Exercises marked with a ⋆ can be handed in for bonus points. Due date is March 22.

**Exercise 1**
Let $a, b \in \mathbb{N}$ be odd numbers with $a - b = 2^k$ for some $k \in \mathbb{N}$. Show that $a$ and $b$ are coprime.

**Exercise 2 (⋆)**
Let $f : \mathbb{N} \to \mathbb{R}_+$ be a monotone increasing function with $f(a) + f(b) \leq f(a + b)$. Show that $f(1) + f(2) + f(4) + f(8) + \ldots + f(n) = O(f(n))$.

*Note:* You may assume that $n$ is a power of two.

**Exercise 3**
A floating point number $\hat{z} = a2^e$ is represented as a pair $(a, e)$ of integers. We say that $\hat{z}$ is a $k$-bit approximation of $z \in \mathbb{R}$ if $a$ is a $k$-bit number and $|\hat{z} - z| \leq 2^{-k+1}z$. Let $M(k)$ be the time required to multiply two $k$-bit integers. The goal of this exercise is to show that a $k$-bit approximation of $1/b$ for $b \in \mathbb{N}$ can be computed in time $O(M(k))$.

1. Show how to multiply and add floating point numbers. Determine the time required for those operations.

2. Show that given a $t$-bit approximation $x_n$ of $1/b$, one can compute a $(2t - c)$-bit approximation $x_{n+1}$ of $1/b$ in time $O(M(t))$. Here, $c > 0$ is some constant.

*Hint:* Use Newton iteration applied to the function $f(x) = 1/x - b$. Note that to keep within an acceptable running time, you may only use $O(t)$ bits of $b$.

3. Show how to compute a $k$-bit approximation of $1/b$ in time $O(M(k))$.

**Exercise 4**
Show that given two numbers $a, b \in \mathbb{N}$ of length at most $n$, one can compute $\lfloor a/b \rfloor$ and $a \mod b$ in time $O(M(n))$. This shows that multiplication in $\mathbb{Z}_N$ can be performed in time $O(M(\log N))$.

**Exercise 5 (⋆)**
There is a constant $c$ such that for all $a \geq b > 1$ the Euclidean algorithm on $(a, b)$ takes time at most $c \log(a) \log(b)$. 
Exercise 6
Let $B = \{b_1, \ldots, b_n\} \subset \mathbb{R}^n$ be a set of linearly independent vectors. The lattice generated by $B$ is the set of integer linear combinations $L = L(B) = \{\sum_{j=1}^{n} \lambda_j b_j | \lambda_1, \ldots, \lambda_n \in \mathbb{Z}\}$. Any set $B' \subset L$ of linearly independent vectors with $L(B') = L$ is called a basis of the lattice $L$.

1. Show that adding an integer multiple of one basis vector to another basis vector does not change the lattice generated by the basis.
2. Let $P = \{\sum_{j=1}^{n} \lambda_j b_j | 0 \leq \lambda_j < 1 \text{ for all } j = 1 \ldots n\}$ be the fundamental parallelepiped. Show that $P \cap L = \{0\}$.

Exercise 7
Let $\alpha > 0$ be a real number. Our goal is to find rational approximations of $\alpha$ with small denominator. Consider the line $L_\alpha = \{(x, y) \in \mathbb{R}^2 | y = \alpha x\}$ of slope $\alpha$ through the origin and define a sequence of vectors in the following way:

- $b_0 = e_1, b_1 = e_2$
- $b_{2j} = b_{2j-2} + \mu_{2j} b_{2j-1},$ where $\mu_{2j} \in \mathbb{Z}$ is maximal such that $b_{2j}$ is not above $L_\alpha$.
- $b_{2j+1} = b_{2j-1} + \mu_{2j+1} b_{2j},$ where $\mu_{2j+1} \in \mathbb{Z}$ is maximal such that $b_{2j+1}$ is not below $L_\alpha$.
- The sequence ends if $b_n \in L_\alpha$.

Show the following:

1. The sequence of $b_n$ and $\mu_n$ is well-defined. If it is infinite, then the sequence of $b_n$ is unbounded.
2. Every pair of adjacent vectors $(b_n, b_{n+1})$ in the sequence forms a lattice basis of $\mathbb{Z}^2$.
3. The slope of every $b_{2j} = (q, p)$ is a best approximation to $\alpha$ from below in the following sense: $\alpha - p/q = \min\{\alpha - p'/q' | p', q' \in \mathbb{Z}, 0 < q' \leq q, p'/q' \leq \alpha\}$. Similarly, the slope of every $b_{2j+1}$ is a best approximation from above.
4. Suppose that $\alpha = p/q$ for some $p, q \in \mathbb{Z}$. Find and describe the relationship of the sequence of $b_n$ and $\mu_n$ to the intermediate data generated by the Euclidean algorithm run on $p$ and $q$. 

2