Math 173A - RSA and Primality Testing

1. Why should you choose your public exponent to be 1 or 2 in RSA?

2. Suppose $n = pqr$ is the product of three distinct primes. How would an RSA-type scheme work in this case? In particular, what relation would the encryption and decryption exponents e and d satisfy?

3. The number 561 factors as $3 \cdot 11 \cdot 17$. First use Fermat's little theorem to show that

$$a^{561} \equiv a \pmod{3}, \quad a^{561} \equiv a \pmod{11}, \quad a^{561} \equiv a \pmod{17},$$

for every value of a. Explain why these three congruences imply that $a^{561} \equiv a \pmod{561}$ for all a.