1: Let $C$ be the circle of radius 1 centred at $(0, 1)$. Let $D$ be the circle of radius 2 centred at $(a, 2)$ where $a > 0$ and $D$ is externally tangent to $C$. Let $E$ be the circle of radius $r$ centred at $(x, 0)$ where $0 < x < a$ and $E$ is externally tangent to both $C$ and $D$. Find the values of $x$ and $r$.

Solution: The distance between the centres of two externally tangent circles is the sum of their radii. Applying this rule to the circles $C$ and $D$ gives $a^2 + 1^2 = (2 + 1)^2 = 9$, and so $a = 2\sqrt{2}$. Applying the rule to the circles $C$ and $E$ gives $x^2 + 1 = (1 + r)^2 = 1 + 2r + r^2$ and so $x^2 = 2r + r^2$. Applying the rule to the circles $D$ and $E$ gives $(a - x)^2 + 4 = (2 + r)^2$, and so $a^2 - 2ax + x^2 = 4r + r^2$. Put in $a = 2\sqrt{2}$ and $x^2 = 2r + r^2$ to get $8 - 4\sqrt{2}x + 2 + r^2 = 4r + r^2$, and so $4\sqrt{2}x = 8 - 2r$, that is $2\sqrt{2}x = 4 - r$. Square both sides to get $8x^2 = 16 - 8r + r^2$. Put in $x^2 = 2r + r^2$ to get $8(2r + r^2) = 16 - 8r + r^2$, and so $7r^2 + 24r - 16 = 0$ hence $(7r - 4)(r + 4) = 0$. Since $r > 0$ we must have $r = \frac{4}{7}$. Since $2\sqrt{2}x = 4 - r = \frac{24}{7}$, we have $x = \frac{6\sqrt{2}}{7}$.

2: Let $a_n$ be the $n^{\text{th}}$ positive integer $k$ such that $\lfloor \sqrt{k} \rfloor$ divides $k$. Find $n$ such that $a_n = 600$.

Solution: We have $\lfloor \sqrt{k} \rfloor = \ell$ when $\sqrt{k} - 1 < \ell \leq \sqrt{k}$, or equivalently when $\ell^2 - 1 < k < (\ell + 1)^2$. In this case, $\ell = \lfloor \sqrt{k} \rfloor$ divides $k$ when $k$ is a multiple of $\ell$ with $\ell^2 - 1 < k < (\ell + 1)^2$, that is when $k = \ell^2$, $k = \ell^2 + \ell$ or $k = \ell^2 + 2\ell = (\ell + 1)^2 - 1$. Thus the values of $k$ for which $\lfloor \sqrt{k} \rfloor$ divides $k$ are

$1^2, 1^2 + 1, 1^2 + 2, 2^2, 2^2 + 2, 2^2 + 4, 3^2, 3^2 + 3, 3^2 + 6, 4^2, 4^2 + 4, 4^2 + 8, 5^2, 5^2 + 5, 5^2 + 10, \ldots$

and so we have $a_{3m-2} = m^2$, $a_{3m-1} = m^2 + m$ and $a_{3m} = m^2 + 2m = (m + 1)^2 - 1$. Note that $24^2 = 576$ and $24^2 + 24 = 600$, so for $m = 24$ we have $600 = m^2 + m = a_{3m-1} = a_{71}$. Thus we can take $n = 71$ to get $a_n = 600$. 
3: A Mersenne prime is a prime of the form \( p = 2^k - 1 \) for some positive integer \( k \). For a positive integer \( n \), let \( \sigma(n) \) be the sum of the positive divisors of \( n \). Show that \( \sigma(n) \) is a power of 2 if and only if \( n \) is a product of distinct Mersenne primes.

Solution: When \( n = 1 \) we have \( \sigma(n) = 1 = 2^0 \) which (for convenience) we consider to be a product of zero Mersenne primes. Let \( n \geq 2 \), say \( n = \prod_{i=1}^\ell p_i^{m_i} \) where the \( p_i \) are distinct primes and \( m_i \geq 1 \). Recall (or show) that

\[
\sigma(n) = \prod_{i=1}^\ell (1 + p_i + p_i^2 + \cdots + p_i^{m_i}).
\]

If \( n \) is a product of distinct Mersenne primes then each \( m_i = 1 \) and each \( p_i \) is a Mersenne prime, say \( p_i = 2^{k_i} - 1 \), so we have \( \sigma(n) = \prod_{i=1}^\ell (1 + p_i) = \prod_{i=1}^\ell 2^{k_i} = 2^{k_1 + k_2 + \cdots + k_\ell} \).

Suppose, conversely, that \( \sigma(n) \) is a power of 2, say \( \sigma(n) = 2^k \). We need to show that each \( m_i = 1 \) and that each \( p_i \) is a Mersenne prime. Since \( \prod_{i=1}^\ell (1 + p_i + \cdots + p_i^{m_i}) = \sigma(n) = 2^k \) it follows, from unique factorization, that each term \((1 + p_i + \cdots + p_i^{m_i})\) is a power of 2, say

\[
(1 + p_i + \cdots + p_i^{m_i}) = 2^{\ell_i}.\]

It suffices to show that each \( m_i = 1 \) since this implies \( 1 + p_i = 2^{\ell_i} \) so that each \( p_i \) is a Mersenne prime. Suppose, for a contradiction, that \( m_i \geq 2 \). Note that \( p_i \) is odd since if \( p_i \) was even then \( 1 + p_i + \cdots + p_i^{m_i} \) would be odd. Note that \( m_i \) must be odd since if \( m_i \) was even then \( 1 + p_i + \cdots + p_i^{m_i} \) would be odd. Let \( m_i = 2\ell_i + 1 \) and note that \( \ell_i \geq 1 \). Thus we have

\[
2^{\ell_i} = (1 + p_i + p_i^2 + \cdots + p_i^{2\ell_i + 1}) = (1 + p_i)(1 + p_i^2 + p_i^4 + \cdots + p_i^{2\ell_i})
\]

and so \( 1 + p_i \) and \( 1 + p_i^2 + \cdots + p_i^{2\ell_i} \) are both powers of 2. Note that \( \ell_i \) must be odd since if \( \ell_i \) was even then \( 1 + p_i^2 + p_i^4 + \cdots + p_i^{2\ell_i} \) would be odd. Let \( \ell_i = 2r_i + 1 \) and note that \( r_i \geq 0 \). Then

\[
2^{\ell_i} = (1 + p_i)(1 + p_i^2 + \cdots + p_i^{2r_i + 1}) = (1 + p_i)(1 + p_i^2)(1 + p_i^4 + \cdots + p_i^{4r_i}).
\]

Thus \( (1 + p_i^2) \) is a power of 2. But this is not possible, since \( p_i \neq 2 \) and \( p_i \) is odd so that \( p_i^2 + 1 = 2 \mod 4 \).

4: Let \( \{a_n\} \) be a sequence of positive real numbers such that \( \sum_{n=1}^{\infty} a_n < \infty \). Show that there exists a sequence \( \{c_n\} \) of positive real numbers with \( \lim_{n \to \infty} c_n = \infty \) such that \( \sum_{n=1}^{\infty} c_n a_n < \frac{1}{2} \).

Solution: Let \( S = \sum_{n=1}^{\infty} a_n \). Recall (or show) that for all \( \epsilon > 0 \) there exists \( m \in \mathbb{Z}^+ \) such that \( \sum_{n=m+1}^{\infty} a_n < \epsilon \).

For each \( 0 \leq \ell \in \mathbb{Z} \) choose \( m_\ell \) with \( 1 = m_0 < m_1 < m_2 < m_3 < \cdots \) such that \( \sum_{n=m_\ell}^{\infty} a_n < \frac{\epsilon}{4^{\ell}} \). For all \( n \in \mathbb{Z}^+ \) with \( m_{\ell-1} \leq n < m_\ell \), let \( c_n = \frac{\ell-3}{S} \). Then

\[
\sum_{n=1}^{\infty} c_n a_n = \sum_{n=1}^{m_1-1} c_n a_n + \sum_{n=m_1}^{m_2-1} c_n a_n + \sum_{n=m_2}^{m_3-1} c_n a_n + \sum_{n=m_3}^{m_4-1} c_n a_n + \cdots
\]

\[
= \sum_{n=1}^{m_1-1} \frac{1}{4} a_n + \sum_{n=m_1}^{m_2-1} \frac{1}{4^{2}} a_n + \sum_{n=m_2}^{m_3-1} \frac{1}{4^{3}} a_n + \sum_{n=m_3}^{m_4-1} \frac{1}{4^{4}} a_n + \cdots
\]

\[
= \frac{1}{4} m_1 - 1 \sum_{n=1}^{m_1} a_n + \frac{1}{4^{2}} \sum_{n=m_1}^{m_2} a_n + \frac{1}{4^{3}} \sum_{n=m_2}^{m_3} a_n + \frac{1}{4^{4}} \sum_{n=m_3}^{m_4} a_n + \cdots
\]

\[
< \frac{1}{4} \sum_{n=1}^{m_1} a_n + \frac{1}{4^{2}} \sum_{n=m_1}^{m_2} a_n + \frac{1}{4^{3}} \sum_{n=m_2}^{m_3} a_n + \frac{1}{4^{4}} \sum_{n=m_3}^{m_4} a_n + \cdots
\]

\[
= \frac{1}{4} \cdot S + \frac{1}{4^{2}} \cdot S + \frac{1}{4^{3}} \cdot S + \frac{1}{4^{4}} \cdot S + \cdots = \frac{S}{4}.
\]
5: Find the minimum possible value of \( f'(2) \) given that \( f(x) \) is a polynomial with nonnegative real coefficients such that \( f(1) = 1 \) and \( f(2) = 3 \).

Solution: When \( \text{deg}(f) = 0 \) we cannot have \( f(1) = 1 \) and \( f(2) = 3 \). When \( \text{deg}(f) = 1 \), to get \( f(1) = 1 \) and \( f(2) = 3 \) we must have \( f(x) = 2x - 1 \), but then the coefficients of \( f(x) \) are not all nonnegative. Let

\[
f(x) = \sum_{k=0}^{n} a_k x^k = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n
\]

where \( n \geq 2 \) and each \( a_k \geq 0 \). We have \( f(1) = 2 \) and \( f(2) = 3 \) when

\[
a_0 + a_1 + a_2 + a_3 + \cdots + a_n = 1 \tag{1}
\]

\[
a_0 + 2a_1 + 4a_2 + 8a_3 + \cdots + 2^n a_n = 3 \tag{2}
\]

Subtract (1) from (2) to get

\[
a_1 + 3a_2 + 7a_3 + \cdots + (2^n - 1)a_n = 2 \tag{3}
\]

and subtract (3) from (1) to get

\[
a_0 - 2a_2 - 6a_3 - \cdots - (2^n - 2)a_n = -1 \tag{4}
\]

then rewrite equations (3) and (4) as

\[
a_1 = 2 - 3a_2 - 7a_3 - \cdots - (2^n - 1)a_n \tag{5}
\]

\[
a_0 = -1 + 2a_2 + 6a_3 + \cdots + (2^n - 2)a_n \tag{6}
\]

From (6) we see that since \( a_0 \geq 0 \) we must have \( 2a_2 + 6a_3 + 14a_4 + \cdots + (2^n - 2)a_n \geq 0 \geq 1 \), that is

\[
a_2 + 3a_3 + 7a_4 + \cdots + (2^{n-1} - 1)a_n \geq \frac{1}{2} \tag{7}
\]

Also, we have

\[
f'(x) = \sum_{k=1}^{n} ka_k x^{k-1} = a_1 + 2a_2 x + 3a_3 x^2 + \cdots + na_n x^n,
\]

and so

\[
f'(2) = a_1 + 4a_2 + 12a_3 + \cdots + n2^{n-1}a_n
\]

\[
= (2 - 3a_2 - 7a_3 - \cdots - (2^n - 1)a_n) + 4a_2 + 12a_3 + \cdots + n2^{n-1}a_n, \text{ by (5)}
\]

\[
= 2 + a_2 + 5a_3 + \cdots + (n2^{n-1} - 2^n + 1)a_n
\]

\[
= 2 + a_2 + 5a_3 + \cdots + ((n - 2)2^{n-1} + 1)a_n
\]

\[
\geq 2 + a_2 + 3a_3 + \cdots + (2^{n-1} - 1)a_n
\]

\[
\geq 2 + \frac{1}{2} = \frac{5}{2}.
\]

Note that equality can be attained by choosing \( a_2 = \frac{1}{2} \) and \( a_k = 0 \) for \( k \geq 3 \) then using (5) and (6) to get \( a_1 = \frac{1}{2} \) and \( a_0 = 0 \). Indeed when \( f(x) = \frac{1}{2} x + \frac{1}{4} x^2 \), we have \( f'(x) = \frac{1}{2} + x \), \( f(1) = 1 \), \( f(2) = 3 \) and \( f'(2) = \frac{5}{2} \).
6: Let $a_0 = a_1 = 1$ and let $a_{2n} = a_{n-1} + a_n$ and $a_{2n+1} = a_n$ for $n \geq 1$. Define $f : \mathbb{Z}^+ \to \mathbb{Q}^+$ by $f(n) = \frac{a_n}{a_{n-1}}$. Show that $f$ is bijective.

Solution: First we note that $f(1) = \frac{a_1}{a_0} = 1$ and for $k \geq 1$ we have

$$f(2k) = \frac{a_{2k}}{a_{2k-1}} = \frac{a_{k-1} + a_k}{a_{k-1}} = 1 + \frac{a_k}{a_{k-1}} = 1 + f(k),$$

and

$$f(2k + 1) = \frac{a_{2k+1}}{a_{2k}} = \frac{a_k}{a_k + a_{k-1}} = \frac{1}{1 + \frac{a_k}{a_{k-1}}} = \frac{1}{1 + f(k)}$$

and, in particular, $f(2k) > 1$ and $f(2k + 1) < 1$. Suppose, for a contradiction, that $f$ is not injective. Let $n$ be the smallest positive integer such that $f(n) = f(m)$ for some $m > n$. We cannot have $n = 1$ since when $m > 1$ is even we have $f(m) > 1$ and when $m > 1$ is odd we have $f(m) < 1$. If $n$ is even then $m$ must also be even since $f(m) = f(n) > 1$, but if we let $n = 2k$ and $m = 2l$ then we have $f(n) = f(m) \implies f(2k) = f(2l) \implies 1 + f(k) = 1 + f(l) \implies f(k) = f(l)$, which contradicts the choice of $n$. If $n$ is odd then $m$ must also be odd since $f(m) = f(n) < 1$, but if we let $n = 2k + 1$ and $m = 2l + 1$ then we have $f(n) = f(m) \implies f(2k + 1) = f(2l + 1) \implies \frac{1}{1 + f(l)} = \frac{1}{1 + f(k)} \implies f(k) = f(l)$, which again contradicts the choice of $n$. Thus $f$ is injective.

It remains to show that $f$ is surjective. Let $m \in \mathbb{Z}^+$ and suppose, inductively, that for all $a, b \in \mathbb{Z}^+$ with $a < m$ and $b < m$ there exists $n \in \mathbb{Z}^+$ such that $f(n) = \frac{a}{b}$. Let $a, b \in \mathbb{Z}^+$ with $a \leq m$ and $b \leq m$. If $a < m$ and $b < m$ then, by the induction hypothesis, we can choose $n \in \mathbb{Z}^+$ such that $f(n) = \frac{a}{b}$. If $a = b = m$ then we can choose $n = 1$ to get $f(n) = 1 = \frac{a}{b}$. If $a = m$ and $b < m$ then $1 \leq a - b < m$, so, by the induction hypothesis, we can choose $k \in \mathbb{Z}^+$ such that $f(k) = \frac{a - b}{b}$ and then for $n = 2k$ we have $f(n) = f(2k) = 1 + f(k) = 1 + \frac{a - b}{b} = \frac{a}{b}$. Finally, if $a < m$ and $b = m$ then, by the induction hypothesis, we can choose $k \in \mathbb{Z}^+$ such that $f(k) = \frac{a}{b - n}$ and then for $n = 2k + 1$ we have $f(n) = f(2k + 1) = \frac{1}{1 + \frac{a}{b - n}} = \frac{1}{1 + \frac{a}{b - 2k}} = \frac{a}{b}$. It follows, by induction, that for all $a, b \in \mathbb{Z}^+$ there exists $n \in \mathbb{Z}^+$ such that $f(n) = \frac{a}{b}$, hence $f$ is surjective.
1: Let $C$ be the sphere of radius 1 centred at $(0, 1, 1)$. Let $D$ be the sphere of radius 2 centred at $(a, 2, 2)$ where $a > 0$ and $D$ is externally tangent to $C$. Let $E$ be the sphere of radius $r$ centred at $(x, r, r)$ where $0 < x < a$ and $E$ is externally tangent to both $C$ and $D$. Find the values of $x$ and $r$.

Solution: The distance between the centres of two externally tangent circles is the sum of their radii. Applying this rule to the circles $C$ and $D$ gives $a^2 + 2 \cdot 1^2 = (2 + 1)^2 = 9$, and so $a = \sqrt{7}$. Applying the rule to the circles $C$ and $E$ gives $x^2 + 2(1-r)^2 = (1+r)^2$ and so $x^2 = -1 + 6r - r^2$. Applying the rule to the circles $D$ and $E$ gives $(a-x)^2 + 2(1-r)^2 = (2+r)^2$, and so $a^2 - 2ax + x^2 = 4 + 12r - r^2$. Put in $a = \sqrt{7}$ and $x^2 = -1 + 6r - r^2$ to get $7 - 2\sqrt{7}x + (-1 + 6r - r^2) = -4 + 12r - r^2$, and so $2\sqrt{7}x = 10 - 6r$, that is $\sqrt{7}x = 5 - 3r$. Square both sides to get $7x^2 = 25 - 30r + 9r^2$. Put in $x^2 = -1 + 6r - r^2$ to get $7(-1 + 6r - r^2) = 25 - 30r + 9r^2$, and so $16r^2 - 72r + 32 = 0$ hence $2r^2 - 9r + 4 = 0$, that is $(2r-1)(r-4) = 0$. Thus either $r = \frac{1}{2}$ or $r = 4$. Also, since $\sqrt{7}x = 5 - 3r$ we have $x = \frac{5-3r}{\sqrt{7}}$. If we had $r = 4$ then we would have $x = \frac{5-12}{\sqrt{7}} = -\sqrt{7}$ which is not possible, since $x > 0$. Thus we must have $r = \frac{1}{2}$ and $x = \frac{5-\frac{3}{2}}{\sqrt{7}} = \frac{\sqrt{7}}{2}$.

2: Let $a_n$ be the $n^{th}$ positive integer $k$ such that $\left\lfloor \sqrt[k]{\ell} \right\rfloor$ divides $k$. Find $n$ such that $a_n = 600$.

Solution: Let us say that $k$ is allowable when $\left\lfloor \sqrt[k]{\ell} \right\rfloor$ divides $k$. We have $\left\lfloor \sqrt[k]{\ell} \right\rfloor = \ell$ when $\sqrt[k]{\ell} - 1 < \ell \leq \sqrt[k]{\ell}$, or equivalently when $\ell \leq \sqrt[k]{\ell} < \ell + 1$, or equivalently when $\ell^3 \leq k < (\ell+1)^3$. Since $\ell^3 + (3\ell+3)\ell = (\ell+1)^3 - 1$, the allowable values of $k$ with $\left\lfloor \sqrt[k]{\ell} \right\rfloor = \ell$ are $\ell^3, \ell^3 + \ell, \ell^3 + 2\ell, \cdots, \ell^3 + (3\ell+3)\ell$.

Thus for each $\ell \in \mathbb{Z}^+$, there are exactly $3\ell + 4$ allowable values of $k$ with $\left\lfloor \sqrt[k]{\ell} \right\rfloor = \ell$. The total number of allowable values of $k$ with $1 \leq k < 8^3$ is \( \sum_{\ell=1}^{7} (3\ell + 4) = 7 + 10 + 13 + 16 + 19 + 22 + 25 = 112. \)

Since $600 - 512 = 88 = 11 \cdot 8$, There are 12 more allowable values of $k$ with $8^3 = 512 \leq k \leq 600$, namely $8^3, 8^3 + 1, 8^3 + 2, \cdots, 8^3 + 11 \cdot 8 = 600$. Thus when $n = 112 + 12 = 124$ we have $a_n = 600$. 

Solutions to the Big E Problems, 2018
3: Define \( f : (1, \infty) \to \mathbb{R} \) by \( f(x) = \int_x^{x^2} \frac{dt}{\ln t} \). Find the range of \( f \).

Solution: We claim that \( f \) is increasing. Let \( g(u) = \int_u^x \frac{dt}{\ln t} \). By the Fundamental Theorem of Calculus, we have \( g'(u) = \frac{1}{\ln u} \). Since \( f(x) = \int_x^{x^2} \frac{dt}{\ln t} - \int_x^x \frac{dt}{\ln t} = g(x^2) - g(x) \), we have

\[
\begin{align*}
    f'(x) &= 2x g'(x^2) - g'(x) = 2x \frac{1}{\ln(x^2)} - \frac{1}{\ln x} = \frac{2x}{\ln x} - 1 = \frac{x-1}{\ln x}
\end{align*}
\]

and so \( f'(x) > 0 \) for all \( x > 1 \). Thus \( f \) is increasing, as claimed. Because \( f : (0, \infty) \to \mathbb{R} \) is increasing and continuous, it follows that the range of \( f \) is the interval \((a, b)\) where \( a = \lim_{x \to 1+} f(x) \) and \( b = \lim_{x \to \infty} f(x) \).

For all \( t \in [x, x^2] \) we have \( \ln t \leq \ln(x^2) = 2 \ln x \), hence \( \frac{1}{\ln t} \geq \frac{1}{2 \ln x} \), and so

\[
\begin{align*}
    f(x) &= \int_x^{x^2} \frac{dt}{\ln t} \geq \int_x^x \frac{dt}{2 \ln x} = \frac{x^2 - x}{2 \ln x}.
\end{align*}
\]

By l'Hospital's Rule, \( \lim_{x \to \infty} \frac{x^2 - x}{2 \ln x} = \lim_{x \to \infty} \frac{2x - 1}{2/x} = \lim_{x \to \infty} (x^2 - \frac{1}{2} x) = \infty \) and so \( b = \lim_{x \to \infty} f(x) = \infty \).

Make the substitution \( \ln t = u \), so that \( t = e^u \) and \( dt = e^u du \) to get \( f(x) = \int_x^{x^2} \frac{dt}{\ln t} = \int_{\ln x}^{2 \ln x} \frac{e^u}{u} du \).

When \( \ln x \leq u \leq 2 \ln x \) we have \( x \leq e^u \leq x^2 \), so for all \( x > 1 \)

\[
\begin{align*}
    f(x) &= \int_{\ln x}^{2 \ln x} \frac{e^u}{u} du \leq \int_{\ln x}^{2 \ln x} \frac{x^2}{u} du = \left[ x^2 \ln u \right]_{u=\ln x}^{2 \ln x} = x^2 \ln (\frac{2 \ln x}{\ln x}) = x^2 \ln 2
\end{align*}
\]

\[
\begin{align*}
    f(x) &= \int_{\ln x}^{2 \ln x} \frac{e^u}{u} du \geq \int_{\ln x}^{2 \ln x} \frac{x}{u} du = \left[ x \ln u \right]_{u=\ln x}^{2 \ln x} = x \ln (\frac{2 \ln x}{\ln x}) = x \ln 2.
\end{align*}
\]

Since \( x \ln 2 \leq f(x) \leq x^2 \ln 2 \) for all \( x > 1 \) and \( \lim_{x \to 1+} x \ln 2 = \ln 2 = \lim_{x \to \infty} x^2 \ln 2 \) it follows, from the Squeeze Theorem, that \( a = \lim_{x \to 1+} f(x) = \ln 2 \). Thus the range of \( f(x) \) is the interval \((\ln 2, \infty)\).
Let $p$ be a prime number, let $\mathbb{Z}_p$ be the field of integers modulo $p$, and let $M_3(\mathbb{Z}_p)$ be the ring of $3 \times 3$ matrices with entries in $\mathbb{Z}_p$. Find the number of functions $F : \mathbb{Z} \to M_3(\mathbb{Z}_p)$ such that $F(k+l) = F(k) + F(l)$ and $F(kl) = F(k)F(l)$ for all $k, l \in \mathbb{Z}$.

Solution: When $R$ is a ring, a function $F : \mathbb{Z} \to R$ such that $F(k+l) = F(k) + F(l)$ and $F(kl) = F(k)F(l)$ for all $k, l \in \mathbb{Z}$ is called a ring homomorphism. Recall (or prove) that the ring homomorphisms $F : \mathbb{Z} \to R$ are the maps of the form $F(k) = ka$ for some $a \in R$ with $a^2 = 1$. It follows that the number of ring homomorphisms $F : \mathbb{Z} \to M_3(\mathbb{Z}_p)$ is equal to the number of matrices $A \in M_3(\mathbb{Z}_p)$ with $A^2 = A$.

When $F$ is a field, a matrix $A \in M_n(F)$ such that $A^2 = A$ is called a projection matrix. Recall (or prove) that a projection matrix $A \in M_n(F)$ is determined by its image and its kernel and that we have $F^n = \text{Im}A \oplus \text{Ker}A$. It follows that the number of projection matrices $A \in M_n(F)$ with $\text{rank}(A) = r$ is equal to the number of pairs $(U, V)$ where $U$ and $V$ are subspaces of $F^n$ with $\dim(U) = r$ and $\dim(V) = n - r$ and $U \cap V = \{0\}$.

Let $F = \mathbb{Z}_p$. The number of $r$-dimensional subspaces $U \subseteq F^n$ is equal to $rac{p^n - 1)(p^n - p)(p^n - p^2)\cdots(p^n - p^{r-1})}{(p^r-1)(p^r-p)(p^r-p^2)\cdots(p^r-p^{r-1})}$ because to choose an independent set $\{u_1, u_2, \cdots, u_r\}$ there are $p^n - 1$ ways to choose $u_1 \in F^n \setminus \{0\}$, then $p^n - p$ ways to choose $u_2 \in F^n \setminus \text{Span}\{u_1\}$, then $p^n - p^2$ ways to choose $u_3 \in F^n \setminus \text{Span}\{u_1, u_2\}$ and so on, so the number of independent sets $\{u_1, u_2, \cdots, u_r\}$ is equal to $(p^n - 1)(p^n - p) \cdots (p^n - p^{r-1})$, and when $U = \text{Span}\{u_1, u_2, \cdots, u_r\}$, a similar argument shows that the number of different bases $\{v_1, v_2, \cdots, v_r\}$ for $U$ is equal to $(p^r - 1)(p^r - p) \cdots (p^r - p^{r-1})$. Another similar argument shows that, once we have chosen an $r$-dimensional subspace $U \subseteq F^n$, the number of $(n - r)$-dimensional subspaces $V \subseteq F^n$ with $U \cap V = \{0\}$ is equal to $rac{(p^n - p^r)(p^n - p^{r+1})\cdots(p^n - p^{n-1})}{(p^r-1)(p^r-p)(p^r-p^2)\cdots(p^r-p^{r-1})}$.

Letting $a_r$ be the number of projection matrices $A \in M_3(\mathbb{Z}_p)$ with $\text{rank}(A) = r$, the total number of projection matrices is

$$a_0 + a_1 + a_2 + a_3 = 1 + \frac{(p^3 - 1)}{(p-1)} \cdot \frac{(p^3 - p)(p^3 - p^2)}{(p^2 - 1)(p^2 - p)} + \frac{(p^3 - 1)(p^3 - p)}{(p^2 - 1)(p^2 - p)} \cdot \frac{(p^3 - p^2)}{(p-1)} + 1$$

$$= 1 + (p^2 + p + 1)p^2 + (p^2 + p + 1)p^2 + 1$$

$$= 2(p^4 + p^3 + p^2 + 1).$$
5: Let \( a_0 = a_1 = 1 \) and let \( a_{2n} = a_{n-1} + a_n \) and \( a_{2n+1} = a_n \) for \( n \geq 1 \). Define \( f : \mathbb{Z}^+ \to \mathbb{Q}^+ \) by \( f(n) = \frac{a_n}{a_{n-1}} \).

Show that \( f \) is bijective.

Solution: First we note that \( f(1) = \frac{a_1}{a_0} = 1 \) and for \( k \geq 1 \) we have

\[
f(2k) = \frac{a_{2k}}{a_{2k-1}} = \frac{a_{k-1} + a_k}{a_{k-1}} = 1 + \frac{a_k}{a_{k-1}} = 1 + f(k),
\]

and, in particular, \( f(2k) > 1 \) and \( f(2k+1) < 1 \). Suppose, for a contradiction, that \( f \) is not injective. Let \( n \) be the smallest positive integer such that \( f(n) = f(m) \) for some \( m > n \). We cannot have \( n = 1 \) since when \( m > 1 \) is even we have \( f(m) > 1 \) and when \( m > 1 \) is odd we have \( f(m) < 1 \). If \( n \) is even then \( m \) must also be even since \( f(m) = f(n) > 1 \), but if we let \( n = 2k \) and \( m = 2l \) then we have \( f(n) = f(m) = f(2k) = f(2l) = 1 + f(k) = 1 + f(l) \), which contradicts the choice of \( n \). If \( n \) is odd then \( m \) must also be odd since \( f(m) = f(n) < 1 \), but if we let \( n = 2k+1 \) and \( m = 2l+1 \) then we have \( f(n) = f(m) = f(2k+1) = f(2l+1) \), which again contradicts the choice of \( n \). Thus \( f \) is injective.

It remains to show that \( f \) is surjective. Let \( m \in \mathbb{Z}^+ \) and suppose, inductively, that for all \( a, b \in \mathbb{Z}^+ \) with \( a < m \) and \( b < m \) there exists \( n \in \mathbb{Z}^+ \) such that \( f(n) = \frac{a}{b} \). Let \( a, b \in \mathbb{Z}^+ \) with \( a \leq m \) and \( b \leq m \). If \( a \leq m \) and \( b < m \) then, by the induction hypothesis, we can choose \( n \in \mathbb{Z}^+ \) such that \( f(n) = \frac{a}{b} \). If \( a = b = m \) then we can choose \( n = 1 \) to get \( f(n) = 1 = \frac{a}{b} \). If \( a = m \) and \( b < m \) then \( 1 \leq a - b < m \), so, by the induction hypothesis, we can choose \( k \in \mathbb{Z}^+ \) such that \( f(k) = \frac{a}{b} \) and then for \( n = 2k \) we have \( f(n) = f(2k) = 1 + f(k) = 1 + \frac{a}{b} = \frac{a}{b} \). Finally, if \( a < m \) and \( b = m \) then, by the induction hypothesis, we can choose \( k \in \mathbb{Z}^+ \) such that \( f(k) = \frac{a}{b} \) and then for \( n = 2k+1 \) we have \( f(n) = f(2k+1) = 1 + \frac{a}{b} = \frac{a}{b} \). It follows, by induction, that for all \( a, b \in \mathbb{Z}^+ \) there exists \( n \in \mathbb{Z}^+ \) such that \( f(n) = \frac{a}{b} \), hence \( f \) is surjective.

6: Let \( n \in \mathbb{Z}^+ \) and let \( N = \{1, 2, 3, \ldots, n\} \). Let \( S \) be a set of subsets of \( N \) with the property that for all \( A, B \subseteq N \), if \( A \subseteq S \) and \( A \subseteq B \) then \( B \subseteq S \). Define \( f : [0, 1] \to \mathbb{R} \) by \( f(x) = \sum_{A \subseteq S} x^{|A|}(1-x)^{|N \setminus A|} \). Show that \( f \) is nondecreasing.

Solution: For \( A \subseteq S \) and \( x \in [0, 1] \), let \( R_A(x) \) be the rectangular box \( R_A(x) = \prod_{k=1}^n I_{A,k}(x) \) where \( I_{A,k}(x) \) is the interval

\[
I_{A,k}(x) = \begin{cases} [0, x] & \text{if } k \in A, \\ [x, 1] & \text{if } k \notin A. 
\end{cases}
\]

Note that when \( A, B \subseteq S \) with \( A \neq B \), the boxes \( R_A(x) \) and \( R_B(x) \) are disjoint (because when \( k \) lies in exactly one of the two sets \( A \) and \( B \), the intervals \( I_{A,k}(x) \) and \( I_{B,k}(x) \) are disjoint). It follows that

\[
f(x) = \sum_{A \subseteq S} x^{|A|}(1-x)^{|N \setminus A|} = \sum_{A \subseteq S} \text{Vol}(R_A(x)) = \text{Vol}(\bigcup_{A \subseteq S} R_A(x)).
\]

Let \( 0 \leq x \leq y \leq 1 \). We claim that \( \bigcup_{A \subseteq S} R_A(x) \subseteq \bigcup_{A \subseteq S} R_A(y) \). Let \( t = (t_1, t_2, \ldots, t_n) \in \bigcup_{A \subseteq S} R_A(x) \). Choose \( A \subseteq S \) such that \( t \in R_A(x) \). Since \( t \in R_A(x) \) we have \( t_k \in I_{A,k}(x) \) for all \( k \), that is \( t_k \in [0, x] \) when \( k \in A \) and \( t_k \in [x, 1] \) when \( k \notin A \), and hence \( A = \{k \in N \mid t_k < x\} \). Let \( B = \{k \in N \mid t_k < y\} \) so that \( t_k \in [0, y] \) when \( k \in B \) and \( t_k \in [y, 1] \) when \( k \notin B \). Since \( x \leq y \) we have \( A \subseteq B \). Since \( A \subseteq B \) and \( A \subseteq S \) we have \( B \subseteq S \). Since \( t_k \in [0, y] \) when \( k \in B \) and \( t_k \in [y, 1] \) when \( k \notin B \) we have \( t \in R_B(y) \). Since \( t \in R_B(y) \) and \( R_B(y) \subseteq \bigcup_{A \subseteq S} R_A(y) \) we have \( t \in \bigcup_{A \subseteq S} R_A(y) \). This shows that \( \bigcup_{A \subseteq S} R_A(x) \subseteq \bigcup_{A \subseteq S} R_A(y) \), as claimed. Thus \( f(x) = \text{Vol}(\bigcup_{A \subseteq S} R_A(x)) \leq \text{Vol}(\bigcup_{A \subseteq S} R_A(y)) = f(y) \)

and so \( f \) is nondecreasing, as required.