Problems Set #1

1. Suppose that $\mathbf{z} \in \mathbb{C}^2$, that A is an invertible 2×2 matrix with coefficients in $\mathbb{C}$, and that V is a line through the origin (i.e., a linear subspace). Show that one of the two following holds:

(a) There is at most one n such that $A^n \mathbf{z} \in V$; or

(b) There is an entire coset $i + m\mathbb{Z}$ of $\mathbb{Z}$ such that $A^n \mathbf{z} \in V$ for all n in this coset.

This can be proved using simple linear algebra and group theory. [Hint: Show that if $\mathbf{z} \neq 0$ and two iterates of $\mathbf{z}$ are in V, then $A^m V = V$ for some $m \neq 0$.]

2. Show that $|a+b|_p \leq \max(|a|_p, |b|_p)$ for any $a, b \in \mathbb{Q}_p$.

3. Let $f(t) = \sum_{n=0}^{\infty} a_n t^n$, where $a_n \in \mathbb{Q}_p$ for $n \in \mathbb{N}$. Suppose that $\lim_{n\to\infty} |a_n|_p = 0$.

(a) Show that $f(t)$ converges uniformly on the closed unit disc of radius 1 in $\mathbb{Q}_p$.

(b) Show that if $|a_i|_p < |a_0|_p$ for all $i > 0$, then for all z in the disc of radius 1 in $\mathbb{Q}_p$, we have $f(z) \neq 0$.

(c) Show that if $|a_i|_p < |a_n|_p$ for all $i > n$, then f has at most n zeroes on the closed unit disc of radius 1 in $\mathbb{Q}_p$. [Hint: Use induction plus (b)]

(d) Show that f has at most finitely many zeroes on the closed unit disc of radius 1 in $\mathbb{Q}_p$.

4. The sequence $\{a_n\}_{n\geq 1}$ is defined by

$$a_1 = 20;\ a_2 = 30 \text{ and } a_{n+2} = 3a_{n+1} - a_n$$

for every integer $n \geq 1$. Find all positive integers n for which $1 + 5a_n a_{n+1}$ is a perfect square.

5. Let p be any prime. Give an explicit example (e.g., in terms of an explicit Cauchy sequence or other concrete construction) of a transcendental element of $\mathbb{Q}_p$. (Recall that an element z in a field extension of $\mathbb{Q}$ is said to be transcendental if it is not a root of any nonconstant polynomial with coefficients in $\mathbb{Q}$.)

Problems Set #2

1. Let $S = \{\frac{2}{39}, \pi^2, \alpha\}$ where $\alpha^2 + \alpha + 1 = 0$. For which p is there an embedding $j : \mathbb{Q}(S) \longrightarrow \mathbb{Q}_p$ such that $j(S) \subset \mathbb{Z}_p$?

2. Let $p \geq 5$ be a prime number. Find the largest length of an arithmetic progression of positive integers whose terms do not contain the digit 1 in their p-adic expansion.

3. Let a be an integer larger than 1. For each $n \in \mathbb{N}$, let $x_n = (a+1) \cdot a^n - 1$. Prove that there exist infinitely many numbers in the above sequence which are pairwise coprime.

4. An infinite arithmetic progression whose terms are integers contains a perfect square and a perfect cube. Show that the arithmetic progression also contains the sixth power of an integer.

5. We define the sequence $\{a_n\}_{n \in \mathbb{N}}$ by $a_1 = 3$, $a_2 = 2$ and for each $n \geq 2$ we have

$$a_{n-1}a_{n+1} = a_n^2 + 5.$$

Prove that $a_n \in \mathbb{N}$ for each $n \in \mathbb{N}$. [Hint: Show that a_n is a linear recurrence sequence.]

Problems Set #3

1. The Chebotarev density theorem says the following. Let $f(x) \in \mathbb{Q}[x]$ be a polynomial of positive degree. Let T be the roots of f in $\overline{\mathbb{Q}}$ and let G be the Galois group of the splitting field of f. (Then G acts on T in the usual way.) Then the proportion of primes such that $f(x)$ has a root modulo p is equal to the proportion of elements of G that fix an element of T. For each of the following polynomials f, calculate the proportion of p such that f has a root modulo p.
   (1) $f(x) = x^2 + 1$.
   (2) $f(x) = x^3 - 5$.
   (3) $f(x) = x^3 + x^2 + x + 1$.
   (4) $f(x) = x^4 - 7$.

2. Let S_n be the automorphism group of the set $\{1, \ldots, n\}$ (as usual). Let $i, j \in \{1, \ldots, n\}$ with $i \neq j$. For what proportion of $\sigma \in S_n$ is there some r such that $\sigma^r(i) = j$? (Equivalently, for what what proportion of $\sigma \in S_n$ are i and j in the same cycle when σ is decomposed into disjoint cycles)? [Hint: Start by working a few examples. If you figure out the answer and can't prove it, we'll give hints on a proof on Monday.]]

3. Let a be an integer larger than 1. For each $n \in \mathbb{N}$, let $x_n = (a+1) \cdot a^n - 1$. Prove that there exist infinitely many numbers in the above sequence which are pairwise coprime.

4. An infinite arithmetic progression whose terms are integers contains a perfect square and a perfect cube. Show that the arithmetic progression also contains the sixth power of an integer.

5. We define the sequence $\{a_n\}_{n \in \mathbb{N}}$ by $a_1 = 3$, $a_2 = 2$ and for each $n \geq 2$ we have

$$a_{n-1}a_{n+1} = a_n^2 + 5.$$

Prove that $a_n \in \mathbb{N}$ for each $n \in \mathbb{N}$. [Hint: Show that a_n is a linear recurrence sequence.]

Problems Set #4

Problem 1. Solve in $\mathbb{Z}$ the equation

$$x^4 - 4x^2y + 5y^2 + z^2 - yz = 0.$$

Problem 2. Solve in $\mathbb{Z}$ the equation

$$x^4 + 5y^4 - 7z^4 = 0.$$

Problem 3. Solve in $\mathbb{Z}$ the equation

$$x^2 - y^3 = 23.$$

Problem 4. Find all rational points on the curve given by the equation:

$$x^4 - 3x^2y^2 + 3y^4 - 2y + 2 = 0.$$

Problem 5. Find all rational points on the curve

$$x^2 - 3y^2 = 2.$$

Problem 6. Find all integers m and n such that

$$3^m - 2^n = 1.$$

Problems Set #5

Problem 1. Let S be the group of automorphisms of the affine plane generated by

$$\Phi : \mathbb{C}^2 \longrightarrow \mathbb{C}^2 \text{ given by } \Phi(x, y) = (2x, y)$$

and

$$\Psi : \mathbb{C}^2 \longrightarrow \mathbb{C}^2 \text{ given by } \Psi(x, y) = (x, 3y).$$

Find all $f \in S$ such that $f(1, 1)$ lies on the line given by the equation $x + 1 = y$.

Problem 2. Let S be the semigroup of transformations of the affine space generated by

$$\Phi_1 : \mathbb{C}^3 \longrightarrow \mathbb{C}^3 \text{ given by } \Phi_1(x, y, z) = (x + 1, y, z);$$
$$\Phi_2 : \mathbb{C}^3 \longrightarrow \mathbb{C}^3 \text{ given by } \Phi_2(x, y, z) = (x, y + 1, z)$$

and

$$\Phi_3 : \mathbb{C}^3 \longrightarrow \mathbb{C}^3 \text{ given by } \Phi_3(x, y, z) = (x, y, 3z).$$

Find all $f \in S$ such that $f(0, 0, 1)$ lies on the surface given by the equation $x^2 + y^4 = z$.

Problem 3. A special case of the Dynamical Mordell-Lang conjecture is for the action of one-variable polynomials on each coordinate of $\mathbb{A}^N$ (for any integer $N \geq 2$). In other words, one has N polynomials $f_1, \ldots, f_N \in \mathbb{C}[z]$ and $\Phi : \mathbb{A}^N \longrightarrow \mathbb{A}^N$ be given by

$$\Phi(x_1, \ldots, x_N) = (f_1(x_1), \ldots, f_N(x_N)).$$

Then the Dynamical Mordell-Lang Conjecture predicts that for each $\alpha \in \mathbb{A}^N(\mathbb{C})$, and for each irreducible subvariety $V \subset \mathbb{A}^N$, if $V(\mathbb{C}) \cap \mathrm{Orb}_\Phi(\alpha)$ is Zariski dense in V, then V is periodic.

Prove that if one knows that the Dynamical Mordell-Lang Conjecture holds for $N = 2$ and for curves contained in $\mathbb{A}^2$, then the Dynamical Mordell-Lang Conjecture holds for all curves contained in $\mathbb{A}^N$ for arbitrary integer $N \geq 2$.

Problem 4. Find the third coefficient of the 2-adic uniformizing power series for the 2-adic analytic function

$$f(z) = \sum_{n=1}^{\infty} \frac{4^n}{n+2} \cdot z^n$$

with respect to the fixed point $z = 0$. In other words, for the power series

$$u(z) = z + c_2 z^2 + c_3 z^3 + c_4 z^4 + \cdots + c_n z^n + \cdots$$

satisfying the identity

$$f(u(z)) = u\left(\frac{4}{3} \cdot z\right),$$

find c_3.

Problem 5. The Chebotarev density theorem says the following. Let $f(x) \in \mathbb{Q}[x]$ be a polynomial of positive degree. Let T be the roots of f in $\overline{\mathbb{Q}}$ and let G be the Galois group of the splitting field of f. (Then G acts on T in the usual way.) Then the proportion of primes such that $f(x)$ has a root modulo p is equal to the proportion of elements of G that fix an element of T. For each of the following polynomials f, calculate the proportion of p such that f has a root modulo p.

(1) $f(x) = x^2 + 1$.
(2) $f(x) = x^3 - 5$.

(3) $f(x) = x^3 + x^2 + x + 1$.
(4) $f(x) = x^4 + x^3 + x^2 + x + 1$.
(5) $f(x) = x^4 - 7$.

Problem 6. Let S_n be the automorphism group of the set $\{1, \ldots, n\}$ (as usual). Let $i, j \in \{1, \ldots, n\}$ with $i \neq j$. For what proportion of $\sigma \in S_n$ is there some r such that $\sigma^r(i) = j$? (Equivalently, for what what proportion of $\sigma \in S_n$ are i and j in the same cycle when σ is decomposed into disjoint cycles)? [Hint: Start by working a few examples. If you figure out the answer and can't prove it, we'll give hints on a proof on Monday.]

Problems Set #6

Problem 1. For each nonzero complex number c, find all points (x, y) on the curve

$$x + y = c$$

such that both x and y are roots of unity.

Problem 2. Find all points (x, y) on the curve

$$y^2 - x^3 - x = 0$$

such that both x and y are roots of unity.

Problem 3. Prove directly that there exist at most finitely many points (x, y) with both x and y roots of unity on the curve

$$y^2 - xy + x^2 - x + y = 0.$$

Find all such points on the above curve, or find an explicit upper bound for the number of such points.

Problem 4. Let $f \in \mathbb{C}[z]$ be a polynomial of degree $d \geq 1$. We denote by $\mathrm{Prep}(f)$ the set of all preperiodic points for $f(z)$, i.e., the set of all $c \in \mathbb{C}$ such that the orbit of c under f is finite. Prove that $f(z) = \zeta z^d$, where ζ is a root of unity if and only if $\mathrm{Prep}(f)$ is the set $\{0\} \cup \mu_\infty$, where μ_∞ is the set of all complex roots of unity.

Problems Set #7

Problem 1. Show that for any $\alpha, \beta \in \overline{\mathbb{Q}}$, we have

$$h(\alpha\beta) \leq h(\alpha) + h(\beta).$$

Problem 2. Show that for any $\alpha, \beta \in \overline{\mathbb{Q}}$, we have

$$h(\alpha + \beta) \leq h(\alpha) + h(\beta) + \log 2.$$

Problem 3. Let α be a root of a *monic polynomial* $f(x) \in \mathbb{Z}[x]$ of degree $d \geq 1$. That is $f(x) = x^d + a_{d-1}x^{d-1} + \ldots a_0$ with $a_i \in \mathbb{Z}$ for all i, and $f(\alpha) = 0$. Show that any for embedding $\sigma : \mathbb{Q}(\alpha) \hookrightarrow \overline{\mathbb{Q}}_p$, we have $|\sigma(\alpha)|_p \leq 1$.

In all of the following problems, let $f_n(x) = (x^n - 1)(x - 2) + 3$ for $n \geq 3$.

Problem 4. Show that f_n is irreducible. [Hint: There are various ways to do this, one is to take advantage of the fact that the constant term is a prime, which restricts possible factorizations a bit.]

Problem 5. Show that if $f_n(\alpha) = 0$ for $\alpha \in \mathbb{C}$, then $|\alpha| \geq 1$.

Problem 6. Show that if $f_n(\alpha_n) = 0$, then $h(\alpha_n) = \frac{\log 5}{n+1}$. Conclude that if $(\alpha_n)_{n=1}^{\infty}$ is a sequence of algebraic numbers such that $f_n(\alpha_n) = 0$ for each n, then $\lim_{n\to\infty} h(\alpha_n) = 0$.

Problem 7. With $(\alpha_n)_{n=1}^{\infty}$ as in 6. and $g(z) = \log(z - 2)$, show that

$$\lim_{n\to\infty} \frac{1}{\deg \alpha_n} \sum_{\text{conjugates } \alpha_n^\sigma \text{ of } \alpha} g(\alpha_n^\sigma) = 0.$$

[Hint: One easy way is to note that, up to sign, evaluating a monic polynomial P at the roots of a monic polynomial Q is the same as evaluating Q at the roots of P.]

Problem 8. Let $g(z) = \log(z - 2)$. Show that $\int_0^1 g(e^{2\pi i z})\, dz \neq 0$. (You can calculate explicitly with complex analysis if you want, but that is not necessary.)

Problem 9. Conclude that with $(\alpha_n)_{n=1}^{\infty}$ as in 6. and $g(z) = \log(z - 2)$, we have

$$\lim_{n\to\infty} \frac{1}{\deg \alpha_n} \sum_{\text{conjugates } \alpha_n^\sigma \text{ of } \alpha} g(\alpha_n^\sigma) \neq \int_0^1 g(e^{2\pi i z})\, dz$$