Problem 1: Euclidean algorithm
Find the greatest common divisor of 100 and 254, using

- prime factorization
- Euclidean algorithm

Solution: $100 = 2^2 \times 5^2$ and $254 = 2 \times 127$. The largest power of 2 that exists in both is 1. The largest power of 5 that exists in both is 0. The largest power of 127 that exists in both is 0. So the greatest common divisor is $2^1 \times 5^0 \times 127^0 = 2$.

Using the Euclidean algorithm, we have the following sequences obtained by successively finding the remainder of the division:

$$254 \quad 100 \quad 54 \quad 46 \quad 8 \quad 6 \quad 2 \quad 0$$

So the answer is 2.

Problem 2
Find $150 \cdot 2^{125} \mod 127$ in any way you want. *Hint*: 127 is prime.

Solution: By Fermat’s theorem, we know that $2^{127-1} \equiv 1 \pmod{127}$. Therefore, we can write

$$150 \cdot 2^{125} = 75 \cdot 2^{126} \equiv 75 \cdot 1 \pmod{127}$$

So the answer is 75.

Another way to do this without using Fermat’s theorem is to write $2^{125}$ as a sequence of multiplication by 2 and squaring, like this:

$$2^{125} = 2((2(2(2(2)^2)^2)^2)^2)^2$$

Now we build up the number starting from 2 and repeatedly squaring or multiplying by 2. But on the way, we always reduce the number below 127.
So $2^{125} \equiv 64 \pmod{127}$. This means we want to find $150 \times 64$ modulo 127, which is 75 as before.

**Problem 3**

Find integers $x < 17$ and $y < 17$ that satisfy:

\[
2x + y \equiv 4 \pmod{17} \\
5x - 5y \equiv 9 \pmod{17}
\]

**Solution:** From the first equation, we have $y \equiv 4 - 2x \pmod{17}$. Therefore, using the second:

\[
5x - 5(4 - 2x) \equiv 9 \pmod{17} \\
15x \equiv 29 \pmod{17} \\
15x \equiv 12 \pmod{17}
\]

Therefore,

\[
x \equiv 15^{-1} \cdot 12 \pmod{17}
\]

We want the inverse of 15 modulo 17 (we know it exists because 15 and 17 are coprime). This can be obtained using the Euclidean algorithm.

\[
a \quad 17 \quad 15 \quad 2 \quad 1 \quad 0 \\
x \quad 1 \\
y \quad 0 \quad 1 \quad -1 \quad 8
\]

So 1 = 17(−7) + 15(8). Therefore, 8 is the inverse of 15 modulo 17. So $x \equiv 8 \times 12 \pmod{17}$. So $x = 11$. From this, we get that $y \equiv 4 - 22 \pmod{17}$, so $y = 16$.

**Problem 4: Cryptography**

Consider an RSA key set with $p = 17$, $q = 23$, and $e = 3$. What value of $d$ should be used for the secret key? What is the encryption of the message 41?

**Solution:** $d$ is the inverse of $e = 3$ modulo $(p - 1)(q - 1) = 352$, and can be obtained using the Euclidean algorithm as in the previous problem. Observe that we need 3 and 352 to be coprime (which they are).

\[
a \quad 352 \quad 3 \quad 1 \quad 0 \\
x \quad 1 \\
y \quad 0 \quad 1 \quad -117
\]

So $1 = 352(1) + 3(-117)$. So $-117$ is the inverse of 3 modulo 352, which is 235 because $-117 \equiv 235 \pmod{352}$.

Then, $n = pq = 391$, and to encode $x$, we need to compute $x^e \pmod{n}$. This is $41^3 \pmod{391} = 105$. One might want to verify that $105^{235} \pmod{391} = 41$. 