> *The art of doing mathematics consists in finding that special case which contains all the germs of generality.* - David Hilbert.

Question 1. Fermat's little theorem says that if p is prime and $\gcd(2,p) = 1$, then $2^{p-1} \equiv 1 \bmod p$. However, the converse is not true: if m is a number, $\gcd(2,m) = 1$, and $2^{m-1} \equiv 1 \bmod m$, this **does not imply** that m is a prime number. A number m is called a 2-pseudoprime if (a) m is composite, and (b) $2^{m-1} \equiv 1 \bmod m$. Show that 341 is a 2-pseudoprime, i.e., show that $2^{340} \equiv 1 \bmod 341$, but 341 is a composite number.

Question 2.

(a) Verify that if n is composite, i.e., $n = ab$, then the polynomial $x^n - 1$ factors as

$$x^n - 1 = (x^b - 1)(x^{b(a-1)} + x^{b(a-2)} + \cdots + x^b + 1).$$

(b) Show that if n is composite, then $m = 2^n - 1$ is also composite.

(c) Show that if n is a 2-pseudoprime, then $m = 2^n - 1$ is also a 2-pseudoprime.

(d) Use part (c) to show that there are infinitely many 2-pseudoprimes.

Question 3. A Carmichael number is a composite positive integer m such that $b^{m-1} \equiv 1 \bmod m$ for all integers b which are relatively prime to m.

(a) Show that 561 is a 2-pseudoprime and a 5-pseudoprime, i.e., show that

$$2^{560} \equiv 1 \bmod 561, \quad \text{and} \quad 5^{560} \equiv 1 \bmod 561.$$

(b) Show that $b^{80} \equiv 1 \bmod 561$, for all b relatively prime to 561. (Hint: Use Fermat's little theorem.)

(c) Use part (b) to conclude that 561 is a Carmichael number. (In fact, 561 is the smallest Carmichael number.)

(d) Prove that 1105 is also a Carmichael number. (1105 is the second Carmichael number.)

Question 4. Show that for any prime p the polynomial $x^p - x$ factors as

$$x(x-1)(x-2)\cdots(x-(p-1))$$

over $(\mathbb{Z}/p\mathbb{Z})[x]$. Check that this works for $p = 5$.

Question 5. Prove that 74 is a primitive root modulo 89.

Question 6. Find a primitive root modulo 61.

Question 7. Find a primitive root modulo 73.

Question 8. Let p be an odd prime. Show that if b is a primitive root modulo p then

$$b^{(p-1)/2} \equiv -1 \mod p.$$

Question 9. Prove Wilson's theorem using the fact that there exists a primitive root modulo p. (Hint: suppose that g is a primitive root mod p, and write every unit as a power of g.)