Directions: Solve the following problems. All written work must be your own. See the course syllabus for detailed rules.

1. Alice's public key uses modulus

$$N = 22476\ 96411\ 17831.$$

Of course, $N = pq$ for some secret primes p and q. Somehow, Eve is able to compute

$$(p-2)(q-3) = 22476\ 95651\ 24622.$$

Help Eve use this information to factor N. *Hint:* try to adapt the technique for factoring N given $(p-1)(q-1)$ to this new case.

2. [JJJ 3.13(a)] Here, we prove that 561 is a Carmichael number. That is, 561 is composite and yet it has no Fermat witnesses. Note that $561 = 3 \cdot 11 \cdot 17$.

   (a) Prove that if $a \in \mathbb{Z}_{561}^*$, then a satisfies the system

$$\begin{aligned} a^{560} &\equiv 1 \pmod 3 \\ a^{560} &\equiv 1 \pmod{11} \\ a^{560} &\equiv 1 \pmod{17} \end{aligned}$$

   (b) Prove that 561 has no Fermat witnesses.

3. For each pair (n, a) below, determine whether a is (i) a Fermat witness for n; and (ii) a Miller–Rabin witness for n.

   (a) $n = 21$ and $a = 8$
   (b) $n = 1279$ and $a = 1091$
   (c) $n = 1722971$ and $a = 1711330$
   (d) $n = 1722971$ and $a = 2$
   (e) $n = 8533633$ and $a = 3862185$
   (f) $n = 8533633$ and $a = 5393220$