(1) Efficiently compute the greatest common divisor of 82319, 96521.

Use the Euclidean algorithm applied to 96521, 82319: each step is a reduction algorithm step of the form $D - q \cdot d = r$. For each such line, the next replaces the previous dividend $D$ by the previous divisor $d$, and replaces the divisor by the previous remainder $r$. The algorithm terminates when the right-hand side (remainder) is 0. The last non-zero remainder is the greatest common divisor.

\[
\begin{align*}
96521 &- 1 \cdot 82319 = 14202 \\
82319 &- 5 \cdot 14202 = 11309 \\
14202 &- 1 \cdot 11309 = 2893 \\
11309 &- 3 \cdot 2893 = 2630 \\
2893 &- 1 \cdot 2630 = 263 \\
2630 &- 10 \cdot 263 = 0
\end{align*}
\]

Since the last right-hand side before the 0 is 263, the greatest common divisor of 96521, and 82319 is 263.

(2) Efficiently compute a multiplicative inverse of 317 modulo 1013.

Use the (‘extended’) Euclidean algorithm applied to 317 and 1013: each step going forward is a reduction algorithm step of the form $D - q \cdot d = r$. For each such line, the next replaces the previous dividend $D$ by the previous divisor $d$, and replaces the divisor by the previous remainder $r$. The algorithm terminates when the right-hand side (remainder) is 0. The last non-zero remainder is the greatest common divisor.

When the gcd is 1 we can then reverse the algorithm to eventually obtain an expression of the form $a \cdot 317 + b \cdot 1013 = 1$. The reverse algorithm consists of repeatedly substituting back by replacing the remainder of a previous line with its expression on the left-hand side, and regrouping.

\[
\begin{align*}
317 &- 0 \cdot 1013 = 317 \\
1013 &- 3 \cdot 317 = 62 \\
317 &- 5 \cdot 62 = 7 \\
62 &- 8 \cdot 7 = 6 \\
7 &- 1 \cdot 6 = 1 \\
6 &- 6 \cdot 1 = 0 \\
1 &\quad = (1)7 + (-1)6 = (1)7 + (-1)(62 - 8 \cdot 7) \\
&\quad = (-1)62 + (9)7 = (-1)62 + (9)(317 - 5 \cdot 62) \\
&\quad = (9)317 + (-46)62 = (9)317 + (-46)(1013 - 3 \cdot 317) \\
&\quad = (-46)1013 + (147)317 = (-46)1013 + (147)(317 - 0 \cdot 1013) \\
&\quad = (147)317 + (-46)1013
\end{align*}
\]

In general, if $ax + bm = 1$ then $a$ is a multiplicative inverse of $x$ mod $m$, so if $a317 + b1013 = 1$ then $a$ is a multiplicative inverse of 317 mod 1013. Therefore, from $(147) \cdot 317 + (-46) \cdot 1013 = 1$, $(147) \cdot 317 = 1 \mod 1013$, so 147 is a multiplicative inverse of 317 modulo 1013.

(3) Find a solution to the system

\[
\begin{align*}
x &\equiv 4 \mod 53 \\
x &\equiv 2 \mod 79
\end{align*}
\]

Use Sun-Ze’s theorem, of which the computationally effective version is achieved via the extended version of the Euclidean algorithm. To solve a system $x = a \mod p$ and $x = b \mod q$ (with $\gcd(p, q) = 1$), use the extended Euclidean algorithm to find integers $s, t$ so that $sp + tq = 1$. Then $x = sp \cdot b + tq \cdot a$ is a solution (and is the only solution modulo $pq$). In the case at hand, via the extended Euclidean algorithm applied to $p = 53$ and $q = 79$.

\[
\begin{align*}
53 &- 0 \cdot 79 = 53 \\
79 &- 1 \cdot 53 = 26 \\
53 &- 2 \cdot 26 = 1 \\
26 &- 26 \cdot 1 = 0 \\
1 &\quad = (1)53 + (-2)26 = (1)53 + (-2)(79 - 1 \cdot 53) \\
&\quad = (-2)79 + (3)53 = (-2)79 + (3)(53 - 0 \cdot 79) \\
&\quad = (3)53 + (-2)79
\end{align*}
\]
Thus, we get \((3)^{53} + (-2)^{79} = 1\). Thus, our system has solution (from the formula above)

\[ x = (3)^{53} \cdot 2 + (-2)^{79} \cdot 4 = 3873 \mod 53 \cdot 79 \]

(4) Verify (with reasonable efficiency) that 6 is a primitive root modulo 59.

Either anticipating Lagrange’s theorem or by treatment of this special situation as in class, we know that the order of 6 is a divisor of the order of the group \((\mathbb{Z}/59)^\times\) which we know to be 59 – 1 since 59 is prime. It was observed in class that if the order fails to be the maximum possible (namely 59-1 itself) then the actual order of 6 must divide \((59 - 1)/q\) for some prime divisor q of 59-1. Since 59-1 is small enough to be readily factored (with distinct prime factors 2, 29), we should compute (by the fast modular exponentiation algorithm) \(6^{(59-1)/2} \mod 59\), \(6^{(59-1)/29} \mod 59\). The quantity \(6^{(59-1)/2} \mod 59\) is computed as \((6, 29, 1), (6, 28, 6), (36, 14, 6), (57, 7, 6), (57, 6, 47), (4, 3, 47), (4, 2, 11), (16, 1, 11), (16, 0, 58)\). Thus, \(6^{(59-1)/2} \mod 59 = 58\). The quantity \(6^{(59-1)/29} \mod 59\) is computed as \((6, 2, 1), (36, 1, 1), (36, 0, 36)\). Thus, \(6^{(59-1)/29} \mod 59 = 36\). \(6^{(59-1)/2} \mod 59 = 58\), \(6^{(59-1)/29} \mod 59 = 36\). Since neither of these is 1 modulo 59, we conclude that 6 is indeed a primitive root modulo 59.