1. Which of 16, 17, and 18 are Miller-Rabin witnesses that 91 is composite?

2. Use Pollard's $p-1$ method, with $a = 2$, to factor $n = 33748307$. State the smallest $k$ that provides a nontrivial factor of the form $\gcd(a^k-1, n)$.

3. The integer $p = 310000000000013$ is prime. Find an integer $x$ with $x^2 \equiv 1000000000001 \mod p$. [Hint: HW2!]

4. Set $n = 1729 = 7 \times 13 \times 19$, which is Carmichael. Prove that each element $a \in (\mathbb{Z}/n)^\times$ satisfies

$$a^{(n-1)/2} \equiv 1 \mod n.$$ 

Find a Carmichael number that does not have this property.

5. Determine the number of elements of the group $(\mathbb{Z}/1729)^\times$. Out of these, how many are Solovay-Strassen witnesses that 1729 is composite?

6. Using the quadratic sieve method, factor $n = 46698343$. List only the congruences that you use to construct

$$x^2 \equiv y^2 \mod n.$$ 

An RSA cipher has modulus $n$ and encryption key $e = 17$. Use your factorization to decode the message

29034923.

Express the final answer in terms of the nine letter alphabet from the lecture notes.

7. Consider the elliptic curve $y^2 = x^3 + 1$ over the rational numbers. Determine the order of the points $P = (0, 1)$ and $Q = (2, 3)$. [Hint: What is the tangent line to the curve at $P$?]

8. Consider the elliptic curve $y^2 = x^3 - 13x + 5 \mod 31$. Compute the order of the points $(10, 10)$ and $(7, 28)$. Using this, along with the Hasse bound, determine the number of elements in this elliptic curve group.

9. The integer $n = 34547647$ is a product of two primes, $p$ and $q$. Determine these using elliptic curve factorization with $P = (2, 3)$ on $y^2 = x^3 + 2x - 3$. State the smallest $k$ such that computing $k!P$ yields a factor of $n$.

Compute the order of $P$ on the elliptic curve modulo $p$ and modulo $q$.

10. Use the Pocklington-Lehmer test to prove that 99990001 is prime.