1. (30 points)

a) Use the Euclidean algorithm to find the greatest common divisor of 851 and 2479.

2479 divided by 851 is 2, remainder 777
851 divided by 777 is 1, remainder 74
777 divided by 74 is 10, remainder 37
74 divided by 37 is 2, remainder 0

It follows that the gcd is 37.

b) Find integers $x$ and $y$ satisfying the equation

$$2479x + 851y = 111.$$ 

The last equation in (a) is the same as

$$37 = 777 - 10 \cdot 74.$$ 

The preceding one is $74 = 851 - 1 \cdot 777$. Substituting gives

$$37 = 777 - 10 \cdot [851 - 1 \cdot 777] = -10 \cdot 851 + 11 \cdot 777.$$ 

Now use the second equation from (a) to write $777 = 2479 - 2 \cdot 851$. Substituting gives

$$37 = -10 \cdot 851 + 11 \cdot [2479 - 2 \cdot 851] = 11 \cdot 2479 - 32 \cdot 851.$$ 

Now 111 is $3 \cdot 37$. Multiplying this last equation by 3 gives

$$111 = 33 \cdot 2479 - 96 \cdot 851.$$ 

So $x = 33, y = -96$ is one solution.

c) Calculate $\phi(2479)$. We know from (a) that 37 is a prime factor of 2479; dividing gives $2479 = 37 \cdot 67$. These factors are prime. We showed in class that if $p$ and $q$ are distinct primes, then $\phi(pq) = (p - 1)(q - 1)$. So

$$\phi(2479) = 36 \cdot 66 = 2376.$$ 

2. (25 points) This problem is about rational solutions of the equation $x^2 + 2y^2 = 1$. One such solution is $x = -1$ and $y = 0$.

a) Write the equation of a line in the $(x, y)$ plane passing through the point $(-1, 0)$ and having slope $t$.

The equation is

$$y = t(x + 1) + 0 = tx + t.$$
b) Show that the line you wrote in (a) intersects the curve \( x^2 + 2y^2 = 1 \) at points whose \( x \) coordinate satisfies the quadratic equation

\[
(2t^2 + 1)x^2 + 4t^2 x + (2t^2 - 1) = 0.
\]

Substituting the linear equation for \( y \) in the equation for the curve gives

\[
x^2 + 2[t^2 x^2 + 2t^2 x + t^2] = 1,
\]
or

\[
(2t^2 + 1)x^2 + 4t^2 x + (2t^2 - 1) = 0.
\]

c) One root of the equation in (b) is \( x = -1 \). Find the other root.
(The answer should be a formula for \( x \) in terms of \( t \).)

This quadratic in \( x \) can be factored by easy high school algebra, since you know one factor \((x + 1)\):

\[
(2t^2 + 1)x^2 + 4t^2 x + (2t^2 - 1) = (x + 1)((2t^2 + 1)x + (2t^2 - 1)).
\]
The second root is the zero of the second linear factor, or \( x = -\frac{2t^2 - 1}{2t^2 + 1} \).

d) Write a formula (again in terms of \( t \)) for the \( y \) coordinate of the intersection point you calculated in (c).

The formula in (c) gives

\[
x + 1 = \frac{(1 - 2t^2) + (1 + 2t^2)}{2t^2 + 1} = \frac{2}{2t^2 + 1}.
\]

Therefore

\[
y = t(x + 1) = \frac{2t}{2t^2 + 1}.
\]

e) If \( t \) is any rational number, then your formulas from (c) and (d) give the \( x \) and \( y \) coordinates of a rational solution of \( x^2 + 2y^2 = 1 \). Do you get all rational solutions in this way? Explain.

If \((p, q)\) is any rational solution other than \((-1, 0)\), then there is unique line through \((p, q)\) and \((-1, 0)\), and it has slope \( q/(p + 1) \). This is a rational number since we’re assuming \( p \) is not \(-1\). The procedure above (starting with \( t = q/(p + 1) \)) must lead to the solution \((p, q)\). But we definitely don’t get the solution \((-1, 0)\): the formula in (d) shows that \( y = 0 \) can come only from \( t = 0 \), and then the formula in (c) gives \( x = 1 \) (rather than \(-1\)).

3. (15 points) Suppose that \( p \) is an odd prime number. Prove that 9 is not a primitive root modulo \( p \).

If \( p = 3 \), then 9 doesn’t belong to \((\mathbb{Z}/3\mathbb{Z})^\times\), so it isn’t a candidate to be a primitive root. So we may assume that \( p \) is not 3, so 3 and \( p \) are relatively prime. By Fermat’s little theorem, \( 3^{p-1} \equiv 1 \pmod{p} \). Since \( p - 1 \) is even, we can write this as

\[
9^{(p-1)/2} \equiv 1 \pmod{p}.
\]
Therefore 9 has order dividing \((p - 1)/2\), so it is not a primitive root.

4. (20 points) Suppose we want to use the RSA algorithm to encode messages, and we choose the base \(n = 2479\) and the encoding exponent \(e = 47\). This means that a message \(m\) is a number between 0 and 2478, and we encode \(m\) as

\[ s \equiv m^{47} \pmod{2479}. \]

Find a decoding exponent \(d\) so that no matter what the message \(m\) is, it will still be true that

\[ m \equiv s^d \pmod{2479}. \]

From problem 1 we know that \(\phi(2479) = 2376\), so according to the RSA algorithm we need for \(d\) an inverse of 47 modulo 2376. We can calculate using the Euclidean algorithm for 2376 and 47:

\[
\begin{align*}
2376 & \div 47 = 50, \text{ remainder } 26 \quad 2376 = 50 \cdot 47 + 26 \\
47 & \div 26 = 1, \text{ remainder } 21 \quad 47 = 1 \cdot 26 + 21 \\
26 & \div 21 = 1, \text{ remainder } 5 \quad 26 = 1 \cdot 21 + 5 \\
21 & \div 5 = 4, \text{ remainder } 1 \quad 21 = 4 \cdot 5 + 1
\end{align*}
\]

Now we write 1 = 21 − 4 · 5 and substitute in the earlier equations just as in problem 1(b):

\[
\begin{align*}
1 &= 21 - 4 \cdot (26 - 1 \cdot 21) = -4 \cdot 26 + 5 \cdot 21 \\
1 &= -4 \cdot 26 + 5 \cdot (47 - 1 \cdot 26) = 5 \cdot 47 - 9 \cdot 26 \\
1 &= 5 \cdot 47 - 9 \cdot (2376 - 50 \cdot 47) = -9 \cdot 2376 + 455 \cdot 47.
\end{align*}
\]

This last equation gives 455 as an inverse of 47 modulo 2376, so we can choose decoding exponent \(d = 455\).

5. (10 points) Calculate the last two decimal digits of \(2^{80}\).

You are asked to calculate modulo 100. The base two expansion of 80 is

\[ 80 = 64 + 16. \]

Calculating powers of 2 by repeated squaring modulo 100 gives

\[
\begin{align*}
2^2 & \equiv 4 \pmod{100}, & 2^4 & \equiv 16 \pmod{100}, & 2^8 & \equiv 56 \pmod{100}, \\
2^{16} & \equiv 36 \pmod{100}, & 2^{32} & \equiv 96 \pmod{100}, & 2^{64} & \equiv 16 \pmod{100}.
\end{align*}
\]

(For the last entry, for example, we calculate 96\(^2\) = 9216 and keep only the last two digits. More cleverly, we could write

\[ 96^2 \equiv (-4)^2 \equiv 16 \pmod{100} \]

and do the calculation mentally.) From the base two expansion of 80 we get

\[ 2^{80} \equiv 2^{64} \cdot 2^{16} \equiv 16 \cdot 36 \equiv 76 \pmod{100}. \]

(The multiplication of integers in the last step gives 576.) So the last two digits are 76.