(1) a) Use Euclidian algorithm to compute the GCD and LCM of 54 and 42.

Solution: a) 54 = 42 + 12, 42 = 12 · 3 + 6, 12 = 6 · 2 + 0 so the GCD is 6 and the LCM is 54 · 42/6 = 378. b) Since 6 does not divide 8, this equation has no solutions. c) The solutions are (−6 + 7k, 8 − 9k) for any k ∈ Z.

(2) Compute \( \phi(105) \) and \( 11^{4804} \mod 105 \).

Solution: 105 = 3 · 5 · 7 and so \( \phi(105) = 2 · 4 · 6 = 48 \). We have 11^48 = 1 and thus \( 11^{4804} = 11^3 = 121^2 \equiv 16^2 \equiv 256 \equiv 46 \).

(3) Solve \( X \equiv_{25} 4 \) and \( X \equiv_{103} 8 \) for some \( 0 \leq X < 2575 \). (You do not need to compute the final answer eg 22 + 17 · 26 is ok)

Solution: From the first eqn we have \( X = 4 + 25k \) and from the second eqn \( 4 + 25k \equiv_{103} 8 \) so that \( 25k \equiv_{103} 4 \). We now compute the inverse of 25 in \( \mathbb{F}_{103} \). 103 = 4 · 25 + 3 and 25 = 3 · 8 + 1 so 1 = 25 − 8(103 − 4 · 25) = 33 · 25 − 8 · 103 i.e. 33 · 25 \equiv_{103} 1. But then \( k \equiv_{103} 33 · 25k \equiv_{103} 33 · 4 \equiv_{103} 132 \equiv_{103} 29 \). Finally \( X = 4 + 25 · 29 \).

(4) Show that \( \mathbb{F}_{17}[i] \) is not a field and find \( (2 + 3i)^{-1} \).

Solution: We have \( 4^2 + 1^2 = 17 \) so \( (4 + i)(4 − i) = 17 \) so 4 + i is a 0 divisor (but fields never have zero divisors). On the other hand \( N(2 + 3i) = 2^2 + 3^2 = 13 \) is invertible modulo 17 (since \( 13 · 4 = 1 + 3 · 17 \)) and so \( (2 + 3i)^{-1} = (2 − 3i)/13 = (2 − 3i)4 = 8 − 12i = 8 + 5i \).

(5) The powers of 2 mod 11 are given below.

<table>
<thead>
<tr>
<th>2^1</th>
<th>2^2</th>
<th>2^3</th>
<th>2^4</th>
<th>2^5</th>
<th>2^6</th>
<th>2^7</th>
<th>2^8</th>
<th>2^9</th>
<th>2^{10}</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>4</td>
<td>8</td>
<td>5</td>
<td>10</td>
<td>9</td>
<td>7</td>
<td>3</td>
<td>6</td>
<td>1</td>
</tr>
</tbody>
</table>

Use discrete logarithms with base 2 to find all solutions of \( 6x^4 = 8 \) in \( \mathbb{Z}/11\mathbb{Z} \).
(6) a) List the order of each element of the group \( (\mathbb{Z}/7\mathbb{Z})^* \).

<table>
<thead>
<tr>
<th>( a )</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
</tr>
</thead>
<tbody>
<tr>
<td>order of ( a )</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

b) Which of the elements are primitive 6-th roots of 1?

c) Use b) to compute \( \Phi_6(X) \).

Solution: The order of 1 is 1, the order of 2 is 3 (since \( 2^1 \equiv 2 \mod 6 \), \( 2^2 \equiv 4 \mod 6 \), \( 2^3 \equiv 1 \mod 6 \)), the order of 3 is 6 (since \( 3^1 \equiv 3 \mod 6 \), \( 3^2 \equiv 3 \mod 6 \), \( 3^3 \equiv 3 \mod 6 \), \( 3^4 \equiv -3 \mod 6 \), \( 3^5 \equiv -2 \mod 6 \), \( 3^6 \equiv 1 \mod 6 \)), the order of 4 is 3 (since \( 4^1 \equiv 4 \mod 6 \), \( 4^2 \equiv 4 \mod 6 \), \( 4^3 \equiv -2 \mod 6 \), \( 4^4 \equiv 2 \mod 6 \)), the order of 5 is 6 (since \( 5^1 \equiv 5 \mod 6 \), \( 5^2 \equiv 1 \mod 6 \), \( 5^3 \equiv 1 \mod 6 \), \( 5^4 \equiv 5 \mod 6 \), \( 5^5 \equiv 1 \mod 6 \), \( 5^6 \equiv 1 \mod 6 \)). The primitive roots are 3 and 5. Thus \( \Phi_6(X) = (X - 3)(X - 5) = X^2 - 8X + 15 = X^2 - X + 1 \).

(7) Compute the cyclotomic polynomial \( \Phi_{10}(X) \).

Solution:
\[
\Phi_{10}(X) = \frac{X^{10} - 1}{\Phi_2(X) \Phi_5(X)} = \frac{X^{10} - 1}{(X^3 - 1) \Phi_2(X)} = \frac{X^5 + 1}{X + 1} = X^4 - X^3 + X^2 - X + 1.
\]

(8) Does \( X^2 + 4X - 15 = 0 \) have a solution is \( \mathbb{F}_{103} \)?

Solution: The above equation is equivalent to \( (X + 2)^2 = 19 \). We compute
\[
\left( \frac{19}{103} \right) = -(\frac{103}{19}) = -(\frac{8}{19}) = -(\frac{2}{19})^3 = 1
\]

(where the first equality holds as 19, 103 \( \equiv 4 \) 3 and the last as 2 \( \equiv 8 \) 3 so that \( \frac{2}{19} = -1 \)). Therefore the above equation has a solution.

(9) Factor 14 + 5i in to indecomposable elements of \( \mathbb{Z}[i] \) (note: \( 14^2 + 5^2 = 221 = 13 \cdot 17 \)).

Solution: \( (14 + 5i) \cdot (14 + 5i) = N(14 + 5i) = 14^2 + 5^2 = 221 = 13 \cdot 17 \). Since \( 13 = 2^2 + 3^2 \) and \( 17 = 1^2 + 4^2 \), the possible factors are \( 3 \pm 2i \) and \( 4 \pm i \). We now compute
\[
\frac{14 + 5i}{4 - i} = \frac{(14 + 5i)(4 + i)}{17} = \frac{51 + 34i}{17} = 3 + 2i.
\]
The factorization is then \( 14 + 5i = (4 - i)(3 + 2i) \). (Or \( -4 + i)(-3 - 2i) \) or \( (1 + 4i)(-2 + 3i) \) or \( (-1 - 4i)(2 - 3i) \).
The continued fraction algorithm for $\alpha > 1$ is purely periodic of period 2 such that $[\alpha] = [\alpha_2] = [\alpha_4] = 10$ and $[\alpha_1] = [\alpha_3] = [\alpha_5] = 1$, thus

$$\alpha = 10 + \frac{1}{1 + \frac{1}{10 + \cdots}}.$$  

Find $\alpha$. Using this, find all solutions to $X^2 - 35Y^2 = 1$.

Solution: We have $\alpha = 10 + \frac{1}{1 + \frac{1}{10 + \frac{1}{10 + \cdots}}} = 10 + \frac{\alpha}{\alpha + 1} = \frac{11\alpha + 10}{\alpha + 1}$ and so $\alpha^2 - 10\alpha = 10$ i.e. $(\alpha - 5)^2 = 35$ i.e. $\alpha = 5 + \sqrt{35}$ (as $\alpha > 10$). We now compute

$$5 + \sqrt{35} = 10 + \frac{1}{1 + \frac{1}{5 + \sqrt{35}}} = 10 + \frac{5 + \sqrt{35}}{6 + \sqrt{35}},$$

so

$$\sqrt{35} = \frac{5 + \sqrt{35}}{6 + \sqrt{35}} = \frac{6\sqrt{35} + 35}{\sqrt{35} + 6},$$

which tells us that the first solution is $(6,1)$. All other solutions are given by $X_k + \sqrt{35}Y_k = (6 + \sqrt{35})^k$. 