1. Suppose that p and $q = 2p + 1$ are both odd primes. Explain why (a) $2p$ is a quadratic non-residue of q and (b) q has $p - 1$ primitive roots.

Show that the primitive roots of q are precisely the quadratic non-residues of q, other than $2p$.

2. Prove that if n has a primitive root then it has $\phi(\phi(n))$ of them.

3. Let p be an odd prime. Show that every element in $\mathbb{Z}/p\mathbb{Z}$ can be written as the sum of two squares.

4. Do there exist integer solutions to the equation $x^2 \equiv 251 \bmod 779$? *Note that* $771 = 19 \times 41$.

5. Does the equation $x^2+10x+15 \equiv 0 \bmod 45083$ have any integer solutions? *Note that* 45083 *is prime.*

6. Use the Fermat method to factorise 9579, without using a calculator.

7. For any integer $n \geqslant 2$, let $F_n = 2^{2^n} + 1$ be the nth "Fermat number". Suppose that p is a prime factor of F_n.

(i) Show that $\mathrm{ord}_p(2) = 2^{n+1}$.

(ii) Show that

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

(iii) Deduce that $p = 1 + 2^{n+2}k$ for some $k \in \mathbb{N}$.

Hence, or otherwise, verify that $F_4 = 65537$ is prime.

8. Using the Fermat method, factorise 2881, and hence find $\phi(2881)$.

A message has been encrypted using RSA and the encoding $01 \leftrightarrow A$, $02 \leftrightarrow B$, $03 \leftrightarrow C$, etc. with exponent $e = 5$ and modulus $n = 2881$. The message is 2352 2138 0828. What is the plain-text message? *I suggest using a free online modular exponentiation calculator, which you can find by a google search for those terms.*

9. Let $p \geqslant 7$ be a prime. Show that every nonzero element of $\mathbb{Z}/p\mathbb{Z}$ is a sum of two *non-zero* squares.

`ben.green@maths.ox.ac.uk`