# Algebra and Computation

## Problem Set 2

*Due date: April 21$^{st}$, 2017*

---

## Instructions

1. You are strongly encouraged to try out the questions by yourself. But you can collaborate with other classmates; if you do, please mention who you collaborated with.
2. Solutions are expected as a LaTeX document. You may use this very file by obtaining the source files from megh.
3. The deadline is **21st April 2017 (Friday), 2359 hrs**. For each day of delay you lose **7 points** of your total score in this assignment. So if you plan to delay, be smart about it.
4. The total score in this problem set is **65 points**.

---

## Questions

**Question 1.** *Let $\mathbb{F}$ be a field of size at least $n+1$. You are given as input distinct elements $\alpha_0, \alpha_1, \ldots, \alpha_n \in \mathbb{F}$ and elements (not necessarily distinct) $\beta_0, \beta_1, \ldots, \beta_n \in \mathbb{F}$. Find the unique univariate polynomial $f(x) \in \mathbb{F}[x]$ of degree at most $n$ that satisfies $f(\alpha_i) = \beta_i$ for all $i = 0, \ldots, n$, in nearly linear time (i.e. $O(n \operatorname{poly}\log n)$ time.)* **(10 points)**

**Question 2.** *Say we are given polynomials $f(x,y), g(x,y) \in \mathbb{F}_q[x,y]$ and assume that $q \gg (\deg f)(\deg g)$ and $f(x,y), g(x,y)$ are monic with respect to $x$. Make the following sketch a formal algorithm for bivariate GCD computation.*

> *For elements $\{a_1, a_2, \ldots, a_r\}$ from $\mathbb{F}_q$ and compute the gcd of the partial evaluations — $h_{a_i}(x) = \gcd(f(x,a_i), g(x,a_i))$. Find a polynomial $h(x,y)$ of the right degree such that $h(x,a_i) = h_{a_i}(x)$ for all $i \in \{1, \ldots, r\}$ and show that this must indeed be $\gcd(f,g)$.*

*This $r$ must be decided by you.*

**(15 points)**

**Question 3.** *Show that any lattice in $\mathbb{Z}^n$ of rank $r$ has a generating set of at most $r$ vectors.*

*That is, if say $\mathbf{b}_1, \ldots, \mathbf{b}_m \in \mathbb{Z}^n$ such that $\operatorname{rank}_{\mathbb{Q}}(B) = r$, where $B$ is the matrix consisting of the $\mathbf{b}_i$s are rows. Show that there you can find vectors $\mathbf{b}'_1, \ldots, \mathbf{b}'_r \in \mathbb{Z}^n$ such that*

$$\langle \mathbf{b}_1, \ldots, \mathbf{b}_m \rangle_{\mathbb{Z}} = \left\langle \mathbf{b}'_1, \ldots, \mathbf{b}'_r \right\rangle_{\mathbb{Z}}.$$ **(10 points)**

**Question 4.** *Assume the following theorem of Minkowski*

> **Theorem** (Minkowski's theorem)**.** *Suppose $\mathcal{L}$ is a full-rank lattice in $\mathbb{Z}^n$ and let $K$ be a symmetric, convex object such that $\operatorname{vol}(K/2) > \det(\mathcal{L})$ (where by $\det \mathcal{L}$ we mean the matrix with the generating set of the basis listed down as rows). Then, $K$ contains a non-zero lattice point of $\mathcal{L}$.*

*Using the above theorem (or not):*

1. *Show that if $\mathcal{L}$ is a full-rank lattice in $\mathbb{Z}^n$, then the shortest non-zero vector in $\mathcal{L}$ has norm at most $\sqrt{n}\,|\det \mathcal{L}|^{1/n}$.* **(5 points)**

2. *Let $p(x) = x^3 + ax^2 + bx + c \in \mathbb{Z}[x]$ be a given cubic polynomial. For a fixed integer $N > 0$, let $\mathcal{L} := \left\langle N, Nx, Nx^2, p(x), xp(x), x^2p(x) \right\rangle_{\mathbb{Z}} \subseteq \mathbb{Z}^6$ (each element here is a polynomial of degree at most 5; think of that as a vector in $\mathbb{Z}^6$ by listing its coefficients).*

   *Show that the LLL algorithm finds a non-zero $u(x) = u_0 + \cdots + u_5 x^5$ in this lattice of length at most $\sqrt{200N}$.* **(5 points)**

3. *Let $u(x)$ be the polynomial in $\mathcal{L}$ returned by the LLL algorithm and say $k \ll N^{1/10}$. Show that if $u(k) = 0 \bmod N$, then $u(k) = 0$ in $\mathbb{Z}$.* **(5 points)**

4. *In the RSA cryptosystem (with exponent $e = 3$), a message $M \in [N]$ is encrypted as $C = M^e \bmod N$, where $N$ is a known large number that is a product of two unknown primes. But suppose we know* the first 93% of the bits of $M$, that is, $M = 2^k q + x$ where $q, k$ is known but $x$ is unknown. Come up with an algorithm to recover $x$ from $C, q, k$ and $N$ in $\operatorname{poly}(\log N)$ time.* **(15 points)**

*Hello customer, The password for the attached document is:********