0, \xi_1 \ldots \xi_{p-1}\}$, where $\xi_1 \ldots \xi_{p-1}$ are the distinct solutions of $X^{p-1} = 1$ in $\mathbb{Z}_p$. Prove that every $\alpha \in \mathbb{Z}_p$ can be represented as an infinite series $\sum_{k=0}^{\infty} a_k p^k$ with $a_k \in S$ for $k = 0, 1, 2, \ldots$.

2. Let p be a prime number > 2.

   (a) Let $\alpha \in \mathbb{Z}_p^*$ and suppose there is $x_0 \in \mathbb{Z}$ with $x_0^2 \equiv \alpha (\text{mod } p)$. Define the sequence $\{x_n\}_{n=0}^{\infty}$ recursively by

   $$x_{n+1} := x_n - \frac{x_n^2 - \alpha}{2x_n} \quad \text{for } n \geq 0.$$

   Prove that $x_n^2 \equiv \alpha (\text{mod } p^{2^n})$ for $n \geq 0$ and that x_n converges to a limit $\xi \in \mathbb{Z}_p$ with $\xi^2 = \alpha$.

   (b) It is known that for any $x \in \mathbb{R}$, either x or $-x$ is a square of a real number. Determine numbers $\alpha_1, \alpha_2, \alpha_3, \alpha_4 \in \mathbb{Q}_3$ such that for any $\alpha \in \mathbb{Q}_3$, at least one of the numbers $\alpha_i \alpha$ $(i = 1, 2, 3, 4)$ is a square of a number of $\mathbb{Q}_3$. (Hint: Write $\alpha = u 3^m$, where $u \in \mathbb{Z}_3^*$ and $m \in \mathbb{Z}$).

3. Let a be a non-zero complex number and consider the sequence of powers

   $$A = \{a, a^2, a^3, \ldots, a^n, \ldots\}.$$

   (a) Show that every real straight line in the complex plane is given by an equation of the form $\alpha z + \overline{\alpha z} = b$ for suitable $\alpha \in \mathbb{C}$ and $b \in \mathbb{R}$.

   (b) Show that a straight line in $\mathbb{C}$, NOT passing through the origin, contains at most finitely many points of A.

   (c) Characterise those a for which there exists a straight line (possibly through the origin) which contains an infinite number of points of A.

   (d) Suppose that every straight real line (also the ones through the origin) in $\mathbb{C}$ contains at most finitely many points of A. Prove that every curve $P(x, y) = 0$ contains at most finitely many points of A. Here x, y denote the real coordinates in $\mathbb{C}$ and $P \in \mathbb{C}[x, y],\ P \not\equiv 0$.

4. We solve $x^3 - 2y^3 = 1$ in integers x, y by using Skolem's method. It is given that the ring of integers in $\mathbb{Q}(\sqrt[3]{2})$ is $\mathbb{Z}[\sqrt[3]{2}]$ and the unit group is generated by -1 and $u = -1 + \sqrt[3]{2}$.

   (a) Choose a prime p and determine the smallest positive integer e such that $u^e \equiv 1 (\text{mod } p)$.

   (b) Apply Skolem's method with p as in the previous subproblem.