1. (a) Let a be an arbitrary element in H since it is non-empty. Since H is closed under multiplication, $a^k \in H$ for all $k \in \mathbb{N}$. We note that $a^{|G|} = e$ by Corollary 12.4, so $e \in H$. This implies that $a^{|G|-1} = a^{-1}$, so $a^{-1} \in H$. Lastly, for any $a, b \in H$, we have $ab \in H$. Thus, we proved that H is a subgroup of G. $\square$

(b) **Claim 1:** Let $a \in G$. If $o(a) = d$, then if there exist a $k \in \mathbb{N}$ where $a^k = e$ then $d \mid k$.

By contradiction, $d \nmid k$, then by the Division Algorithm, there exist $q, r \in \mathbb{Z}$ where $a^k = a^{qd} \cdot a^r = e$ where $0 < r < d$. However, $a^{qd} = e^q = e$, so $a^r = e$. This contradicts the minimality of $o(a)$. Hence, r must be 0 and $d \mid k$.

Claim 2: Let $a \in G$. For any $k \in \mathbb{N}$, we have $o(a^k) = \frac{o(a)}{\gcd(o(a),k)}$.

Let $d = o(a)$ and $w = d/\gcd(d,k)$. Then $wk = d(k/\gcd(d,k))$ is divisible by d and so $a^{kw} = e$. Furthermore, suppose we have a $n \in \mathbb{N}$ where $a^{kn} = e$. By Claim 1, we get that $d \mid kn$, so:

$$\frac{d}{\gcd(k,d)} \mid \frac{k}{\gcd(k,d)} n$$

We note that $\gcd(d/\gcd(k,d), k/\gcd(k,d)) = 1$. By Corollary 2.20, $w \mid n$. This implies the smallest value for n is w. $\square$

Claim 3: For any positive integer $d \mid m$, there are exactly $\phi(d)$ elements of G with order d

Since G is cyclic, there exist some $g \in G$ with $o(g) = m$ where $G = \{g, g^2, \cdots, g^m\}$. For any $d \mid m$, there exist an integer q where $dq = m$. Let $a = g^q \in G$ thus $a^d = g^{dq} = e$ and $o(a) = d$. Otherwise, $o(a) < d$ implies $q \cdot o(a) < qd = m$, contradicting that $o(g) = m$. Since $o(a) = d$, we note that $a, a^2, \cdots, a^d$ are all unique. We apply Claim 2 to get that for $1 \leq k \leq d$ that $o(a^k) = d/\gcd(d,k)$. It is clear that if $o(a^k) = d$, then $\gcd(d,k) = 1$. We showed all of the a^k are unique, so there exist at least $\phi(d)$ elements with order d.

We now prove all elements $b \in G$ with order d must be in the form a^k. Let $b = g^r$ for $1 \leq r \leq m$. We apply Claim 2 again to get that $o(g^r) = m/\gcd(m,r) = d$. This implies $\gcd(m,r) = m/d = q$. This further implies that $q \mid r$, so there exist an integer k where $1 \leq k \leq d$ that $qk = r$. Thus, $g^r = (g^q)^k = a^k$. This proves that there exist exactly $\phi(d)$ elements with order d. $\square$

Claim 4: For any positive integer $d \mid m$, there is a unique subgroup of G of order d.

Let $a \in G$ where $o(a) = d$ and $a = g^{m/d}$, which exists by Claim 3. We then denote the set $H = \{a, a^2, \cdots a^d\}$. For any $1 \leq i, j \leq d$, $a^i \cdot a^j = a^{i+j}$. If $i + j \leq d$, then $a^{i+j} \in H$. Otherwise, we note that $a^{i+j} = a^{i+j-d} \cdot a^d = a^{i+j-d}$. Since $i + j \leq 2d$ so $i + j - d \leq d$, $a^{i+j} \in H$. By (a), H is a subgroup of G. Note that all elements in H are unique by our proof of Claim 3, so it is also order d.

It remains to prove H is the only subgroup of order d in G. Suppose there exist a subgroup $E \leq G$ with order d. Let $b \in E$, then $b^d = e$ by Corollary 12.4. We note that $b = g^r$ for some $r \in \mathbb{N}$ and $g^{rd} = e$. By Claim 1, $m \mid rd$, which implies that $m/d \mid r$. Hence, there exist some integer k where $1 \leq k \leq d$ and $b = g^r = (g^{m/d})^k = a^k$. Hence, $b \in H$ and $E \subseteq H$. Since they have the same order, $E = H$. $\square$

(c) We note that from Claim 1 of (a) that since all elements α in G are $\alpha^{|G|} = e$, we have $o(\alpha) \mid m$. Let N_d denote the number of elements in G with exactly order d. We have:

$$\sum_{d|m} N_d = m$$

From the degree of the factorization of cyclotomic polynomial for $x^m - 1$, we have:

$$\sum_{d|m} \phi(d) = m$$

We first prove that either $N_d = 0$ or $N_d = \phi(d)$. We assume $N_d > 0$, so there exist an element $a \in G$ where $o(a) = d$. We note that $\langle a \rangle$ is a subgroup of G with order $o(a) = d$. We note that if there exist another $b \in G$ with order d, $\langle b \rangle = \langle a \rangle$ due to the uniqueness of subgroup with order d. Hence, $b \in \langle a \rangle$ and exists in the form a^k for $1 \leq k \leq d$. We apply Claim 2 from (a) to get that $o(a^k) = d/\gcd(d,k)$. Hence, $o(a^k) = o(a)$ iff $\gcd(d,k) = 1$. This proves that $N_d = \phi(d)$. This gives:

$$\sum_{d|m} (N_d - \phi(d)) = 0$$

Since $N_d \leq \phi(d)$, if there exists a $N_d < \phi(d)$, the sum will be negative. Hence, we get that $N_d = \phi(d)$. Since $m \mid m$ and $\phi(m) \geq 1$, there exist an element β where $o(\beta) = m$. We note that $\langle \beta \rangle$ has order m and G also has order m. Thus, $G = \langle \beta \rangle$. $\square$

2. (a) Yes because $2^5 = 32 \equiv -1 \pmod{11}$, so $-1 \in \langle 2 \rangle$.

(b) We assume that $-1 \in \langle 2 \rangle$. This implies that there exist a positive integer k where $2^k \equiv -1 \pmod{23}$. Since -1 is not a square in $\mathbb{Z}/23\mathbb{Z}$, $(\frac{-1}{23}) - 1$. However, $(\frac{2^k}{23}) = (\frac{2}{23}) \cdots (\frac{2}{23})$. By Theorem 11.4 (b), since $23 \equiv -1 \pmod{8}$, $(\frac{2}{23}) = 1$, so $(\frac{2^k}{23}) = (\frac{-1}{23}) = (\frac{2}{23})^k = 1$, a contradiction. Hence, $-1 \notin \langle 2 \rangle$. $\square$

(c) We note that $2^m + 2^n = 2^n(2^{m-n} + 1)$. Since $23 \mid 2024$, $23 \mid 2^n(2^{m-n} + 1)$. By Euclid's Lemma, since $23 \nmid 2^n$, $23 \mid 2^{m-n} + 1$. This implies that $2^{m-n} \equiv -1 \pmod{23}$. However, this implies that $-1 \in \langle 2 \rangle$ in $(\mathbb{Z}/23\mathbb{Z})^\times$. This contradicts (b), so there does not exist such m and n. $\square$

(d) We first note that for any $2^m + 2^n + 2^r$, we can factor it into $2^r(2^{m-r} + 2^{n-r} + 1)$. 2024's prime factorization is $2^3 \cdot 11 \cdot 23$. Hence, if we wish to make it divisible, we need to find m, n, r where $2^r(2^{m-r} + 2^{n-r} + 1)$ is divisible by $8, 11, 23$. The case for 8 is trivial as we simply set $r = 3$. For $11, 23$, $11, 23 \nmid 2^r$, so it must be that $11, 23 \mid 2^{m-r} + 2^{n-r} + 1$. Let $x = m - r$ and $y = n - r$. Finding a solution is equivalent to solving this congruence:

$$2^x + 2^y \equiv -1 \pmod{11}$$
$$2^x + 2^y \equiv -1 \pmod{23}$$

We first consider the congruences for $\pmod{11}$.

k	$2^k \pmod{11}$
1	2
2	4
3	8
4	5
5	10
6	9
7	7
8	3
9	6
10	1

For $2^x + 2^y \equiv -1$, the sum of their congruence must be equal to 10. Hence, the solutions (x, y) are $(3, 1), (4, 4), (6, 0), (7, 8), (9, 2)$. We now consider the congruences for $\pmod{23}$.

k	$2^k \pmod{23}$
1	2
2	4
3	8
4	16
5	9
6	18
7	13
8	3
9	6
10	12
11	1

For $2^x + 2^y \equiv -1$, the sum of their congruence must be equal to 22, which is -1. Hence, the solutions (x, y) are $(6, 2), (7, 5), (9, 4)$. We take interest in the solution $(3, 1)$ from mod 11 and $(7,5)$ from mod 23 as their differences are both 2. From the table, we also learned that $o(2) = 10$ mod 11 and $o(2) = 11$ mod 23. Hence, we note that:

$$2^{10a}(2^3 + 2^1) \equiv -1 \pmod{11}$$
$$2^{11b}(2^7 + 2^5) \equiv -1 \pmod{23}$$

We wish to make $2^{10a}(2^3 + 2^1) = 2^{11b}(2^7 + 2^5)$. We examine this equality to only its degree where $10a + 3 = 11b + 7$, which we can re-arrange to $10a - 11b = 4$. We need to find positive integer solution to a, b. Fortunately, $70 - 66 = 4$, so $a = 7$ and $b = 6$. Hence, $2^{10\cdot7}(2^3 + 2^1) = 2^{11\cdot6}(2^7 + 2^5) = 2^{73} + 2^{71}$. This implies that

$$2^{73} + 2^{71} + 1 \equiv 0 \pmod{11}$$
$$2^{73} + 2^{71} + 1 \equiv 0 \pmod{23}$$

Thus, $x = 73$ and $y = 71$. Lastly, recall that we set $r = 3$. Hence, $m = 73 + 3 = 76$ and $n = 71 + 3 = 74$. Thus, we get that $2024 \mid 2^{76} + 2^{74} + 2^3$. $\square$

3. (a) Let us assume n is a Carmichael Number. Let $p_i^{k_i}$ be one of its prime power factor. Since p_i is an odd prime, by Corollary 12.10, $(\mathbb{Z}/p_i^{k_i}\mathbb{Z})^\times$ is cyclic. Hence there exist a generator element g_i where $\langle g_i\rangle = (\mathbb{Z}/p_i^{k_i}\mathbb{Z})^\times$ and its order is $|(\mathbb{Z}/p_i^{k_i}\mathbb{Z})^\times| = \phi(p_i^{k_i}) = p_i^{k_i-1}(p_i-1)$. By the Chinese Remainder Theorem, there exist an element a where:

$$a \equiv g_i \pmod{p_i^{k_i}}$$
$$a \equiv 1 \pmod{p_j^{k_j}} \text{ for } j \neq i$$

Since g_i is co-prime to $p_i^{k_i}$, a is co-prime to $p_i^{k_i}$ and all such $p_j^{k_j}$. Hence, a must also be co-prime to n. This implies that $a \in (\mathbb{Z}/n\mathbb{Z})^\times$, so $a^{n-1} \equiv 1 \pmod{n}$. In particular $a^{n-1} \equiv g_i^{n-1} \equiv 1 \pmod{p_i^{k_i}}$. By Claim 1 of 1 (a), this implies that $o(g_i) = p_i^{k_i-1}(p_i-1) \mid n-1$ as desired. □

For the converse, let us assume that $p_i^{k_i-1}(p_i-1) \mid n-1$ for all i. Note that $p_i^{k_i-1}(p_i-1) = \phi(p_i^{k_i})$. Let $a \in (\mathbb{Z}/n\mathbb{Z})^\times$. This implies that a is co-prime to n thus a is co-prime to any $p_i^{k_i}$. Hence, $a \in (\mathbb{Z}/p_i^{k_i}\mathbb{Z})^\times$. $(\mathbb{Z}/p_i^{k_i}\mathbb{Z})^\times$ forms a finite group, so by Corollary 12.4, since $|(\mathbb{Z}/p_i^{k_i}\mathbb{Z})^\times| = \phi(p_i^{k_i})$, $a^{\phi(p_i^{k_i})} = 1$ in $(\mathbb{Z}/p_i^{k_i}\mathbb{Z})$. Note that there exist exist an integer m where $\phi(p_i^{k_i}) \cdot m = n-1$, so $a^{\phi(p_i^{k_i})\cdot m} \equiv 1^m = 1$ in $(\mathbb{Z}/p_i^{k_i}\mathbb{Z})$. This implies that $a^{n-1} \equiv 1 \pmod{p_i^{k_i}}$ for all i. Since all $p_i^{k_i}$ are all co-prime to one another, by the Chinese Remainder Theorem (or LCM property), we get that $a^{n-1} \equiv 1 \pmod{n}$ as desired. □

(b) We first note that the $pqr-1$ expanded is $1296k^3 + 396k^2 + 36k$, which could be factorized into $36k(36k^2 + 11k + 1)$. Notice that $6k+1$, $12k+1$, and $18k+1$ are all distinct primes, so $pqr = p_1^1 p_2^1 p_3^1$ with $k_i = 1$ for all $i = 1, 2, 3$. For each p_i, $p_i^{k_i-1}(p_i - 1) = p_i - 1$. We now note that $6k, 12k, 18k \mid 36k(36k^2 + 11k + 1)$. By (a), pqr is a Carmichael number. □

(c) Since p, q are distinct, let us assume $p > q$. We express $pq = p_1^{k_1} p_2^{k_2}$ where $k_i = 1$ for all $i = 1, 2$. Let $p_1 = p$, so $p_1^{k_1-1}(p_1 - 1) = p - 1$. We now show that $p - 1 \nmid pq - 1$. By contradiction, we assume that $p - 1 \mid pq - 1$. Note that $pq - 1 = q(p-1) + q - 1$. Since $p - 1 \mid q(p-1)$, it implies that $p - 1 \mid q - 1$. However, $p - 1 > q - 1$, a contradiction. By (a), pq is not a Carmichael number. □

4. By contradiction, we assume n is a composite number. Let q be a prime factor of n.

Claim 1: Let n be a composite number. There exist prime factors r where $r \leq \sqrt{n}$.

By contradiction, there only exist prime factors where $r > \sqrt{n}$. Since $r \mid n$, there exist integer k where $rk = n$. This implies that $n/k > \sqrt{n} \implies k/n < \sqrt{n}/n \implies k < \sqrt{n}$. Since $r \neq n$ as n is not prime, $k \neq 1$. Let $\hat{p}$ be a prime factor of k, then $\hat{p} \mid k$ and $\hat{p} < \sqrt{n}$, a contradiction. $\square$

By Claim 1, we may assume the existence of a q where $q < \sqrt{n}$. We must have $\gcd(a, q) = 1$, otherwise if $q \mid a$ then $a^{n-1} \equiv 0 \pmod q$, contradicting $a^{n-1} \equiv 1 \pmod n$. Since $\gcd(a, q) = 1$, by Fermat's Little Theorem, we get that $a^{q-1} \equiv 1 \pmod q$.

Since $p \mid n - 1$, write $n - 1 = pt$. We then note that $\gcd(a^t - 1, q) = 1$ by condition (c), so $a^t \not\equiv 1 \pmod q$. This implies that $o_q(a) \nmid t = (n - 1)/p$, but $o_q(a) \mid (n - 1)$.

Claim 2: Let a, b, c be non-zero integers. If $a \mid bc$ but $a \nmid c$, then $\gcd(a, b) > 1$.

By contradiction, we assume $\gcd(a, b) = 1$. By Corollary 2.20, $a \mid c$, a contradiction. $\square$

By Claim 2, this implies that $\gcd(o_q(a), p) > 1$. However, p is prime, so this implies that $\gcd(o_q(a), p) = p$ thus $p \mid o_q(a)$. Since $o_q(a) \mid q - 1$, $p \mid q - 1$ and $p \leq q - 1 < q$. Thus, $q > p > \sqrt{n} - 1$ and $q \geq p + 1 > \sqrt{n}$, so $q > \sqrt{n}$. This is a contradiction to our earlier assumption. Hence, n must be prime. $\square$

5. (a) **Claim:** $\theta_1 + \theta_2 = \zeta^1 + \zeta^2 + \cdots + \zeta^{22} = -1$

We note that $1 + \theta_1 + \theta_2 = 1 + \zeta^1 + \zeta^2 + \cdots + \zeta^{22}$ forms a geometric sum and hence, it is equal to $\frac{\zeta^{23}-1}{\zeta-1} = \frac{0}{\zeta-1} = 0$. Thus, $\theta_1 + \theta_2 = -1$. □

Claim: $\theta_1 \cdot \theta_2 = 6$

We first note that $S = \{2^0, 2^1, 2^8, 2^2, 2^9, 2^3, 2^5, 2^{10}, 2^7, 2^4, 2^6\} = \langle 2 \rangle$ in $(\mathbb{F}_{23})^\times$. We then note that for any quadratic residue $s \in S$, $-s \in T$ because $(\frac{-s}{23}) = (\frac{-1}{23})(\frac{s}{23}) = -1$. Hence, $-s$ is a quadratic non-residue and we also note that each $-s$ is unique by Lemma 7.14 and $\mathbb{F}_{23}$ is a field. Hence, we get that $-S = \{-s : s \in S\}$ contains 11 unique quadratic non-residue, so $-S = T$. Thus, all quadratic residue can be expressed as 2^k and non-residue can be expressed as -2^k for $0 \leq k \leq 10$ in $\mathbb{F}_{23}$.

We now return to product and we note that:

$$\theta_1 \cdot \theta_2 = \sum_{t \in T} (\zeta^t \cdot \sum_{s \in S} \zeta^s) = \sum_{s \in S} \sum_{t \in T} \zeta^{s+t}$$

We now observe that addition of the powers of ζ behaves similarly to addition in $\mathbb{F}_{23}$ as $\zeta^{s+t} = \zeta^{(s+t) \pmod{23}}$. Hence, we then note that for 11 of the terms in the sum $-s = t$, so $s + t = 0$. Hence, $\zeta^{s+t} = \zeta^{23} = 1$, and the sum of the 11 terms is equal to 11. For the remaining 110 terms, we first consider the number of possible pairs where $\zeta^{s+t} = \zeta^1$. We note that:

$$\begin{aligned} 1 &= 13 + 11 = 2^7 - 2^{10} \\ &= 9 + 15 = 2^5 - 2^3 \\ &= 4 + 20 = 2^2 - 2^8 \\ &= 3 + 21 = 2^8 - 2^1 \\ &= 2 + 22 = 2^1 - 2^0 \end{aligned}$$

There exist exactly 5 pairs where $s + t = 1$. We then note that for any $s + t$, it can be translated into $2^d - 2^r$ where $0 \leq d, r \leq 10$. We then note that for any $\hat{s} \in S$, $\hat{s} = 2^k = 2^k(1)$. For each $2^d - 2^r = 1$, $\hat{s} = 2^{d+k} - 2^{r+k}$. Hence, there exist 5 different $s + t = \hat{s}$. For each, $\hat{t} \in T$, $\hat{t} = -2^k = -2^k \cdot 1$ and applying the same logic, there also exist 5 different $s + t = \hat{t}$. Hence, for each $a \in S \cup T$, ζ^a repeats itself 5 times in the 110 terms. Hence, the sum of the 110 terms is equal to $5 \cdot (\zeta^1 + \zeta^2 + \cdots + \zeta^{22}) = -5$. Thus, we sum it with the sum of the other 11 terms to get that $\theta_1 \cdot \theta_2 = 11 - 5 = 6$. □

(b) By the Division Algorithm for polynomials, since $\Phi_{23}(x)$ is a monic polynomial, $F(x) = \Phi_{23}(x)q(x) + r(x)$ for some polynomial $q(x), r(x) \in \mathbb{Z}[x]$. We then note that $F(\zeta^n) = \Phi_{23}(\zeta^n)q(\zeta^n) + r(\zeta^n) = r(\zeta^n)$ (since ζ^n is a root of Φ_{23}). We reframe our focus to $r(x)$ and note that $\deg(r) \leq 21$. We now consider the polynomial of $g(x) = r(x) - r(\zeta)$. We note that $F(\zeta^n) = r(\zeta^n) = r(\zeta)$, so $\zeta^1, \cdots, \zeta^{22}$ are zeroes of $g(x)$, so by Corollary 9.7, $(x - \zeta) \cdots (x - \zeta^{22}) \mid g(x)$. However, we note that $\deg(g) = \deg(r)$ and $22 > \deg(g)$. This leaves that $g(x) = 0$. In other words, $r(x) = r(\zeta)$, so it is a constant function. Since $r(x) \in \mathbb{Z}[x]$, it implies $r(\zeta) = F(\zeta) \in \mathbb{Z}$. □