# 1 Baby Fermat

Assume that $a$ does have a multiplicative inverse mod $m$. Let us prove that its multiplicative inverse can be written as $a^k \pmod{m}$ for some $k \geq 0$.

(a) Consider the sequence $a, a^2, a^3, \dots \pmod{m}$. Prove that this sequence has repetitions.

(b) Assuming that $a^i \equiv a^j \pmod{m}$, where $i > j$, what can you say about $a^{i-j} \pmod{m}$?

(c) Prove that the multiplicative inverse can be written as $a^k \pmod{m}$. What is $k$ in terms of $i$ and $j$?

# 2 RSA Practice

Consider the following RSA schemes and solve for asked variables.

(a) Assume for an RSA scheme we pick 2 primes $p = 5$ and $q = 11$ with encryption key $e = 9$, what is the decryption key $d$? Calculate the exact value.

(b) If the receiver gets 4, what was the original message?

(c) Encode your answer from part (**??**) to check its correctness.

## 3 RSA with Three Primes

Show how you can modify the RSA encryption method to work with three primes instead of two primes (i.e. $N = pqr$ where $p, q, r$ are all prime), and prove the scheme you come up with works in the sense that $D(E(x)) \equiv x \pmod{N}$.

## 4 RSA with Limited Messages

Suppose that Alice only has two possible messages she might send Bob: either "Yes" or "No".

(a) If Alice and Bob use the standard RSA procedure, describe how Eve could find out which message Alice sent.

(b) Describe how Alice and Bob might modify the RSA procedure to stop Eve from using this exploit. *(Hint: Try using a one-time pad somewhere in your procedure)*