MAT 399 Homework 7 – Fall 2026

Due Date: Tuesday, Dec 1

1. Exercise 6.1.1 on page 222. In addition to this exercise, find an illustrative example with values of N, a and r, where $N > 1000$ and $a > 50$, with the property that r is even and $a^{r/2} + 1$ is not divisible by N. Also give the factor of N deduced as $gcd(a^{r/2} - 1, N)$.

2. Exercise 6.2.15 on page 227.

3. Exercise 6.4.7 on page 237.

4. On page 233, show that equation (6.3.22) is True if $\omega \in [0, 1)$. Give reasons based on the definition of θ and $\Delta(\omega, n, x)$. Then show by example with choices of N and $\omega > 1$ that (6.3.22) can be False.

5. Let U_c denote the operator defined on page 234, Definition 6.4.2. Let N=7, c=4, and n=3. Find the unitary matrix for this gate U_c. Which basis states are fixed by U_c?