(**Not** to be turned in, but please make sure you know how to solve all the problems by Week #2.)

Let us set the following notation:

- $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{R}_+$, $\mathbb{R}^n_+$, and $\mathbb{C}$ respectively denote the positive integers, the integers, the rationals, the real numbers, the positive real numbers, the positive orthant (or **positive quadrant** when $n=2$), and the complex numbers.
- Given any $x_1,\ldots,x_n\in\mathbb{C}$ we set $x:=(x_1,\ldots,x_n)$ and define $\mathrm{Log}|x|=(\log|x_1|,\ldots,\log|x_n|)$.
- We'll frequently use **iff** or $\Longleftrightarrow$ as shorthand for "if and only if".
- For any ring R, we let $R^*:=R\setminus\{0\}$. (We use "\" for set-theoretic difference.)
- We let $R^{n\times n}$ denote the collection of all $n\times n$ matrices with entries in R.
- For any $M\in\mathbb{R}^{n\times n}$ with (i,j)-entry $m_{i,j}$ entry, and any vector of variables $y=(y_1,\ldots,y_n)$, we define the formal expression $y^M:=(y_1^{m_{1,1}}\cdots y_n^{m_{n,1}},\ldots,y_1^{m_{1,n}}\cdots y_n^{m_{n,n}})$

Problems

0: Please read the posted pdfs on: (i) Complexity Theory Notation, (ii) the Extended Euclidean Algorithm, and (iii) the first 4 pages of Viro's "Dequantization of Real Algebraic Geometry on Logarithmic Paper."
Note: You need **not** do Problem 0 first: it may be more helpful do it in parallel with the others...

1: Please show how to compute 2^{343} using 13 or fewer integer multiplications.

2: (a) Please find integers a and b such that $17a+437b=1$. **Hint:** Use the Extended Euclidean Algorithm, as described in Bach & Shallit.
(b) Suppose you know that $x^{17}=\alpha$ and $x^{437}=\beta$, for some nonzero complex numbers α and β. Please express x explicitly as a monomial in α and β, *without* solving for x.
Hint: Find a way to apply your solution to Part (a).

3: Recall the following version of De Moivre's formula from 1722:

$$\left(\cos(\theta)+\sqrt{-1}\sin(\theta)\right)^d=\cos(d\theta)+\sqrt{-1}\sin(d\theta),$$

where $d\in\mathbb{Z}$ and $\theta\in\mathbb{R}$.
(a) Please give an explicit formula for all the complex roots of $x^d=c$, where $d\in\mathbb{N}$ and $c\in\mathbb{C}$. Please make sure to include the case $c=0$.
(b) Consider the line segment connecting the points $(0,-\log|c|)$ and $(d,0)$. Please interpret the absolute values of the roots of $x^d=c$ in terms of the slope of this line segment.

5: Let $p\in\mathbb{N}$ be any prime and define $\mathbb{F}_p$ — the finite field with p elements — to be $\mathbb{Z}/p\mathbb{Z}$, i.e., the integers mod p.
(a) Please find all the square roots of 2 in $\mathbb{F}_{17}$.
(b) Please prove that $a^{(p-1)/2}\neq 1 \pmod p$ implies that a has *no* square root in $\mathbb{F}_p$ (unless a is divisible by p).
(c) Please find a function $\eta(d,p)$ such that such that $x^d=c$ has a root in $\mathbb{F}_p\Longleftrightarrow c^{\eta(d,p)}=1$.
Hint: It may help for you to be aware of 3 facts:

- *Fermat's Little Theorem* + a Finite Field Fact: $\mathbb{F}_p^*$ is a cyclic group of order $p-1$. For instance, for $p=97$, any integer in $\{1,\ldots,96\}$ can be obtained as a power of 5 mod 97.
- *Lagrange's Theorem*: H a subgroup of a finite group $G \Longrightarrow \#H|\#G$. For instance, the powers of 64 mod 97 form a group with 8 elements (a subgroup of F_{97}^*), and 8 indeed divides 96.
- *Bézout's Lemma*: For any relatively prime integers u and v, there are integers a and b with $au+bv=1$.

6: Suppose now that $d\in\mathbb{Z}$ and $c\in\mathbb{R}$.

(a) Please find precise conditions on (c,d) under which $x^d=c$ has a *positive* root.

(b) Please find precise conditions on (c,d) under which $x^d=c$ has a *real* root.

NOTE: Please feel free to e-mail comments, questions, and/or corrections.