1. (a) (5 points) Compute $\varphi(667)$.

**Solution:** We have $667 = 23 \cdot 29$, so $\varphi(667) = 22 \cdot 28 = 616$.

(b) (5 points) Say we have $\mathbb{F}_{169} = \mathbb{F}_{13}[\alpha]$. Give one possible choice of $\alpha$.

**Solution:** $\alpha$ is the square root of any quadratic nonresidue mod 13. The quadratic residues mod 13 are 1, 4, 9, 3, 12, 10, so we just pick any nonzero element not in this list; for example, $\alpha^2 = 2$.

(c) (5 points) Consider $\mathbb{F}_3[i]$ where $i^2 = -1$. Compute the order of $1 + i$ in $(\mathbb{F}_3[i])^\times$.

**Solution:** We have $(1 + i)^2 = -i$, $(1 + i)^3 = 1 - i$, $(1 + i)^4 = 2$. Therefore the order of $1 + i$ is at least 4. But by Lagrange’s Theorem, the order must divide $\#(\mathbb{F}_3[i])^\times = 3^2 - 1 = 8$, so the order is 8.

(d) (5 points) Bob uses Alice’s RSA public key $(323, 29)$ to produce the ciphertext 243. Recover the message.

**Solution:** This one was a bit tricky, because if you use $\varphi(323)$ instead of lcm$(p - 1, q - 1)$, the decryption exponent is quite large. But if you use the lcm, the exponent is manageable: $323 = 17 \cdot 19$, and lcm$(16, 18) = 144$. We have $29 \cdot 5 \equiv 1$ (mod 144), so we can use 5 for the decryption exponent. Finally, $243^5 \equiv 116$ (mod 323).

2. (15 points) You are given that $\varphi(85409) = 84804$. Factor 85409.

**Solution:** If $85409 = pq$, then the polynomial

$$x^2 - (p + q)x + pq$$

is given by

$$x^2 - 606x + 85409,$$

since $p + q = 85409 + 1 - \varphi(85409)$. We then use the quadratic formula to find the roots, yielding 223 and 383.
3. (15 points) Apply Miller-Rabin to \( n = 561 \) with the base \( a = 2 \). Summarize the values of the variables in the program with a table, and clearly state your conclusion.

**Solution:**
We have \( n - 1 = 560 = 2^4 \cdot 35 \). We first have to compute \( 2^{35} \pmod{561} \). Using successive squaring, we get \( \pmod{561} \)

\[
\begin{align*}
2^2 &\equiv 4 \\
2^4 &\equiv 16 \\
2^8 &\equiv 256 \\
2^{16} &\equiv 460 \\
2^{32} &\equiv 103 \\
\end{align*}
\]

and so \( 2^{35} \equiv 103 \cdot 4 \cdot 2 \equiv 263 \pmod{561} \). Then we square 263 repeatedly to get the following table:

<table>
<thead>
<tr>
<th>( i )</th>
<th>( 419^{2^i} \pmod{561} )</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>186</td>
</tr>
<tr>
<td>2</td>
<td>67</td>
</tr>
<tr>
<td>3</td>
<td>1</td>
</tr>
</tbody>
</table>

We stop here and observe that \( 67 \not\equiv -1 \pmod{561} \), and hence 561 is composite.

4. (15 points) Let \( p \) be an odd prime and \( a \) an integer with \( p \nmid a \). Show that \( a \) is a quadratic residue mod \( p \) if and only if \( a^{(p-1)/2} \equiv 1 \pmod{p} \).

**Solution:** See HW 8 solutions.

5. (15 points) Let \( E \) be an elliptic curve, let \( P \neq O \) be a point of \( E \), and suppose that the tangent line \( \ell \) to \( E \) at \( P \) is not vertical and does not pass through any other point of \( E \). Find the order of \( P \). Make sure to justify your answer.

**Solution:** The order is 3. Let \( \ell \) be the tangent line at \( P \). The third point of intersection is again \( P \). Reflecting across the x-axis gives us the point \(-P\), and so \( P + P = -P \). Adding \( P \) to both sides yields \( 3P = O \). Therefore the order of \( P \) divides 3. But \( P \neq O \), so \( P \) does not have order 1. Therefore the order is exactly 3.

6. (10 points) The following Python function takes as input an integer \( h \geq 2 \):

```python
def mat(h):
    d=2
    while d <= h:
        if (d**h-d)%h != 0:
            return d
        d = d + 1
    return 0
```

What does the function do? Explain your answer.
**Solution:** The function produces a Fermat witness for $h$, or returns 0 if there are none. Alternatively, the function returns 0 if $h$ is either prime or a Carmichael number, and returns something nonzero otherwise. The Boolean condition is $d^h \equiv d \pmod{h}$, which is satisfied by some $d \mod h$ if and only if either $h$ is prime or a Carmichael number; or in other words, if $d$ is not a Fermat witness. The claim follows.