Ex 1:

1. require that the generic algorithm $\mathcal{A}$ interacts with the group G via provided oracles for group operations
2. for $k=1$: $F(X_1)$ has at most d roots
   for $k-1 \rightsquigarrow k$:
   - write $F(X_1,\dots,X_k) = \sum_{i=1}^{d} X_1^i F_i(X_2,\dots,X_k)$
   - note that $\deg(F_i) \le d-i$, take largest i with $F_i \neq 0$
   - pick $y_2,\dots,y_k \leftarrow \mathbb{Z}_p^{k-1}$, then: $F_i(y_2,\dots,y_k)=0$ with probability at most $\frac{d-i}{p}$
   - if $F_i(y_2,\dots,y_k) \neq 0 =: \lambda$, then $\lambda \cdot X_1^i + \sum_{j=1}^{i-1} X_1^j F_j(y_2,\dots,y_k) =: G(X_1)$ is a polynomial of degree i
     $\Rightarrow \Pr[G(y_1)=0] \le \frac{i}{p}$

   $\Pr[F_1(\vec{y})=0] \le \Pr[G(y_1)=0] + \Pr[F_i(y_2,\dots,y_k)=0] \le \frac{d}{p}$
3. Send ℓ_H, ℓ_G to $\mathcal{A}$, initialize $L = \{(1,\ell_G),(X,\ell_H)\}$
   - Label(x): if $(x,\ell_x) \in L$, outputs ℓ_x,
     else outputs random ℓ_x amongst unchosen S and stores (x,ℓ_x) in L
   - Query(ℓ_0,ℓ_1,a_0,a_1):
     - find $(F_b,\ell_b) \in L$ (can assume wlog that both labels were already queried)
     - set $F = a_0F_0 + a_1F_1$
     - if $(F,\ell) \in L$, output L ("known" element)
     - else output $\ell \leftarrow S$ and store (F,ℓ) in S ("new" element)
4. as x is drawn at random (and independently of z), we have $\Pr[x=z] = \frac{1}{p}$ trivially
5. if:
   - ℓ already chosen $\to$ label function not injective
     - can also just choose ℓ amongst unchosen values
     - $\Pr[\text{same } \ell] \le M^2/p$
   - $\exists (F_0,\ell_0),(F_1,\ell_1) \in L$: $F_0 \neq F_1$ but $F_0(x) = F_1(x)$
     - for 2 fixed polys, we have $(F_0-F_1)(x) = 0$ with prob at most $1/p$
     - in total m^2 such pairs, so union bound yields:
       $\Pr[\exists \text{ such } F_0,F_1 \in L] \le m^2/p$

Ex 2:

1. for $p \in [2, \lfloor\sqrt{n}\rfloor]$:
   if $n/p \in \mathbb{N}$: output 0
   output 1
2. if n is prime, then $(a+b)^n = \sum_{k=0}^{n}\binom{n}{k}a^k b^{n-k} = a^n + b^n \mod p$

   thus: $x^n = (\sum_{i=1}^{x} 1)^n \quad (n)$
   $= \sum_{i=1}^{x} 1^n \quad (n)$
   $= x \quad (n)$

   $\overset{x \text{ inv. mod } n}{\Rightarrow} \quad x^{n-1} = 1 \quad (n)$
3. choose $x \in (1, n-1)$:
   if $x^{n-1} \neq 1 \mod n$: output not prime
   else output maybe prime

4. set of $S = \{x^{n-1} = 1 \mod n \mid x \in [1,n]\}$ forms subgroup of $\mathbb{Z}_n^*$
so if $\gcd(n,x) = 1$ and $x \notin S$, then index of S is at least 2
5. all n such that $\forall x \gcd(n,x) = 1$: $x^{n-1} = 1 \mod n$
6. $x^2 = 1 \mod n \Rightarrow x^2 = q \cdot n + 1$ for some q
$\Rightarrow x^2 - 1 = q \cdot n + 1$
$\Rightarrow \underbrace{(x+1)}_{\geq 2}\underbrace{(x-1)}_{0} = q \cdot n$
$\Rightarrow n$ composite
7. look at sequence
$x^t, x^{2t}, \dots, \underbrace{x^{2^s t}}_{= 1 \mod p}$
- note that it's sequence of squares
- if $x^t \neq 1 \mod p$, then there must be a pair $(-1, 1)$ in the sequence mod p (see 6)
8. see for example https://people.csail.mit.edu/vinodv/COURSES/MAT302-S13/manindra.pdf

Ex 3:
1. see slides
2. - $e \cdot d = 1 \mod (p-1)(q-1) = \varphi(n)$,
so $e \cdot d = s \cdot \varphi(n) + 1$
- $(m^e)^d = m^{s \cdot (p-1)(q-1) + 1} \overset{(2.2)}{=} m \mod p$,
similarly $m^{ed} = m \mod q$
- CRT $\Rightarrow m^{ed} = m \mod n$