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

Since $343=256+64+16+4+2+1=2^8+2^6+2^4+2^2+2^1+2^0$, we immediately obtain $2^{343}=2^{2^8}2^{2^6}2^{2^4}2^{2^2}2^{2^1}2$. So, assuming the powers $2^{2^1},\ldots,2^{2^8}$ have been computed, we only need 5 multiplications. The powers $2^{2^1},\ldots,2^{2^8}$ can easily be computed using 8 multiplications by recursive squaring. (i.e., 2^{2^3} is the square of 2^{2^2}, 2^{2^4} is the square of 2^{2^3}, etc.) So we are done.

2: (a) Please find integers a and b such that $17a+437b=1$. **Hint:** Use the Extended Euclidean Algorithm, as described in Bach & Shallit.

Following the hint, it is easy to obtain that $(a,b)=(180,-7)$ works. (There are in fact infinitely many correct answers.) Maple, for instance, easily gives the preceding answer via the following commands:

igcdex(17,437,'a','b'); [a,b];

(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).

Following the hint, we see that $x=x^1=x^{17\cdot 180+437(-7)}=\left(x^{17}\right)^{180}\left(x^{437}\right)^{-7}=\alpha^{180}\beta^{-7}$ and we are done.

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 $c=0$.

The multiset of roots can be describe explicitly as follows:

$$\left\{|c|^{1/d}\left(\cos\left(\phi+\tfrac{2\pi\ell}{d}\right)+\sqrt{-1}\sin\left(\phi+\tfrac{2\pi\ell}{d}\right)\right)\ |\ \ell\in\{1,\ldots,d\}\right\}$$

where ϕ is the argument of c, i.e., the imaginary part of the complex logarithm of c. Alternatively, one can more concisely write $\left\{e^{\frac{(\mathrm{Log}c)+2\pi\sqrt{-1}\ell}{d}}\ |\ \ell\in\{1,\ldots,d\}\right\}$ where Log is any fixed branch of the complex logarithm function.

(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.

This one was already proved in lecture: In particular, if the slope is s, then the absolute value of all the roots is exactly e^s.

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 $\mathbb{F}_{17}$.

By hand, one quickly obtains (even by brute-force) that the square roots of 2 in $\mathbb{F}_{17}$ are exactly $\{\pm 6\}$ (or $\{6,11\}$).

(b) Please prove, for any odd prime p, 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).

Should $p|a$ then a has square root 0. So let's assume $p\not|a$. If a has square root b then $a=b^2$ (and $b\neq 0$). So $a^{(p-1)/2}=b^{p-1}=1$ where the last equality follows from Fermat's Little Theorem. Having proved the contra-positive, we are done.

(c) Please find a function $\eta(d,p)$ such that such that $x^d = c$ has a root in $\mathbb{F}_p \iff c^{\eta(d,p)} = 1$.
Hint: It may help for you to be aware of 3 facts:

1. *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.
2. *Lagrange's Theorem*: H a subgroup of a finite group $G \implies \#H|\#G$. For instance, the powers of 64 mod 97 form a group with 8 elements (a subgroup of F_{97}^*), and 8 indeed divides 96.
3. *Bézout's Lemma*: For any relatively prime integers u and v, there are integers a and b with $au+bv=1$.

(Note that we should assume $c \neq 0$ since the case $c=0$ is trivial.) In lecture, we already saw the big hint that $\eta(d,p) = \frac{p-1}{\gcd(d,p-1)}$. So let us proceed using this hint...
($\implies$) Should there be a solution $x \in \mathbb{F}_q$ then $x \neq 0$ and we must have that $c^{(p-1)/\gcd(d,p-1)} = x^{d(p-1)/\gcd(d,p-1)} = (x^{p-1})^{d/\gcd(d,p-1)} = 1$ by Fact (1).
($\impliedby$) Suppose $c^{(p-1)/\gcd(d,p-1)} = 1$. By Fact (1), $\mathbb{F}_p^*$ is cyclic so we may assume $c = g^k$ for some generator g and $k \in \{0,\ldots,p-1\}$. But the order of g is $p-1$, so $k(p-1)/\gcd(d,p-1)$ must be a multiple of $p-1$ and thus $\gcd(d,p-1)|k$. So let $j := k/\gcd(d,p-1)$. We will then have that $x = g^j$ is our desired solution. To see this, observe that then $x^d = (g^j)^d = (g^j)^{\gcd(d,p-1)}$, where the last equality follows from Facts (3) and (1). So then, $x^d = g^{j\gcd(d,p-1)} = g^k = c$ and we are done.

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.
[$c>0$ and $d \neq 0$] or [$c=1$ and $d=0$].

(b) Please find precise conditions on (c,d) under which $x^d = c$ has a *real* root.
$c \geq 0$ or d is odd.

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