Directions: Solve the following problems. All written work must be your own. See the course syllabus for detailed rules.

1. [JJJ 2.8] Alice and Bob agree to use the prime $p = 1373$ and the base $g = 2$ for communications using the ElGamal public key cryptosystem.
   (a) Alice chooses $a = 947$ as her private key. What is the value of her public key?
   (b) Bob chooses $b = 716$ as his private key, so his public key is $B = 2^{716} = 469$. Alice encrypts the message $m = 583$ using the random element $t = 887$. What is the ciphertext (c_1, c_2) that Alice sends to Bob?
   (c) Alice decides to choose a new private key $a = 299$ with associated public key $A = 2^{299} = 34$. Bob encrypts a message using Alice's public key and sends her the ciphertext $(661, 1325)$. Decrypt the message.
   (d) Now Bob chooses a new private key and publishes the associated public key $B = 893$. Alice encrypts a message using this public key and sends the ciphertext $(693, 793)$ to Bob. Eve intercepts the transmission. Help Eve by solving the discrete logarithm problem $2^b \equiv 893 \pmod{1373}$ and use the value of b to decrypt the message.

2. Let m be a positive integer and let $g \in \mathbb{Z}_m^*$.
   (a) Let h be the order of g in $\mathbb{Z}_m^*$. Prove that if $g^n \equiv 1 \pmod{m}$, then $h \mid n$.
   (b) Let n be a positive integer. Prove that the order of g in $\mathbb{Z}_m^*$ equals n if and only if $g^n \equiv 1 \pmod{m}$ and $g^{n/q} \not\equiv 1 \pmod{m}$ for each prime q that divides n.

3. Alice and Bob wish to use the ElGamal cryptosystem to communicate, and they are having difficulty deciding on a prime/base pair (p, g). The pairs that they are considering are $(345601, 71482)$ (option A), $(516163, 482305)$ (option B), and $(177007, 145014)$ (option C). Which option do you recommend for Alice and Bob, and why?

4. Shanks's Algorithm By Hand. Let $p = 211$ and let $g = 8$.
   (a) Find the order N of g in $\mathbb{F}_p$.
   (b) Compute List 1 in Shanks's Algorithm for computing $\log_g(h)$.
   (c) Use Shanks's Algorithm to find each of the following discrete logarithms. In each case, explicitly give List 2.

      i. $\log_g(122)$ ii. $\log_g(150)$ iii. $\log_g(200)$

5. Shanks's Algorithm By Computer.
   (a) Implement Shanks's Baby-step/Giant-step algorithm `shanks_discrete_log(g,h,m)` that returns x such that $g^x \equiv h \pmod{m}$ when such an x exists. Submit your code.

      Hint: if implementing the algorithm in python, then you may find the built-in dictionary class useful. See `shanks.py` for code that makes a dictionary storing the first few powers of a base g and a naive, brute-force implementation `naive_discrete_log(g,h,m)`.
   (b) Let $p = 84298814015219$. Use your code to compute $\log_2(3)$ in $\mathbb{F}_p$. With a good implementation, it should take no more than about a minute on modern hardware. (My laptop from about 2016 takes 6 or 7 seconds.)

6. Solve the following systems of congruences.

   (a)

$$\begin{aligned} x &\equiv 18 \pmod{25} \\ x &\equiv 7 \pmod{11} \\ x &\equiv 16 \pmod{32} \end{aligned}$$

   (b)

$$\begin{aligned} 17x &\equiv 8 \pmod{43} \\ 6x &\equiv 41 \pmod{55} \\ 5x &\equiv 4 \pmod{9} \end{aligned}$$

   (c)

$$\begin{aligned} 7x &\equiv 33 \pmod{145} \\ 11x &\equiv 44 \pmod{45} \\ 17x &\equiv 38 \pmod{75} \end{aligned}$$

   Caution: The given moduli are not pairwise relatively prime (for example, $3 \mid 45$ and $3 \mid 75$), so CRT does not apply directly.