Homework on §16–17
Due: Thursday, March 21

A. Silverman 16.1.

B. Silverman 16.2c.

C. Silverman 16.3.

D. Silverman 16.4. Ignore the second paragraph. To generate random numbers, put `import random` at the top of your file, then call `random.randint(a,b)` to get a random number between a and b inclusive.

E. 1. Show that if $\gcd(a, n) = 1$ and $r \equiv s \pmod{\varphi(n)}$, then $a^r \equiv a^s \pmod{n}$.

   2. Show that if $\gcd(a, n) \neq 1$, the above is not necessarily true.

F. Silverman 17.2.

G. Silverman 17.4.