1. **Pollard (10 marks)** Use Pollard’s $p - 1$ algorithm to factor $N = 1739$, given that $N$ is a product of two primes $p$ and $q$ such that $p - 1$ is 3-smooth. Show your work.

2. **Factoring with Cube Roots (20 marks)** Let $p = 1 \pmod{3}$ be a prime number. It turns out that the equation $x^3 = a \pmod{p}$ has either no solutions or three solutions, depending on what $a$ is.

   - Take as example $p = 13$. What are the solutions to the equation $x^3 = 1 \pmod{13}$?
   - Generalizing this, what are the solutions to the equation $x^3 = 1 \pmod{p}$? Prove your statement. (*Hint: let $g$ be a generator of $\mathbb{Z}_p^*$. Think of what the solutions could be as powers of $g$.*)

Now, let $q$ be another prime such that $q = 1 \pmod{3}$ as well, and let $N = pq$.

   - How many solutions does the equation $x^3 = 1 \pmod{N}$ have? Prove your assertion. (*Hint: Chinese Remaindering*).
   - Imagine that I give you $N$ (but not $p$ or $q$) and I also give you a solution to the equation $x^3 = 1 \pmod{N}$ such that (a) $x \neq 1 \pmod{N}$ and (b) $(x + 1)^2 \neq x \pmod{N}$. Show how to use such an $x$ to factor $N$.

3. **(20 marks)** Answer either one of the two questions below.

   - **El Gamal Signatures** Suppose that Samantha the signer uses the El Gamal signature scheme and that she is careless and uses the same ephemeral key $e$ to sign two messages $M$ and $M'$.
     - How can Eve detect that Samantha has made this mistake?
     - If the signature on $M$ is $(\sigma_1, \sigma_2)$ and that on $M'$ is $(\sigma'_1, \sigma'_2)$, explain how Eve can recover $s$, Samantha’s private signing key.

     (*Problem 7.7 from the text*)

   - **Schnorr Signatures** Below is the Schnorr Signature Scheme that you can obtain from the Schnorr identification scheme we saw in class.

     Samantha the signer has a public key $PK = (p, g, g^x \pmod{p})$ where $p$ is a prime, $g$ a generator of $\mathbb{Z}_p^*$ and $x$ is a random number in $\mathbb{Z}_{p-1}$. Her secret key $SK = x$. To sign a message $M \in \mathbb{Z}_{p-1}$, she computes $\sigma_1 = g^a \pmod{p}$ where $a$ is a random number in $\mathbb{Z}_{p-1}$, $c = H(M)$ where $H$ is a “hash function” we mentioned in class, and $\sigma_2 = a + cx \pmod{p-1}$. The signature is $\sigma = (\sigma_1, \sigma_2)$.

     Now, assume as before that Samantha the signer has a faulty random number generator that produces the same random number $a$ when she tries to sign two different messages $M$ and $M'$.
If the signature on $M$ is $(\sigma_1, \sigma_2)$ and that on $M'$ is $(\sigma'_1, \sigma'_2)$, explain how Eve can recover $s$, Samantha’s private signing key. You may assume for the purposes of this problem that $H$ is a one-to-one function.