2 Second assignment with solutions

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.)

   Solution. Let $a \in \mathbb{Z}$, not divisible by p. Then, by Euler's theorem $a^{\phi(p^n)} \equiv a^{p^n - p^{n-1}} \equiv 1 (\text{mod } p^n)$. Hence, $a^{p^n} \equiv a^{p^{n-1}} (\text{mod } p^n)$. Letting $\alpha \in \mathbb{Z}_p^*$, choose an integer a such that $\alpha \equiv a (\text{mod } p^n)$. Then,

   $$\alpha^{p^n} \equiv a^{p^n} \equiv a^{p^{n-1}} \equiv \alpha^{p^{n-1}} (\text{mod } p^n).$$

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

   Solution. For any positive integers n we have $\alpha^{p^n} \equiv \alpha^{p^{n-1}} (\text{mod } p^n)$. Hence $\lim_{n\to\infty} |\alpha^{p^n} - \alpha^{p^{n-1}}|_p = 0$. So the sequence with terms α^{p^n} is a Cauchy sequence in $\mathbb{Z}_p$ (Corollary 2.4 of the notes on p-adic numbers) and therefore convergent. Denote its limit by $\xi = \lim_{n\to\infty} \alpha^{p^n}$. Also,

   $$\xi^p = \lim_{n\to\infty} (\alpha^{p^n})^p = \lim_{n\to\infty} \alpha^{p^{n+1}} = \xi.$$

   Since $|\alpha|_p = 1$ we also have $|\xi|_p = 1$. So it follows from $\xi^p = \xi$ 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 $\mathbb{Z}_p$.

   Solution. From the previous exercise it is clear that $\xi \equiv \alpha (\text{mod } p)$. Hence by taking $\alpha = 1, 2, \ldots, p-1$ we get $p - 1$ distinct solutions of $X^{p-1} = 1$ 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 $a_k \in T$ for $k = 0, 1, 2, \ldots$.

   Solution. Carry out the following algorithm. Define $\alpha_0 = \alpha$. Then, for $k = 0, 1, 2, \ldots$ carry out the following steps.

   i. Determine $a_k \in T$ such that $\alpha_k - a_k \equiv 0 (\text{mod } p)$.

   ii. Define $\alpha_{k+1} = (\alpha_k - a_k)/p$.

   Then, by induction on k we can show that $\alpha \equiv a_0 + a_1 p + \cdots + a_k p^k (\text{mod } p^{k+1})$. Taking the limit $k \to \infty$ gives the desired result.

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

Solution. Note that we might as well take

$$x_{n+1} = \frac{1}{2}\left(x_n + \frac{\alpha}{x_n}\right).$$

By induction we easily see that $x_n \equiv x_0 (\mathrm{mod}\ p)$ for all $n \geq 0$. Since x_0 is a p-adic unit, so are the other x_n. For every $n = 0, 1, 2, \ldots$ we have

$$x_{n+1}^2 - \alpha = \frac{1}{4}(x_n^2 + 2\alpha^2/x_n^2 + \alpha^2) - \alpha^2 = \frac{1}{4}(x_n - \alpha/x_n)^2.$$

For the p-adic valuations this implies

$$|x_{n+1}^2 - \alpha|_p = |x_n - \alpha/x_n|^2 = |x_n^2 - \alpha|^2,$$

because $|2|_p = |x_n|_p = 1$. By induction we obtain $|x_n^2 - \alpha|_p = |x_0^2 - \alpha|_p^{2^n}$, which proves our first assertion because $|x_0^2 - \alpha|_p \leq 1/p$.

For all positive integers n we have $x_{n+1}^2 \equiv x_n^2 (\mathrm{mod}\ p^{2^n})$. Hence

$$0 \equiv x_{n+1}^2 - x_n^2 \equiv (x_{n+1} - x_n)(x_{n+1} + x_n) (\mathrm{mod}\ p^{2^n}).$$

Note that $x_{n+1} + x_n \equiv 2x_0 \neq 0 (\mathrm{mod}\ p)$. Hence we get $|x_{n+1} - x_n|_p \leq p^{2^n}$. So, by Corollary 2.4, x_n is a Cauchy sequence with a limit ξ. Since $\lim_{n\to\infty} x_n^2 = \alpha$ we conclude that $\xi^2 = \alpha$.

(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 $\alpha = u3^m$, where $u \in \mathbb{Z}_3^*$ and $m \in \mathbb{Z}$).

Solution. For the numbers α_i we can take

$$\alpha_1 = 1,\ \alpha_2 = -1,\ \alpha_3 = 3,\ \alpha_4 = -3.$$

Write $\alpha = u3^m$ as in the hint. If m is even and $u \equiv 1 (\mathrm{mod}\ 3)$ we see that α/α_1 is a square. If m is even and $u \equiv -1 (\mathrm{mod}\ 3)$ the quotient α/α_2 is a square. If m is odd and $u \equiv 1 (\mathrm{mod}\ 3)$ the quotient α/α_3 is a square. If m is odd and $u \equiv -1 (\mathrm{mod}\ 3)$ the quotient α/α_4 is a square.

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 $b \in \mathbb{R}$.

Solution. Suppose the line is given by the equation $ax + cy = b$. We change to the new coordinates $z, \overline{z}$ by letting $x = (z + \overline{z})/2, y = (z - \overline{z})/2i$. We obtain $(a - ci)z + (a + ci)\overline{z} = 2b$.

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

Solution. Let the straight line be given by $\alpha z + \overline{\alpha z} = 1$ (after normalizing the constant term). A point a^n lies on this line if $\alpha a^n + \overline{\alpha} \overline{a}^n = 1$. By the Skolem-Lech-Mahler theorem this equation in $n \in \mathbb{Z}$ has at most finitely many solutions, unless one of the ratios $a/1, a/\overline{a}$ is a root of unity. If a is a root of unity, the set A is finite, so we are done. The quotient $a/\overline{a}$ is a root of unity if and only if the argument of a is a rational multiple of 2π. Rewrite the equation as $a^n(1 + \overline{a}^n/a^n) = 1$. Since $1 + \overline{a}^n/a^n$ assumes finitely many distinct values there exist numbers $c_1, c_2 > 0$ such $c_1 < |a|^n < c_2$ for every solution n. If $|a| \neq 1$ there are at most finitely many solutions. If $|a| = 1$ the number a is a root of unity again.

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

Solution. From the previous exercise it follows that this happens if the argument of a is a rational multiple of 2π, $|a| \neq 1$ and the lines pass through the origin with arguments which are integer multiples of the argument 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. Suppose also that $|a| \neq 1$. 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 $P \in \mathbb{C}[x, y],\ P \not\equiv 0$.

Solution. Rewrite the polynomial equation $P(x, y) = 0$ as a polynomial equation $Q(z, \overline{z}) = 0$. The point a^n lies on this curve if $Q(a^n, \overline{a}^n) = 0$. Suppose that $Q = \sum_{i,j} q_{ij} z^i \overline{z}^j$. Then the equation reads

$$\sum_{i,j} q_{i,j} (a^i \overline{a}^j)^n = 0.$$

According to the Skolem-Lech-Mahler theorem the existence of infinitely many solutions n implies that there exist i, j and k, l such that $q_{ij}, q_{kl} \neq 0$ and $a^{i-k}/\overline{a}^{j-l}$ is a root of unity. In particular the absolute value must be 1. Hence $|a|^{i-k-(j-l)} = 1$. Hence either $|a| = 1$, which we excluded, or $i - k - (j - l) = 0$. The latter implies that $a/\overline{a}$ is a root of unity. But in that case the points a^n lie on a finite number of lines through the origin.

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 $u^e \equiv 1 (\text{mod } p)$.

Solution. We mention two possibilities. When $p = 3$ we have $(-1 + \sqrt[3]{2})^3 = 1 + 3(\sqrt[3]{2} - \sqrt[3]{2^2})$. When $p = 5$, then $(-1 + \sqrt[3]{2})^8 = 1 + 5(20\sqrt[3]{2} - 16\sqrt[3]{2^2})$.

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

Solution. The equation $x^3-2y^3=1$ implies that $x-y\sqrt[3]{2}$ is a unit in $\mathbb{Z}[\sqrt[3]{2}]$. Hence there exists $n\in\mathbb{Z}$ such that

$$x-y\sqrt[3]{2}=\pm(-1+\sqrt[3]{2})^n.$$

Note that this means that the coefficient of $(-1+\sqrt[3]{2})^n$ is zero. Letting ω be a primitive root of unity, the conjugates of $\sqrt[3]{2}$ are given by $\omega\sqrt[3]{2}$ and $\omega^2\sqrt[3]{2}$. The coefficient of $(-1+\sqrt[3]{2})^n$ is given by $1/6$ times

$$w_n=\sqrt[3]{2}(-1+\sqrt[3]{2})^n+\omega\sqrt[3]{2}(-1+\omega\sqrt[3]{2})^n+\omega^2\sqrt[3]{2}(-1+\omega^2\sqrt[3]{2})^n,$$

which is the trace of $\sqrt[3]{2}(-1+\sqrt[3]{2})^n$. This follows from

$$\sqrt[3]{2}(a+b\sqrt[3]{2}+c\sqrt[3]{2}^2)+\omega\sqrt[3]{2}(a+b\omega\sqrt[3]{2}+c\omega^2\sqrt[3]{2}^2)+\omega^2\sqrt[3]{2}^2(a+b\omega^2\sqrt[3]{2}+\omega\sqrt[3]{2}^2)=6c.$$

We solve $w_n=0$ with Skolem's method using $p=5$. Then $w_n(\text{mod } 5)$ is periodic in n with period 8. We compute that modulo 5,

$$w_0\equiv 0,\ w_1\equiv 0,\ w_2\equiv 1,\ w_3\equiv 2,\ w_4\equiv 1,\ w_5\equiv 2,\ w_6\equiv 3,\ w_7\equiv 1.$$

Hence $w_n=0$ implies that $n\equiv 0,1(\text{mod } 8)$.

Let us consider the subproblem $w_{8n}=0$. We know $w_0=0$ and compute that w_8 is not divisible by 25. Hence Proposition 3.2.1 with $\theta_1=\sqrt[3]{2},\alpha_1=(-1+\sqrt[3]{2}),p=5,m=8$ implies that $n=0$ is the only solution.

Let us consider the subproblem $w_{8n+1}=0$. We know $w_1=0$ and compute that w_9 is not divisible by 25. Proposition 3.2.1 with $\theta_1=\sqrt[3]{2}(-1+\sqrt[3]{2}),\alpha_1=(-1+\sqrt[3]{2}),p=5,m=8$ implies that $n=0$ is the only solution.

Putting the two subproblems together implies that $n=0,1$ are the only integer solutions to $w_n=0$. Hence $x-y\sqrt[3]{2}=\pm(-1+\sqrt[3]{2})^0=\pm 1$ or $x-y\sqrt[3]{2}=\pm(-1+\sqrt[3]{2})^1=\pm(-1+\sqrt[3]{2})$. We deduce that the only solutions are $x=1,y=0$ and $x=-1,y=-1$.