DIOPHANTINE APPROXIMATION
HOMEWORK I

Due October 18

Total number of points: 60. Grade: number of points/6

---

5 **1.** Let a be an integer with $a \geqslant 3$ and put

$$\xi := \sum_{n=1}^{\infty} 10^{-a^{2n}}.$$

Prove that there are infinitely many pairs $(x, y) \in \mathbb{Z}^2$ with

$$\left| \xi - \frac{x}{y} \right| \leqslant y^{-a}, \quad y > 0, \ \gcd(x, y) = 1.$$

2. Complete the following irrationality proof for π (attributed to Cartwright, 1945).
Assume that $\pi = \frac{a}{b}$ with $a, b \in \mathbb{Z}_{>0}$, $\gcd(a, b) = 1$.

3 *a)* Define

$$I_n := \int_{-1}^{1} (1 - x^2)^n \cos(\tfrac{1}{2}\pi x) dx \quad \text{for } n = 0, 1, 2, \dots .$$

Prove that

$$I_0 = \tfrac{4}{\pi}, \ \ I_1 = \tfrac{32}{\pi^3}, \quad I_n = \tfrac{8n}{\pi^2}\Big((2n-1) I_{n-1} - (2n-2) I_{n-2} \Big) \ \text{for } n \geqslant 2.$$

3 *b)* Prove that $\frac{a^{2n+1}}{n!} \cdot I_n \in \mathbb{Z}$ for $n \geqslant 0$.

4 *c)* Prove that $0 < \frac{a^{2n+1}}{n!} \cdot I_n < 1$ for n sufficiently large, and deduce a contradiction.

3. Let C be a central symmetric convex body in $\mathbb{R}^n$. For $\mathbf{x} \in \mathbb{R}^n$, define $\|\mathbf{x}\|_C := \min\{\lambda \in \mathbb{R}_{\geqslant 0} : \mathbf{x} \in \lambda C\}$.

5 *a)* Prove that $\|\cdot\|_C$ defines a norm on $\mathbb{R}^n$.

5 *b)* Prove that for $\lambda \geqslant 0$ we have $\lambda C = \{\mathbf{x} \in \mathbb{R}^n : \|\mathbf{x}\|_C \leqslant \lambda\}$.

5 **4.** The symmetric convex hull of a subset S of $\mathbb{R}^n$ is defined to be the intersection of all convex sets, symmetric about $\mathbf{0}$, that contain S. The symmetric convex hull of S is itself a convex set, symmetric about $\mathbf{0}$.

Prove that if $\mathbf{v}_1, \dots, \mathbf{v}_r$ are points in $\mathbb{R}^n$, then the symmetric convex hull of $\mathbf{v}_1, \dots, \mathbf{v}_r$ is given by

$$\left\{ \sum_{i=1}^{r} x_i \mathbf{v}_i : x_1, \dots, x_r \in \mathbb{R}, \sum_{i=1}^{r} |x_i| \leqslant 1 \right\}.$$

5. Let p be a prime number with $p \equiv 1 \pmod 4$.

2 *a)* Prove that there is an integer x_0 with $x_0^2 \equiv -1 \pmod p$.
Hint. You may use that the group $(\mathbb{Z}/p\mathbb{Z})^*$ is cyclic. Prove that it has an element of order 4.

1 *b)* Let L be the lattice $\{(x, y) \in \mathbb{Z}^2 : x \equiv x_0 y \pmod p\}$. Prove that $x^2 + y^2 \equiv 0 \pmod p$ for $(x, y) \in L$.

7 *c)* Apply Minkowski's theorem with $C = \{(x, y) \in \mathbb{R}^2 : x^2 + y^2 \leqslant A\}$ for appropriate A and the lattice L from b) and deduce that there is $(x, y) \in \mathbb{Z}^2$ with $x^2 + y^2 = p$.

5 **6.** *a)* Let $l_i = \xi_{i1} X_1 + \dots + \xi_{im} X_m$ $(i = 1, \dots, n)$ be linear forms with real coefficients, satisfying

$$\{\mathbf{x} = (x_1, \dots, x_m) \in \mathbb{Z}^m : l_i(\mathbf{x}) \in \mathbb{Z} \text{ for } i = 1, \dots, n\} = \{\mathbf{0}\}.$$

Prove that there are infinitely many tuples $(\mathbf{x}, \mathbf{y}) = (x_1, \dots, x_m, y_1, \dots, y_n) \in \mathbb{Z}^{m+n}$ with

$$|l_i(\mathbf{x}) - y_i| \leqslant \Big(\max_{1 \leqslant i \leqslant m} |x_i| \Big)^{-m/n} \text{ for } i = 1, \dots, n, \ \mathbf{x} \neq \mathbf{0}.$$

5 *b)* (Dirichlet's theorem for Gaussian numbers). Let ζ be a complex number not belonging to the field $\mathbb{Q}(i) = \{x+iy : x, y \in \mathbb{Q}\}$. Prove that there are infinitely many pairs $(z, w) \in \mathbb{Z}[i] \times \mathbb{Z}[i]$ (where $\mathbb{Z}[i] = \{x + iy : x, y \in \mathbb{Z}\}$) such that

$$|z - \zeta w| \leqslant \frac{4}{\pi}|w|^{-1},\ w \neq 0.$$

Hint. Prove that for every integer $Q \geqslant 2$ there are $z, w \in \mathbb{Z}[i]$ with

$$|z - \zeta w| \leqslant \tfrac{4}{\pi}Q^{-1}, \quad |w| \leqslant Q, \quad w \neq 0.$$

To this end, consider the lattice in $\mathbb{R}^4$,

$$\big\{(\mathrm{Re}\,(z - \zeta w), \mathrm{Im}\,(z - \zeta w), \mathrm{Re}\,w, \mathrm{Im}\,w) : \ z, w \in \mathbb{Z}[i]\big\}$$

and apply Minkowski's first convex body theorem.

7. Let C be a symmetric convex body in $\mathbb{R}^n$, and L a lattice in $\mathbb{R}^n$. Denote by $\lambda_1, \ldots, \lambda_n$ the successive minima of C with respect to L. Then there are linearly independent vectors $\mathbf{v}_1, \ldots, \mathbf{v}_n \in L$ such that $\mathbf{v}_i \in \lambda_i C$ for $i = 1, \ldots, n$.

5 *a)* Let M be the lattice with basis $\mathbf{v}_1, \ldots, \mathbf{v}_n$. Prove that $[L : M] \leqslant n!$.

5 *b)* Assume that $n = 2$. Prove that L has a basis $\{\mathbf{w}_1, \mathbf{w}_2\}$ with $\mathbf{w}_1 \in \lambda_1 C$, $\mathbf{w}_2 \in \lambda_2 C$.
Hint. Let $\mathbf{v}$, $\mathbf{v}_2$ be vectors in L with $\mathbf{v}_i \in \lambda_i C$ for $i = 1, 2$ and M the lattice with basis $\mathbf{v}_1$, $\mathbf{v}_2$. Then by a), $[L : M] = 1$ or $[L : M] = 2$. Assume that $[L : M] = 2$. Take $\mathbf{w}_1 = \mathbf{v}_1$. Replace $\mathbf{v}_2$ by another vector $\mathbf{w}_2 \in L$.