1. We define $f : \mathbb{Z} \to \mathcal{O}(N)$ by

$$f(n) = \{ d \in \mathbb{N} \mid d \mid n \}.$$ 

Prove $\forall a, b \in \mathbb{Z},$

$$D(a) \cap D(b) = D(b) \cap D(a+b).$$

Let $a, b \in \mathbb{Z}$ be arbitrary.

1. Assume $d \in D(a) \cap D(b).$
   Then $d \in \mathbb{N}$ and $d \mid a$ and $d \mid b.$
   Thus $d \mid (a+b),$ so $d \in D(a+b)$ and $d \in D(b) \cap D(a+b).$

2. Assume $d \in D(b) \cap D(a+b).$
   Then $d \in \mathbb{N}$ and $d \mid b$ and $d \mid (a+b).$
   Thus, $d \mid a$ and $d \in D(a)$ and $d \in D(a) \cap D(b).$

From 1 & 2, $D(a) \cap D(b) = D(b) \cap D(a+b).$

Since $a, b \in \mathbb{Z}$ were arbitrary, we conclude this holds for all $a, b \in \mathbb{Z}.$
2. We define \( h : \mathbb{Z}^+ \to \mathbb{Z}^+ \) by
\[
h(1) = 1, \quad h(2) = 4 \quad \text{and} \quad h(n) = h(n-1) + h(n-2)
\]
for all \( n \geq 3 \). \( \checkmark \) This is \( P(n) \)

Prove: \( \forall n \in \mathbb{Z}^+ \), \( \gcd(h(n), h(n+1)) = 1 \).

By simple induction
Base case: \( \gcd(h(1), h(2)) = \gcd(1, 4) = 1 \).

IH: Assume for some \( k \geq 1 \)
\[
\gcd(h(k), h(k+1)) = 1.
\]
Then \( k+2 \geq 3 \), so
\[
h(k+2) = h(k+1) + h(k).
\]
Thus,
\[
\gcd(h(k+1), h(k+2)) = \gcd(h(k+1), h(k+1) + h(k)) = \gcd(h(k+1), h(k)) \quad (\text{by problem } \#1)
\]
\[
= 1 \quad \text{by the IH}.
\]
Thus \( \forall k \in \mathbb{Z}^+ \), \( P(k) \to P(k+1) \) \( \land P(1) \)

So we conclude:
\[
\forall n \in \mathbb{Z}^+ \, P(n) \text{ holds.}
\]
3. (a) Let \( m, n \) be arbitrary positive integers and assume \( m < n \).
We consider cases:

(i) \( m \leq \frac{n}{2} \)

Because \( (n \mod m) < m \), we have \( (n \mod m) < \frac{n}{2} \).

(ii) \( m > \frac{n}{2} \).

Then \( (n \mod m) = n - m \)

\[
< n - \frac{n}{2} = \frac{n}{2}
\]

Because \( m \) in either case \( (n \mod m) < \frac{n}{2} \),
we conclude it holds for all positive integers \( m \) and \( n \) with \( m < n \).

(b). Let \( P(n) \) be:

For all natural numbers \( m \) such that \( m < n \),
\( \gcd(m, n) \) makes at most \( 2 \left\lceil \log_2 n \right\rceil \) recursive calls.

**Base case**

\( n = 1 \). The only natural number \( m \) that is less than \( n \) is \( m = 0 \), and
\( \gcd(0, 1) \) makes 0 recursive calls, and \( 0 \leq 2 \left\lceil \log_2 1 \right\rceil = 0 \).

**IH:** For some \( k \geq 1, P(1), P(2), \ldots, P(k) \) are true. Consider \( k + 1 \) and some natural number \( m < k + 1 \). Note that \( k + 1 \geq 2 \),
so \( 2 \left\lceil \log_2 (k+1) \right\rceil \geq 2 \).

(a) If \( m = 0 \), no recursive calls are made, and \( 0 \leq 2 \).
3(b), cont.

If \( m > 0 \) then a recursive call gcd\((r,m)\) is made, with \( r = (m+1 \mod m) \). Then \( 0 \leq r < m \), and by part (a), \( r < \frac{k+1}{2} \).

(b) If \( r = 0 \), then no more recursive calls are made, for a total of 1, and

\[
1 \leq 2 \leq 2 \lceil \log_2 (k+1) \rceil
\]

(c) If \( r > 0 \), then another recursive call is made with gcd\((s,r)\), where \( s = (m \mod r) \). Then \( 0 \leq s < r \).

Because \( r < \frac{k+1}{2} \) and \( k \geq 1 \), we have \( r \leq k \), so \( P(r) \) holds, by the Induction Hypothesis.

That is, gcd\((s,r)\) makes at most

\[
2 \lceil \log_2 r \rceil
\]

recursive calls. Thus, the total number of recursive calls for gcd\((k+1,m)\) is at most 2 more than this, or

\[
2 + 2 \lceil \log_2 r \rceil.
\]

Because \( r \leq \frac{k+1}{2} \), \( \log_2 r \leq \log_2 (k+1) - 1 \), and \( \lceil \log_2 r \rceil \leq \lceil \log_2 (k+1) \rceil - 1 \). Thus, the total number of recursive calls is at most:

\[
2 + 2 \lceil \log_2 (k+1) \rceil - 2 \leq 2 \lceil \log_2 (k+1) \rceil
\]

which shows \( P(k+1) \) holds in all three cases: (i), (ii), (iii), which concludes the Induction.
4(a)

(i) $n = 7$
$\{1, 2, 3, 4, 5, 6\}$

(ii) $n = 21$
$\{1, 2, 4, 5, 8, 10, 11, 13, 16, 17, 19, 20\}$

(iii) $n = 25$
$\{1, 2, 3, 4, 6, 7, 8, 9, 11, 12, 13, 14, 16, 17, 18, 19, 21, 22, 23, 24\}$

(b) \(\phi(pq) = (p-1)(q-1)\) \(\Leftarrow\) to be proved

There are \(q\) multiples of \(p\): \(p, 2p, 3p, \ldots, qp\)
There are \(p\) multiples of \(q\): \(q, 2q, 3q, \ldots, pq\)
And one multiple of both: \(pq\)
All other numbers are relatively prime to \(pq\), so
\(pq - p - q + 1 = (p-1)(q-1)\)

(c) \(\phi(p^2) = p(p-1)\).

There are \(p\) multiples of \(p\): \(p, 2p, \ldots, p^2\)
and all other numbers in the range are relatively prime to \(p\), so
\(p^2 - p = p(p-1)\)
5.
(a) inverse of 4 mod 27
\[\gcd(4, 27)\]
\[q = 6, r = 3 \quad 3 = 27 - 6 \cdot 4\]
\[\gcd(3, 4)\]
\[q = 1, r = 1 \quad 1 = 4 - 3\]
so \[1 = 4 -(27-6 \cdot 4)\]
\[= 7 \cdot 4 - 27\]
Thus 7 is the inverse of 4 mod 27:
\[7 \cdot 4 = 28 = 1 \pmod{27}\]

(b) inverse of 5 mod 16
\[\gcd(5, 16)\]
\[q = 3, r = 1 \quad 1 = 16 - 3 \cdot 5\]
Thus \[-3 = 13 \pmod{16}\] is the inverse of 5 mod 16:
\[13 - 5 = 65 = 1 \pmod{64}\]

(c) inverse of 8 mod 35
\[\gcd (8, 35)\]
\[q = 4, r = 3 \quad 3 = 35 - 4 \cdot 8\]
\[\gcd (3, 8)\]
\[q = 2, r = 2 \quad 2 = 8 - 2 \cdot 3\]
\[\gcd (2, 3)\]
\[q = 1, r = 1 \quad 1 = 3 - 2\]
so \[1 = 3 - (8 - 2 \cdot 3)\]
\[= 3 - 8\]
\[= 3/35 - 9 \cdot 8 - 0\]
\[= 3 - 13 - 8\]
Thus \[-13 = 22 \pmod{35}\] is the inverse of 8 mod 35:
\[22 \cdot 8 = 176 = 1 \pmod{35}\]
We find the GCD of the encryption exponent \( e = 23 \) as follows:

\[
\begin{align*}
11 & \mid 1080 \\
1 & \mid 92 \\
1 & \mid 160 \\
1 & \mid 188 \\
22 & \div 22 \\
\end{align*}
\]

\[
gcd(23, 1080) = 46, \quad r = 22
\]

\[
gcd(22, 23) = 1, \quad r = 1
\]

So the inverse of \( 23 \mod 1080 \) is:

\[
d = 47
\]

\[
23 \cdot 47 \equiv 1 \mod 1080
\]

We form the table of powers of \( 314 \) by repeated squaring:

\[
\begin{align*}
2 & \left( (314)^2 \mod 1147 \right) = 1101 \\
4 & \left( (1101)^2 \mod 1147 \right) = 969 \\
8 & \left( (969)^2 \mod 1147 \right) = 715 \\
16 & \left( (715)^2 \mod 1147 \right) = 810 \\
32 & \left( (810)^2 \mod 1147 \right) = 16
\end{align*}
\]

To find \( (314)^d \equiv (314)^{97} \mod 1147 \):

\[
5 \text{ multiplications } \mod 1147
\]

Because \( 47 = 32 + 8 + 4 + 2 + 1 \)

Thus, we can do 4 multiplications \mod 1147 to find the product \mod 1147:

\[
\begin{align*}
16 \cdot (715) \cdot (969) \cdot (1101) \cdot (314) & \mod 1147 \\
1117 & \mod 1147 \\
49 & \mod 1147 \\
965 & \mod 1147 \\
\end{align*}
\]

\[
(202) \equiv (149) \mod 1147
\]