PRACTICE PROBLEMS: SET 3

MATH 437/537: PROF. DRAGOS GHIIOCA

1. PROBLEMS

Problem 1. Let $d, n \in \mathbb{N}$ such that $d \mid n$. Prove that if $d \neq n$, then
\[ d - \phi(d) < n - \phi(n). \]

Problem 2. Let $p \geq 5$ be a prime number. Let $a, b \in \mathbb{N}$ such that $\gcd(a, b) = 1$ and
\[ \sum_{i=1}^{p-1} \frac{1}{i} = \frac{a}{b}. \]
Prove that $p^2 \mid a$.

Problem 3. Let $m, n \in \mathbb{N}$ such that $m\phi(m) = n\phi(n)$. Prove that $m = n$.

Problem 4. Show that if $p$ is an odd prime number, then
\[ 1^2 \cdot 3^2 \cdots (p-4)^2 \cdot (p-2)^2 \equiv (-1)^{\frac{p+1}{2}} \pmod{p}. \]

Problem 5.
(i) Show that if $n$ is an odd positive integer, then $\phi(n) = \phi(2n)$.
(ii) Let $m$ be a positive integer such that $\gcd(m, 6) = 1$. Show that for each integer $a \geq 2$, we have
\[ \phi(2^a m) = \phi(2^{a-1} 3m). \]

Problem 6. Show that if $m \mid n$, then $\phi(m) \mid \phi(n)$.

Problem 7. Show that there is no positive integer $n$ such that $\phi(n) = 14$.

Problem 8. Show that if $n$ is an odd positive integer, then $\phi(n) \geq \sqrt{n}$.

Problem 9. Show that a positive integer $n$ is composite if and only if $\phi(n) \leq n - \sqrt{n}$.

Problem 10. Show that there exist arbitrarily long sequences of consecutive positive integers such that no integer in the sequence is a power of a prime number.

Problem 11. Find the number of solutions of the congruence
\[ x^2 \equiv x \pmod{m} \]
for each positive integer $m$.

Problem 12. Let $a, b, c \in \mathbb{N}$. If $\gcd(a, b) = 1$ prove that there exists $x \in \mathbb{N}$ such that $\gcd(a + bx, c) = 1$. 
Problem 13.
(a) Let \( n \in \mathbb{N} \). Prove that the equation \( \phi(n) = k \) has at most finitely many solutions \( n \in \mathbb{N} \).
(b) Let \( k \) be a positive integer. Show that if the equation \( \phi(n) = k \) has exactly one solution \( n \), then \( 36 \mid n \).

Problem 14. Let \( f \in \mathbb{Z}[x] \). For each \( m \in \mathbb{N} \), let \( N(m) \) be the number of solutions of the congruence equation \( f(x) \equiv 0 \pmod{m} \) and let \( \phi_f(m) \) be the number of \( a \in \{0, \ldots, m-1\} \) such that \( \gcd(f(a),m) = 1 \).

(i) Show that if \( \gcd(m,n) = 1 \), then \( \phi_f(mn) = \phi_f(m) \cdot \phi_f(n) \).
(ii) Show that if \( \alpha \in \mathbb{N} \) and if \( p \) is a prime number, then \( \phi_f(p^\alpha) = p^{\alpha-1} \cdot \phi_f(p) \).
(iii) Show that if \( p \) is a prime number, then \( \phi_f(p) = p - N(p) \).
(iv) Conclude that if \( n \in \mathbb{N} \), then
\[
\phi_f(n) = n \cdot \prod_{\substack{p \text{ prime} \\mid n}} \left(1 - \frac{N(p)}{p}\right).
\]

Problem 15. Let \( m \in \mathbb{N} \), and let \( a \in \mathbb{Z} \). Prove that
\[
a^m \equiv a^{m-\phi(m)} \pmod{m}.
\]

Problem 16. Find all positive integers \( n \) such that \( \phi(n) \mid n \).

Problem 17. Prove that for each positive rational number \( \frac{a}{b} \) there exist \( m, n \in \mathbb{N} \) such that
\[
\frac{a}{b} = \frac{\phi(m)}{\phi(n)}.
\]

Problem 18. Let \( n \geq 2 \) be an integer. Prove that each positive integer less than \( n! \) is a sum of at most \( (n-1) \) distinct divisors of \( n! \).

Problem 19. Let \( A = \{a^2 + ab + b^2 : a, b \in \mathbb{N}\} \) and let \( p \) be a prime number. Prove that if \( p^2 \in A \), then \( p \in A \).

Problem 20. An infinite arithmetic progression whose terms are integers contains a perfect square and a perfect cube. Show that the arithmetic progression also contains the sixth power of an integer.

Problem 21. Let \( n \) be an integer larger than 1, and let \( n \) positive integers satisfying the conditions:
\[
1 < a_1 < a_2 < \cdots < a_n < (2n - 1)^2
\]
and
\[
\gcd(a_i, a_j) = 1 \text{ if } i \neq j.
\]
Prove that there exists \( i \in \{1, \ldots, n\} \) such that \( a_i \) is prime.
2. Solutions

Problem 1. If \( d = 1 \), then \( d - \phi(d) = 1 - 1 = 0 \). On the other hand, since \( n \neq d \) (and \( n \) is a positive integer) we get that \( n \geq 2 \) in which case \( \phi(n) \leq n - 1 < n \) (since \( \phi(n) \) counts all the integers between 0 and \( n - 1 \) which are relatively prime with \( n \), and 0 is not relatively prime with \( n \), if \( n > 1 \)). Thus, if \( d = 1 \), the inequality holds.

So, from now on we assume that \( d \geq 2 \).

For each positive integer \( m \), we let

\[ S_m := \{ i : 0 \leq i \leq m - 1 \text{ and } \gcd(i, m) > 1 \} \]

Then \( |S_m| = m - \phi(m) \).

Since \( d \mid n \), if \( \gcd(i, d) > 1 \) then \( \gcd(i, n) > 1 \). Noting also that \( d \leq n \), we conclude that \( S_d \subset S_n \). But \( d \in S_n \) (since \( d \mid n \) and \( d \neq n \), while \( \gcd(d, n) = d > 1 \) by our assumption). On the other hand, \( d \notin S_d \) (by the definition of \( S_d \)). In conclusion, the set \( S_n \) is strictly larger than the set \( S_d \). Hence

\[ n - \phi(n) > d - \phi(d) \]

Problem 2. We group the first with the last fraction, the second with the next to the last fraction, i.e., in general:

\[ \frac{1}{i} + \frac{1}{p-i} = \frac{p}{i(p-i)} \]

for all \( i = 1, \ldots, p - 1 \). Therefore,

\[ \sum_{i=1}^{p-1} \frac{p}{i(p-i)} = \frac{2a}{b} \]

We will prove that if \( c, d \in \mathbb{N} \) such that \( \gcd(c, d) = 1 \) and

\[ \sum_{i=1}^{p-1} \frac{1}{i(p-i)} = \frac{c}{d} \]

then \( p \mid c \). This will suffice for deriving the desired conclusion. Indeed, we would then get

\[ \frac{pc}{d} = \frac{2a}{b} \]

and so, \( pc \cdot b = 2ad \), which yields \( p^2 \mid 2da \).

But \( p \nmid d \) (since \( p \mid d \) and \( \gcd(c, d) = 1 \)) and also \( p \nmid 2 \) (since \( p \geq 5 \)). Therefore we would obtain \( p^2 \mid a \), as desired.

So, we are left to prove that \( p \mid c \). For each \( i \in \{1, \ldots, p - 1\} \) there exists a unique inverse of \( i \) modulo \( p \), i.e., there exists a bijective function

\[ f : \{1, \ldots, p - 1\} \rightarrow \{1, \ldots, p - 1\} \]

such that \( f(i) \) is the inverse of \( i \) modulo \( p \). So,

\[ if(i) \equiv 1 \pmod{p} \]

and thus \( i^2f(i)^2 \equiv 1 \pmod{p} \).

Moreover, \( i(p-i)f(i)^2 \equiv -1 \pmod{p} \) (since \( p - i \equiv -i \pmod{p} \)). Hence

\[ -i(p-i)f(i)^2 \equiv 1 \pmod{p} \]

so, there exist (negative) integers \( m_i \), such that

\[ \frac{1}{i(p-i)} = \frac{-f(i)^2}{pm_i + 1} \]
Let \( N = \prod_{i=1}^{p-1} (pm_i + 1) \) and for each \( i \), we let \( N_i = N/(pm_i + 1) \). Since \( pm_i + 1 \equiv 1 \pmod{p} \) for each \( i \), we conclude that \( N \), and also each integer \( N_i \) is congruent to 1 modulo \( p \). Because

\[
\frac{c}{d} = \sum_{i=1}^{p-1} \frac{1}{i(p-i)} = -\sum_{i=1}^{p-1} \frac{f(i)^2N_i}{N},
\]

we already conclude that \( p \nmid d \) (since \( p \nmid N \) and also \( \gcd(c, d) = 1 \)). All we need to prove is that \( p \mid c \) which would follow if we could prove that

\[
p \mid \left( -\sum_{i=1}^{p-1} f(i)^2N_i \right).
\]

Because \( N_i \equiv 1 \pmod{p} \) for each \( i \), then we obtain that

\[
\sum_{i=1}^{p-1} f(i)^2N_i \equiv \sum_{i=1}^{p-1} f(i)^2 \equiv \sum_{i=1}^{p-1} i^2 \pmod{p},
\]

where in the last congruence we used the fact that the function \( f \) is a bijection on the set \( \{1, \ldots, p-1\} \). On the other hand,

\[
\sum_{i=1}^{p-1} i^2 = \frac{(p-1)p(2p-1)}{6}.
\]

Since \( p \geq 5 \), we obtain that \( \gcd(p, 6) = 1 \) and so, the integer \( \frac{(p-1)p(2p-1)}{6} \) must be divisible by \( p \). Thus

\[
p \mid \left( -\sum_{i=1}^{p-1} f(i)^2N_i \right)
\]

and hence \( p \mid c \) which yields \( p^2 \mid a \), as previously explained.

**Problem 3.** We let \( m = \prod_{i=1}^{r} p_i^{\alpha_i} \) and \( n = \prod_{j=1}^{s} q_j^{\beta_j} \) be the decomposition of \( m \), resp. \( n \) into a product of powers of primes. We allow for the possibility that either \( m \) or \( n \) equals 1 in which case \( r \) or \( s \) equal to 0. We will prove that \( m = n \) by induction on \( r + s \).

The base is \( r = s = 0 \) which automatically yields \( m = n = 1 \). Therefore we proved the base case of our induction. We assume now that we proved that \( m = n \) for all cases when \( r + s < k \) (for some integer \( k \geq 1 \)) and next we prove that also when \( r + s = k \), we get \( m = n \).

Indeed, we let \( p \) be the largest prime number which divides either \( m \) or \( n \). Without loss of generality, we may assume \( p = p_1 \). We claim that there exists \( j \in \{1, \ldots, s\} \) such that \( p = q_j \) (in this case we already know that \( s \geq 1 \) since otherwise \( n = 1 \) which would contradict the fact that \( m\phi(m) > 1 \)). Now, if \( q_j < p \) for all \( j = 1, \ldots, s \) (note that by our assumption, we already knew that \( p \geq q_j \) for each \( j \)), then also \( p > q_j - 1 \) for each \( j \), and thus

\[
p \nmid n\phi(n) = \prod_{j=1}^{s} 2^{\beta_j} - 1(q_j - 1),
\]

because \( p \) is a prime number larger than each prime factor from the above product. So, indeed, there exists \( j \) such that \( p = q_j \). Without loss of generality we may assume \( j = 1 \).
We claim that $\alpha_1 = \beta_1$. Indeed, otherwise we may assume (without loss of
generality) that $\alpha_1 > \beta_1$. So, $m\phi(m) = n\phi(n)$ yields
\[
\prod_{i=1}^{r} p_i^{2\alpha_i - 1}(p_i - 1) = \prod_{j=1}^{s} q_j^{2\beta_j - 1}(q_j - 1)
\]
and so,
\[
p^{2(\alpha_1 - \beta_1)} \prod_{i=2}^{r} p_i^{2\alpha_i - 1}(p_i - 1) = \prod_{j=2}^{s} q_j^{2\beta_j - 1}(q_j - 1).
\]
Moreover, now we know that $p > q_j$ for each $j = 2, \ldots, s$, and hence
\[
p \nmid \prod_{j=2}^{s} q_j^{2\beta_j - 1}(q_j - 1).
\]
This is a contradiction with the fact that $p \mid p^{2(\alpha_1 - \beta_1)} \prod_{i=2}^{r} p_i^{2\alpha_i - 1}(p_i - 1)$ (because
$\alpha_1 > \beta_1$). So, indeed $\alpha_1 = \beta_1$, which yields that
\[
\prod_{i=2}^{r} p_i^{2\alpha_i - 1}(p_i - 1) = \prod_{j=2}^{s} q_j^{2\beta_j - 1}(q_j - 1).
\]
More precisely, if we let $m_1 = \frac{m}{p_1}$ and $n_1 = \frac{n}{q_1}$, then
\[
m_{1,\phi(m)} = n_{1,\phi(n)}.
\]
But the number of prime factors for $m_1$ and $n_1$ is now $r - 1$, respectively $s - 1$, and thus by the inductive hypothesis we may conclude that $m_1 = n_1$. Because $p_1 = q_1$
and $\alpha_1 = \beta_1$, we get that also $m = n$, as desired.

**Problem 4.** We have
\[
(-1)^{\frac{r - 1}{2}} \cdot 1^2 \cdot 3^2 \cdots (p - 4)^2 \cdot (p - 2)^2
\equiv 1 \cdot (-1) \cdot 3 \cdot (-3) \cdots (p - 4) \cdot (-p + 4) \cdot (p - 2) \cdot (2 - p)
\equiv 1 \cdot (p - 1) \cdot 3 \cdot (p - 3) \cdots (p - 4) \cdot 4 \cdot (p - 2) \cdot 2
\equiv (p - 1)!
\equiv -1 \pmod{p},
\]
where the last congruence is Wilson’s Theorem. Therefore
\[
1^2 \cdot 3^2 \cdots (p - 4)^2 \cdot (p - 2)^2 \equiv (-1)^{\frac{r - 1}{2}} \pmod{p},
\]
as desired.

**Problem 5.**

(i) Because $n$ is odd, we have $\gcd(2, n) = 1$ and so, $\phi(2n) = \phi(2) \cdot \phi(n) = \phi(n)$.

(ii) Because $\gcd(2, m) = 1$, we have
\[
\phi(2^a m) = \phi(2^a) \cdot \phi(m) = 2^{a-1} \phi(m).
\]
Because $\gcd(2, 3) = \gcd(2, m) = \gcd(3, m) = 1$, we have
\[
\phi \left(2^{a-1} 3\right) = \phi(2^{a-1}) \phi(3) \phi(m) = 2^{a-1} \cdot 2 \cdot \phi(2) = 2^{a-1} \phi(m).
\]
In the above equalities we also used the fact that $a \geq 2$ which yields that
$2^{a-1}$ is a nontrivial power of 2, and thus $\phi(2^{a-1}) = 2^{a-2}$ (note that if $a = 1$, say, then $\phi(2^{a-1}) = \phi(1) = 1 \neq 2^{a-2}$).
This finishes the proof of part (ii).

**Problem 6.** Clearly the statement follows immediately for \( m = 1 \), and so we may assume \( m \geq 2 \). Let \( m = \prod_{i=1}^{r} p_i^{\alpha_i} \), where \( r \geq 1 \), for some distinct prime numbers \( p_i \) and also some exponents \( \alpha_i \geq 1 \). Since \( m \mid n \), then

\[
  n = n_1 \cdot \prod_{i=1}^{r} p_i^{\beta_i},
\]

where \( \gcd(n_1, m) = 1 \) and \( \beta_i \geq \alpha_i \) for each \( i = 1, \ldots, r \). In other words, \( n \) has to be divisible by each prime \( p_i \) at an exponent at least as large as the exponent of \( p_i \) in \( m \), and perhaps, \( n \) might be divisible also by other prime numbers different than the ones appearing in the prime factorization of \( m \) – this explains the integer \( n_1 \) which is relatively prime with \( m \).

We compute

\[
  \phi(n) = \phi(n_1) \cdot \prod_{i=1}^{r} \phi(p_i^{\beta_i})
  = \phi(n_1) \cdot \prod_{i=1}^{r} p_i^{\beta_i - 1}(p_i - 1)
  = \phi(n_1) \prod_{i=1}^{r} p_i^{\beta_i - \alpha_i} \cdot \prod_{i=1}^{r} p_i^{\alpha_i - 1}(p_i - 1)
  = \phi(n_1) \prod_{i=1}^{r} p_i^{\beta_i - \alpha_i} \phi(m),
\]

which proves indeed that \( \phi(m) \mid \phi(n) \).

**Problem 7.** Let \( n = p_1^{\alpha_1} \cdots p_k^{\alpha_k} \) be a positive integer (in its prime power decomposition) such that \( \phi(n) = 14 \). So,

\[
  p_1^{\alpha_1 - 1}(p_1 - 1) \cdots p_k^{\alpha_k - 1}(p_k - 1) = 14.
\]

Thus no prime \( p_i \) is larger than 13 because otherwise \( p_i - 1 > 14 \). However, if any of the primes \( p_i \) equals 13 or 7, then \( p_i - 1 \) (and so, \( \phi(n) \)) is divisible by 3, which is impossible as \( 3 \nmid 14 \). Also, no prime \( p_i \) can equal 11, because then \( 5 \mid \phi(n) \) which contradicts the fact that \( 5 \mid 14 \). Finally, no \( p_i \) can equal 5 because then \( 4 \mid \phi(n) \) which is impossible because \( 4 \nmid 14 \).

So, we conclude that the only primes which may divide \( n \) are 2 and 3. But then \( \phi(n) \) is only divisible by powers of 2 and 3 (also note that \( 3 - 1 = 2 \)), which contradicts the fact that \( 7 \mid 14 = \phi(n) \). Therefore, we conclude that there exists no positive integer \( n \) such that \( \phi(n) = 14 \).

**Problem 8.** If \( n = 1 \), then \( \phi(n) = \phi(1) = 1 = \sqrt{1} \). So, from now on, we assume \( n \) is an odd integer larger than 1.

Let \( n = p_1^{\alpha_1} \cdots p_k^{\alpha_k} \) be the prime power decomposition of \( n \). We know that each prime \( p_i \geq 3 \) (because \( n \) is odd). So,

\[
  \phi(n) = p_1^{\alpha_1 - 1}(p_1 - 1) \cdots p_k^{\alpha_k - 1}(p_k - 1),
\]
while
\[ \sqrt{n} = p_1^{\alpha_1} \cdots p_k^{\alpha_k}. \]

Therefore, it suffices to show that for each \( i = 1, \ldots, k \) we have
\[ p_i^{\alpha_i - 1}(p_i - 1) \geq p_i^{\alpha_i}. \]

Hence, our question is equivalent with showing that if \( p \geq 3 \) is a prime number, and if \( \alpha \geq 1 \) is an integer, then
\[ p^{\alpha - 1}(p - 1) \geq p^{\alpha}. \]

If \( \alpha \geq 2 \), then \( \frac{\alpha}{2} - 1 \geq 0 \), and so,
\[ \alpha - 1 \geq \frac{\alpha}{2}, \]
which immediately proves (1). So, assume from now on that \( \alpha = 1 \), which means that we have to prove that for \( p \geq 3 \), we have
\[ p - 1 \geq \sqrt{p}. \]

This is certainly true for \( p = 3 \) (because \( 2 > \sqrt{3} \)), while for \( p \geq 4 \), we have
\[ \sqrt{p} \geq 2 > \frac{1}{\sqrt{p}} + 1, \]
and so, \( \sqrt{p} - \frac{1}{\sqrt{p}} > 1 \). Multiplying this last inequality by \( \sqrt{p} \) yields
\[ p - 1 > \sqrt{p}, \]
as desired.

**Problem 9.** First we show that if \( n \) is not composite, then \( \phi(n) > n - \sqrt{n} \). Indeed, there are two types of non-composite positive integers \( n \): either \( n \) is a prime number, or \( n = 1 \). If \( n = 1 \), then
\[ \phi(1) = 1 > 0 = 1 - \sqrt{1}. \]

If \( n \) is a prime number, then \( \phi(n) = n - 1 > n - \sqrt{n} \) because \( \sqrt{n} > 1 \) (note that any prime number \( n \) is larger than one).

Secondly, we will show that if \( n \) is composite, then indeed
\[ \phi(n) \leq n - \sqrt{n}. \]

Inequality (2) is equivalent with showing that \( \sqrt{n} \leq n - \phi(n) \). Now, the function \( \phi(n) \) represents the number of nonnegative integers less than \( n \) which are relatively prime with \( n \). So, \( \sqrt{n} \leq n - \phi(n) \) is equivalent with showing that there are at least \( \sqrt{n} \) nonnegative integers less than \( n \) which share a common divisor larger than one with \( n \).

Now, because \( n \) is a composite integer, then \( n = ab \) for some integers \( a, b > 1 \). Without loss of generality, we may assume \( a \leq b \). Hence
\[ a^2 \leq ab = n, \]
which means that \( a \leq \sqrt{n} \).

Now we count the nonnegative integers less than \( n \) which are divisible by \( a \); there are \( \frac{n}{a} \) such integers (note that \( a \mid n \) and so, \( \frac{n}{a} \in \mathbb{N} \)). Because \( a \leq \sqrt{n} \), we get that there are at least
\[ \frac{n}{a} \geq \sqrt{n}. \]
nonnegative integers less than \( n \) which are divisible by \( a \), and so, each one of these integers is not relatively prime with \( n \). This concludes our proof.

**Problem 10.** Let \( k \in \mathbb{N} \); we have to find a positive integer \( n \) such that for each \( i = 1, \ldots, k \), \( n + i \) is not a power of a prime number.

Let \( p_1, \ldots, p_k \) be distinct prime numbers, and consider the system of congruences:

\[
\begin{align*}
    n &\equiv -1 + p_1 \pmod{p_1^2} \\
    n &\equiv -2 + p_2 \pmod{p_2^2} \\
    & \vdots \\
    n &\equiv -k + p_k \pmod{p_k^2}
\end{align*}
\]

Since the above moduli are relatively prime, we conclude by the Chinese Remainder Theorem that there exists a (unique) solution \( x_0 \) modulo \( P := \prod_{i=1}^{k} p_i^2 \). So, all solutions in integers for the above system are of the form \( x_0 + \ell P \) for \( \ell \in \mathbb{Z} \). We choose \( \ell_0 \in \mathbb{N} \) large enough so that \( n := x_0 + \ell P > P \). Then for each \( i = 1, \ldots, k \) the positive integer \( n + i \) is divisible by \( p_i \), but not by \( p_i^2 \). Furthermore,

\[ n + i > P \geq p_i^2, \]

which yields that \( n + i \) cannot be the power of a prime number. Indeed, if it were the power of a prime number, since \( p_i \mid n + i \) then \( n + i = p_i^{\alpha_i} \) for some \( \alpha_i \in \mathbb{N} \).

However, \( n + i > p_i^2 \) which yields that \( \alpha_i > 2 \) contradicting the fact that \( p_i^2 \nmid n + i \) (see the above congruence modulo \( p_i^2 \)).

Thus we found \( k \) distinct consecutive positive integers none of which being a power of a prime number.

**Problem 11.** If \( m = 1 \), clearly there exists a unique solution modulo 1 to our congruence which is also modulo 1. So, from now on, assume \( m \geq 2 \). We consider the prime factorization of \( m \):

\[ m = \prod_{i=1}^{r} p_i^{\alpha_i}, \]

where the \( p_i \)'s are distinct primes and \( \alpha_i \geq 1 \).

The congruence \( x^2 \equiv x \pmod{m} \) is equivalent with the following system of congruences:

\[
\begin{align*}
    x^2 &\equiv x \pmod{p_1^{\alpha_1}} \\
    x^2 &\equiv x \pmod{p_2^{\alpha_2}} \\
    & \vdots \\
    x^2 &\equiv x \pmod{p_r^{\alpha_r}}
\end{align*}
\]

Now, for each \( i = 1, \ldots, r \), the congruence equation

\[ x^2 \equiv x \pmod{p_i^{\alpha_i}} \]

yields

\[ p_i^{\alpha_i} \mid x(x - 1). \]

Now, \( \gcd(x, x - 1) = 1 \) which means that not both \( x \) and \( x - 1 \) could be divisible by \( p_i \). Therefore, either \( p_i^{\alpha_i} \mid x \) or \( p_i^{\alpha_i} \mid (x - 1) \). In conclusion, the congruence equation

\[ x^2 \equiv x \pmod{p_i^{\alpha_i}} \]

has precisely two solutions modulo \( p_i^{\alpha_i} \):

\[ x \equiv 0 \pmod{p_i^{\alpha_i}} \quad \text{and} \quad x \equiv 1 \pmod{p_i^{\alpha_i}}. \]
Now, the above analysis applies to each congruence equation from the above system of congruences. Since the moduli of those congruences are relatively prime, we conclude by the Chinese Remainder Theorem that there exist $2^r$ distinct solutions to the congruence
\[ x^2 \equiv x \pmod{m}. \]
Indeed, for each set of choices of either $x \equiv 0 \pmod{p_i^{a_i}}$ or $x \equiv 1 \pmod{p_i^{a_i}}$ (for $i = 1, \ldots, r$) we have then a unique solution for $x^2 \equiv x \pmod{m}$. Since there are $2^r$ possible choices, we are done.

**Problem 12.** Let $d = \gcd(a, c)$. If $d = 1$, then we may simply take $x = c$ and thus
\[ \gcd(a + bc, c) = \gcd(a, c) = 1. \]
So, from now on assume $d \geq 2$. Let $q_1, \ldots, q_r$ be all the distinct prime factors of $d$. Also, let \{\(p_1, \ldots, p_s\}\} be the (possibly empty set of) other prime factors of $c$ different from the $q_i$’s. We consider the following system of congruences:
\[
\begin{align*}
    x &\equiv 1 \pmod{q_1} \\
    x &\equiv 1 \pmod{q_2} \\
    \quad \quad \quad \cdots \\
    x &\equiv 1 \pmod{q_r} \\
    x &\equiv 0 \pmod{p_1} \\
    x &\equiv 0 \pmod{p_2} \\
    \quad \quad \quad \cdots \\
    x &\equiv 0 \pmod{p_s}
\end{align*}
\]
Since the moduli of the above congruences are all relatively prime we conclude, by the Chinese Remainder Theorem, that there exists a (unique) solution $x_0$ of the above system of congruences. So, all solutions in integers of the above system of congruences are of the form $x_0 + \ell N$, where
\[ N = \prod_{i=1}^r q_i \cdot \prod_{j=1}^s p_j. \]
Clearly (for $\ell$ sufficiently large), we may choose a solution $x \in \mathbb{N}$ for the above system of congruences. We claim that
\[ \gcd(a + bx, c) = 1. \]
In order to prove this, it suffices to prove that
\[ \gcd(a + bx, q_i) = 1 \text{ for all } i = 1, \ldots, r, \text{ and } \gcd(a + bx, p_j) = 1 \text{ for all } j = 1, \ldots, s. \]
Now, for each $i = 1, \ldots, r$, we have
\[ a + bx \equiv a + b \equiv b \not\equiv 0 \pmod{q_i}. \]
Indeed, we know that $a \equiv 0 \pmod{q_i}$ (since $q_i \mid d \mid a$) but because $\gcd(a, b) = 1$, then $b \not\equiv 0 \pmod{q_i}$ for each $i = 1, \ldots, r$.
Also, for each $j = 1, \ldots, s$ we have:
\[ a + bx \equiv a \not\equiv 0 \pmod{p_j}. \]
Indeed, $p_j$ is a prime factor of $c$ which does not appear in $\gcd(a, c)$ which means that $p_j \not\mid a$. This concludes our proof.

**Problem 13.**
(a) Let \( n \in \mathbb{N} \) such that \( \phi(n) = k \).

If \( p \) is a prime number larger than \( k + 1 \), then \( p \nmid n \). Indeed, otherwise,

\[
(p - 1) \mid \phi(n)
\]

which yields \( p - 1 \leq \phi(n) = k \); this is a contradiction with the assumption that \( p > k + 1 \).

Let \( p_1, \ldots, p_r \) be the finitely many prime numbers less than or equal to \( k + 1 \). For each \( i = 1, \ldots, r \), we let

\[
\alpha_i = 2 + \lceil \log_{p_i} k \rceil.
\]

We claim that the exponent of \( p_i \) in \( n \) is less than \( \alpha_i \). Indeed, if \( \exp_{p_i}(n) \geq \alpha_i \),

then because \( p_i^{\exp_{p_i}(n) - 1} \mid \phi(n) \), we would get

\[
k \geq p_i^{\alpha_i - 1} = p_i^{1 + \lceil \log_{p_i} k \rceil} > p_i^{\log_{p_i}(k)} = k,
\]

which is a contradiction. So, we proved that

\[
n = \prod_{i=1}^{r} p_i^{\beta_i},
\]

where \( 0 \leq \beta_i \leq \alpha_i - 1 \). Therefore, there are at most

\[
\prod_{i=1}^{r} \alpha_i \text{ possible solutions } n \text{ to the equation } \phi(n) = k.
\]

(b) Let \( k \in \mathbb{N} \), and assume \( n \) is the only positive integer satisfying \( \phi(n) = k \).

We need to prove that \( 36 \mid n \), which is equivalent with showing that both \( 4 \mid n \) and also \( 9 \mid n \).

We first prove that \( n \) is even. Indeed, if \( n \) were odd, then because \( \phi \) is a multiplicative function, i.e. \( \phi(ab) = \phi(a)\phi(b) \) whenever \( \gcd(a, b) = 1 \), we would get

\[
\phi(2n) = \phi(2)\phi(n) = \phi(n) = k.
\]

This would contradict the fact that \( n \) is the only solution to the equation \( \phi(x) = k \). So, \( 2 \mid n \); therefore there exists \( m \in \mathbb{N} \) such that \( n = 2m \). We claim that \( m \) is also even. Indeed, if \( m \) were odd, then again as before, we would have

\[
k = \phi(m) = \phi(2m) = \phi(2)\phi(m) = \phi(m);
\]

thus contradicting the uniqueness of \( n \) as a solution for \( \phi(x) = k \). So, \( m \) is even and hence \( 4 \mid n \).

Now, let \( a = \exp_2(n) \); as proved above, \( a \geq 2 \). Also, let \( n_1 \in \mathbb{N} \) such that \( n = 2^n n_1 \). If \( 3 \nmid n_1 \), then (since \( \gcd(2, 3) = \gcd(2, n_1) = \gcd(3, n_1) = 1 \)) we get

\[
\phi(2^n - 3n_1) = \phi(2^n)\phi(3)\phi(n_1) = 2^{n-2} \cdot 2 \cdot \phi(n_1) = 2^{n-1} \phi(n_1) = \phi(2^n n_1) = \phi(n) = k.
\]

This contradicts the uniqueness of \( n \) as a solution to \( \phi(x) = k \) and thus, we must have \( 3 \mid n_1 \). So, let \( n_1 = 3n_2 \). Now, if \( 3 \nmid n_2 \) then

\[
\phi(2^{n_2} n_2) = 2^a \phi(n_2) = 2^{a-1} \cdot 2 \cdot \phi(n_2) = \phi(2^a)\phi(3)\phi(n_2) = \phi(2^a 3n_2) = \phi(n) = k
\]
which again contradicts the uniqueness of $n$ as a solution for the equation $\phi(x) = k$. In conclusion $3 \mid n_2$ and so, $9 \mid n$.

Because $4 \mid n$ and $9 \mid n$, we obtain that $36 \mid n$.

**Problem 14.**

(i) Each $a \in \{0, \ldots, mn - 1\}$ is uniquely determined by $a_1 \in \{0, \ldots, m - 1\}$ and $a_2 \in \{0, \ldots, n - 1\}$ such that

$$a \equiv a_1 \pmod{m} \text{ and } a \equiv a_2 \pmod{n}.$$  

Indeed, the above statement is simply the Chinese Remainder Theorem. Furthermore, because $a \equiv a_1 \pmod{m}$ we have that $f(a) \equiv f(a_1) \pmod{m}$, while because $a \equiv a_2 \pmod{n}$ we have that $f(a) \equiv f(a_2) \pmod{n}$.

Now, the requirement that $\gcd(f(a), mn) = 1$ translates into

$$\gcd(f(a), m) = 1 \text{ and } \gcd(f(a), n) = 1,$$

which is thus equivalent to asking that

$$\gcd(f(a_1), m) = 1 \text{ and } \gcd(f(a_2), n) = 1.$$  

Therefore each $a \in \{0, \ldots, mn - 1\}$ satisfying $\gcd(f(a), mn) = 1$ corresponds to a unique pair

$$(a_1, a_2) \in \{0, \ldots, m - 1\} \times \{0, \ldots, n - 1\}$$

satisfying $\gcd(f(a_1), m) = 1$ and $\gcd(f(a_2), n) = 1$. In conclusion,

$$\phi_{f(mn)} = \phi_f(m)\phi_f(n).$$

(ii) Clearly, $\gcd(f(a), p^\alpha) = 1$ if and only if $\gcd(f(a), p) = 1$. So, for each $a \in \{0, \ldots, p^\alpha - 1\}$ we let $a_0 \in \{0, \ldots, p - 1\}$ be the unique integer such that $a \equiv a_0 \pmod{p}$. Clearly, to each $a_0 \in \{0, \ldots, p - 1\}$ there are precisely $p^{\alpha - 1}$ integers $a \in \{0, \ldots, p^\alpha - 1\}$ such that

$$a \equiv a_0 \pmod{p}.$$  

Indeed, $a$ is any of the integers $a_0 + \ell p$ for $\ell \in \{0, \ldots, p^{\alpha - 1} - 1\}$.

Now, $\gcd(f(a), p) = 1$ if and only if $\gcd(f(a_0), p) = 1$ since $f(a) \equiv f(a_0) \pmod{p}$ (due to (3)). So, indeed $\phi_f(p^\alpha) = p^{\alpha - 1}\phi_f(p)$.

(iii) For any $a \in \{0, \ldots, p - 1\}$ there are only two possibilities:

- either $\gcd(f(a), p) = 1$
- or $f(a) \equiv 0 \pmod{p}$.

Therefore $\phi_f(p) + N(p) = p$ which proves the desired claim.

(iv) If $n = 1$, then clearly $\phi_f(1) = 1$ since each integer is relatively prime with 1. Hence the formula holds in this case (note that the product is empty since there are no prime numbers dividing 1). So, from now on assume $n \geq 2$.

Let $n = \prod_{i=1}^{r} p_i^{\alpha_i}$ be the prime power factorization of $n$. Using part (i), we conclude that

$$\phi_f(n) = \prod_{i=1}^{r} \phi_f(p_i^{\alpha_i}).$$

Then using part (ii) we get

$$\phi_f(p_i^{\alpha_i}) = p_i^{\alpha_i - 1}\phi_f(p) = p_i^{\alpha_i} - \phi_f(p) \frac{\phi_f(p)}{p},$$
while using part (iii) we have

\[ (6) \quad \phi_f(p) = p - N(p). \]

Putting (4), (5) and (6) together we obtain

\[ \phi_f(n) = \prod_{i=1}^r p_i^{\alpha_i} \left(1 - \frac{N(p)}{p}\right), \]

as desired.

**Problem 15.** If \( m = 1 \) then the statement is vacuously true. So from now on assume \( m \geq 2 \).

Let \( m = \prod_{i=1}^r p_i^{\alpha_i} \) be the prime power factorization of \( m \). We have to prove that

\[ a^m \equiv a^{m-\phi(m)} \pmod{p_i^{\alpha_i}} \]

or, equivalently \( a^m \phi(m) (a^{\phi(m)} - 1) \equiv 0 \pmod{p_i^{\alpha_i}}, \)

for each \( i = 1, \ldots, r \).

**Case 1.** \( p_i \nmid a \)

Then \( \gcd(a, p_i^{\alpha_i}) = 1 \) and so, by Fermat’s Theorem we have

\[ a^{\phi(p_i^{\alpha_i})} \equiv 1 \pmod{p_i^{\alpha_i}}. \]

Since

\[ \phi(m) = \prod_{i=1}^r \phi(p_i^{\alpha_i}), \]

we conclude that

\[ a^{\phi(m)} \equiv \left(a^{\phi(p_i^{\alpha_i})}\right)^{\prod_{j \neq i} \phi(p_j^{\alpha_j})} \equiv 1 \pmod{p_i^{\alpha_i}}. \]

Therefore

\[ a^{m-\phi(m)} (a^{\phi(m)} - 1) \equiv 0 \pmod{p_i^{\alpha_i}}, \]

as desired.

**Case 2.** \( p_i | a \)

In this case we will prove that \( p_i^{\alpha_i} | a^{m-\phi(m)} \) which in turn will yield

\[ a^{m-\phi(m)} (a^{\phi(m)} - 1) \equiv 0 \pmod{p_i^{\alpha_i}}, \]

as desired. Now,

\[ \exp_{p_i} \left(a^{m-\phi(m)}\right) = (m - \phi(m)) \cdot \exp_{p_i}(a) \geq m - \phi(m), \]

because \( \exp_{p_i}(a) \geq 1 \) in this case. So, we have to prove that

\[ (7) \quad \alpha_i \leq m - \phi(m). \]

We have

\[ m - \phi(m) = m \cdot \left(1 - \prod_{i=j}^r \left(1 - \frac{1}{p_j}\right)\right) \geq m \left(1 - \left(1 - \frac{1}{p_i}\right)\right) = \frac{m}{p_i}. \]

So, in order to prove (7) it suffices to prove

\[ (8) \quad \frac{m}{p_i} \geq \alpha_i. \]
Clearly, $\frac{m}{p_i} \geq p_i^{\alpha_i-1}$, and thus in order to prove (8) it suffices to prove

$$p_i^{\alpha_i-1} \geq \alpha_i.$$  

Since $p_i \geq 2$ and $\alpha_i \geq 1$, inequality (9) follows from the following statement.

**Claim.** For each $k \in \mathbb{N}$ we have $2^k - 1 \geq k$.

**Proof of Claim.** The proof is immediate by induction on $k$. The case $k = 1$ is clear, and thus we assume that $2^{k-1} \geq k$ for some $k \geq 1$, and next we prove that also $2^k \geq k + 1$. Indeed,

$$2^k = 2 \cdot 2^{k-1} \geq 2k \geq k + 1,$$

because $k \geq 1$ (and in the above inequality we also used the inductive hypothesis). This concludes the proof of our **Claim**.

So, the above **Claim** establishes the validity of (9) which in turn finishes the proof of **Case 2**.

Since **Case 1** and **Case 2** cover all possibilities for $a$, we conclude that always

$$a^m \equiv a^{m - \phi(m)} \pmod{m}.$$

**Problem 16.** If $n = 1$ we get that indeed $\phi(1) \mid 1$. So, from now on assume $n \geq 2$. We let

$$n = \prod_{i=1}^{r} p_i^{\alpha_i}$$

be the prime power factorization of $n$. We assume $\phi(n) \mid n$; hence

$$\prod_{i=1}^{r} p_i^{\alpha_i-1}(p_i - 1) \mid \prod_{i=1}^{r} p_i^{\alpha_i},$$

which is equivalent with the following divisibility

$$\prod_{i=1}^{r} (p_i - 1) \mid \prod_{i=1}^{r} p_i.$$

Without loss of generality we may assume

$$p_1 < p_2 < \cdots < p_r.$$

Therefore, $p_1 - 1$ is not divisible by any of the primes $p_i$ (for $i = 1, \ldots, r$). So, in order for (10) to hold we need that $p_1 - 1 = 1$; hence $p_1 = 2$.

We note that if $n$ is a power of $2$, i.e., $r = 1$ and thus $n = 2^{\alpha_1}$ then indeed

$$\phi(n) = \phi(2^{\alpha_1}) = 2^{\alpha_1-1} \mid 2^{\alpha_1} = n.$$

Now assume $r \geq 2$. Then (10) yields

$$\prod_{i=2}^{r} (p_i - 1) \mid 2 \cdot \prod_{i=2}^{r} p_i.$$

Since $3 \leq p_2 < \cdots < p_r$ we note that $p_2 - 1$ is an integer larger than 1 which is not divisible by any of the primes $p_j$ for $j = 2, \ldots, r$. So,

$$(p_2 - 1) \mid 2$$

which automatically yields that $p_2 = 3$. We note that if $r = 2$ and thus $n = 2^{\alpha_1}3^{\alpha_2}$, then indeed

$$\phi(n) = \phi(2^{\alpha_1}3^{\alpha_2}) = 2^{\alpha_1}3^{\alpha_2-1} \mid 2^{\alpha_1}3^{\alpha_2} = n.$$
Now assume $r \geq 3$. Then (11) yields

$$\prod_{i=3}^{r} (p_i - 1) \mid 3 \cdot \prod_{i=3}^{r} p_i.$$  

Since $5 \leq p_3 < \cdots < p_r$ we note that $p_3 - 1$ is an integer larger than 3 which is not divisible by any of the primes $p_j$ for $j = 3, \ldots, r$. So,

$$(p_3 - 1) \mid 3,$$

which is impossible (since $p_3 \geq 5$). In conclusion, if $\phi(n) \mid n$, then either

$$n = 2^\alpha$$

with $\alpha \geq 0$

or

$$n = 2^\alpha 3^\beta$$

with $\alpha, \beta \geq 1$.

**Problem 17.** So, we let $a$ and $b$ in lowest terms. We let

$$a = \prod_{i=1}^{r} p_i^{\alpha_i}$$

and

$$b = \prod_{j=1}^{s} q_j^{\beta_j}$$

be the prime power expansions of $a$ and $b$ with the understanding that either $r$ or $s$ (or even both) could equal 0 (i.e., $a$, or $b$ or both equal 1). Since we may assume that $\gcd(a, b) = 1$ then we know that $p_i \neq q_j$ for each $i$ and $j$.

Then we let

$$m = \prod_{i=1}^{r} p_i^{\alpha_i + 1} \cdot \prod_{j=1}^{s} q_j$$

and

$$n = \prod_{i=1}^{r} p_i \cdot \prod_{j=1}^{s} q_j^{\beta_j + 1}.$$ 

It is immediate to see that

$$\frac{a}{b} = \frac{\phi(m)}{\phi(n)}.$$

**Problem 18.** It is immediate to verify the conclusion for $n = 2$ and $n = 3$; so assume from now on that $n \geq 4$. Consider the following sets of integers:

$$A_1 = \{0, 1, 2, \ldots, n - 1\}$$

$$A_2 = \{0, n, n \cdot 2, \ldots, n \cdot (n - 2)\}$$

$$A_3 = \{0, n(n - 1), n(n - 1) \cdot 2, \ldots, n(n - 1) \cdot (n - 1) \cdot (n - 3)\}$$

$$\ldots$$

$$A_i = \{0, n(n-1) \cdots (n-i+2), n(n-1) \cdots (n-i+2) \cdot 2, \ldots, n(n-1) \cdots (n-i+2)(n-i)\}$$

$$\ldots$$

$$A_{n-2} = \{0, n(n-1) \cdots 4, n(n - 1) \cdots 4 \cdot 2\}$$

$$A_{n-1} = \{0, n(n - 1) \cdots 3\}.$$ 

Each set $A_i$ has $(n + 1 - i)$ elements.
For finitely many sets $B_1, \ldots, B_t$ of real numbers we define

$$B_1 + B_2 + \cdots + B_t := \{b_1 + b_2 + \cdots + b_t : b_i \in B_i \text{ for each } i\}.$$

Then we check easily that

$$A_1 + A_2 = \{0, 1, \ldots, n(n-1) - 1\}$$

$$A_1 + A_2 + A_3 = \{0, 1, \ldots, n(n-1)(n-2) - 1\}$$

$$\cdots$$

$$A_1 + A_2 + \cdots + A_i = \{0, 1, \ldots, n(n-1)\cdots(n-i+1) - 1\}$$

$$\cdots$$

$$A_1 + A_2 + \cdots + A_{n-1} = \{0, 1, \ldots, n(n-1)\cdots2 - 1\}.$$

So, indeed, each positive integer less than $n!$ is a sum of $(n-1)$ integers, each one from a different set $A_i$ from above. Since for each $i$, the numbers in $A_i$ are either equal to 0, or they are a divisor of $n!$, we conclude that each positive integer less than $n!$ is a sum of at most $(n-1)$ divisors of $n!$.

**Problem 19.** Let $S = \{m \in \mathbb{N} : mp \in A\}$. Clearly, $S$ is nonempty because $p \in S$ (since $p^2 \in A$). So, let $m_0$ be the least element of $S$; we’ll prove that $m_0 = 1$.

Now, we know there exist $a_0, b_0 \in \mathbb{N}$ such that $m_0p = a_0^2 + a_0b_0 + b_0^2$. Because $a_0, b_0 \in \mathbb{N}$ and $m_0 \leq p$, then both $a_0^2 < p^2$ and also $b_0^2 < p^2$ which yields that $1 \leq a_0, b_0 \leq p - 1$. Assume $m_0 > 1$.

On the other hand, if $m_0 \mid a_0$ and $m_0 \mid b_0$ then $m_0^2 \mid a_0^2 + a_0b_0 + b_0^2$, and therefore $m_0^2 \mid m_0p$ which in turn yields $m_0 \mid p$ and because $m_0 > 1$ then $m_0 = p$. However then $p \mid a_0$ and $p \mid b_0$ which is a contradiction with $1 < a_0, b_0 \leq p - 1$. Thus not both $a_0$ and $b_0$ are divisible by $m_0$.

Let $a_1, b_1 \in \mathbb{Z}$ be the least (in absolute value) integers such that $a_0 \equiv a_1 \pmod{m_0}$ and $b_0 \equiv b_1 \pmod{m_0}$; in particular $|a_1|, |b_1| \leq \frac{m_0}{2}$. So,

$$a_1^2 + a_1b_1 + b_1^2 \equiv a_0^2 + a_0b_0 + b_0^2 \equiv 0 \pmod{m_0},$$

and also $0 < a_1^2 + a_1b_1 + b_1^2 < m_0^2$. Indeed, the right hand side inequality is immediate form the fact that $|a_1|, |b_1| \leq \frac{m_0}{2}$ and that $m_0 > 0$, while the left hand side inequality is a consequence of the fact that not both $a_1$ and $b_1$ equal 0 (since that would mean that both $a_0$ and $b_0$ are divisible by $m_0$ which was ruled out above). Indeed, note that in general

$$x^2 + xy + y^2 = \left(x + \frac{y}{2}\right)^2 + \frac{3y^2}{4} \geq 0,$$

with equality if and only if $y = 0$ and also $x = 0$. So, we conclude that

$$m_0 \mid a_1^2 + a_1b_1 + b_1^2,$$

and $0 < a_1^2 + a_1b_1 + b_1^2 < m_0^2$.

Thus there exists $m_1 \in \mathbb{N}$ with $m_1 < m_0$ such that $a_1^2 + a_1b_1 + b_1^2 = m_0m_1$. Now, multiplying this last equality with the original equality: $a_0^2 + a_0b_0 + b_0^2 = m_0p$ and also using the identity:

$$(x_1^2 + x_1y_1 + y_1^2)(x_2^2 + x_2y_2 + y_2^2) = (x_1y_2 - x_2y_1)^2 + (x_1y_2 - x_2y_1)(x_1x_2 + x_2y_1 + y_1y_2) + (x_1x_2 + x_2y_1 + y_1y_2)^2,$$

we conclude that

$$m_0^2m_1 = (a_0b_1 - a_1b_0)^2 + (a_0b_1 - a_1b_0)(a_0a_1 + a_1b_0 + b_0b_1) + (a_0a_1 + a_1b_0 + b_0b_1)^2.$$
But \( m_0 \mid a_0 b_1 - a_1 b_0 \) and also \( m_0 \mid a_0 a_2 + a_1 b_0 + b_0 b_1 \) since \( a_0 \equiv a_1 \pmod{m_0} \), \( b_0 \equiv b_1 \pmod{m_0} \) and \( a_0^2 + a_0 b_0 + b_0^2 \equiv 0 \pmod{m_0} \). So, we define the integers:

\[
a_2 := \frac{a_0 b_1 - a_1 b_0}{m_0} \quad \text{and} \quad b_2 := \frac{a_0 a_2 + a_1 b_0 + b_0 b_1}{m_0}.
\]

Now, if \( a_0 b_1 < a_1 b_0 \), we simply consider (by the same argument) the integers:

\[
a_2 := \frac{a_1 b_0 - a_0 b_1}{m_0} \quad \text{and} \quad b_2 := \frac{a_1 a_0 + a_0 b_1 + b_0 b_1}{m_0}.
\]

Either way, we have found integers \( a_2, b_2 \) such that \( pm_1 = a_2^2 + a_2 b_2 + b_2^2 \) and moreover \( a_2 \geq 0 \). If \(-a_2 \leq b_2 < 0 \) then we use that

\[
a_2^2 + a_2 b_2 + b_2^2 = (b_2)^2 + (a_2 + b_2)(-b_2) + (a_2 + b_2)^2,
\]

while if \( b_2 < -a_2 \) then we use that

\[
a_2^2 + a_2 b_2 + b_2^2 = (-a_2 - b_2)^2 + (-a_2 - b_2)a_2 + a_2^2,
\]

and so, replacing \( (a_2, b_2) \) by either \( (a_2 + b_2, -b_2) \) or by \( (-a_2 - b_2, a_2) \) we obtain that

\[
pm_1 = a_2 + a_2 b_2 + b_2^2,
\]

and \( a_2, b_2 \geq 0 \). Now, if \( a_2 = 0 \) (same analysis if \( b_2 = 0 \)) then \( pm_1 = b_2^2 \) and therefore \( p \mid b_2 \) and thus \( p \mid m_1 \) which contradicts the fact that \( 1 \leq m_1 < m_0 \leq p \).

In conclusion, \( m_1 \in S \); this contradicts the minimality of \( m_0 \). In conclusion, \( m_0 = 1 \) and so, \( p \in A \), as desired.

**Problem 20.** Let \( \{a + ir\}_{i \geq 0} \) be the arithmetic progression. According to the hypothesis, there exists some integers \( x_0, y_0, i, j \) such that

\[
x_0^2 = a + iv \quad \text{and} \quad y_0^3 = a + jv.
\]

In other words, for each prime power \( p^\alpha \) dividing \( r \), the two congruences

\[
x^2 \equiv a \pmod{p^\alpha} \quad \text{and} \quad y^3 \equiv a \pmod{p^\alpha}
\]

are solvable. In order to achieve our conclusion we have to prove that for each such prime power \( p^\alpha \) also the congruence equation

\[
z^6 \equiv a \pmod{p^\alpha}
\]

is solvable. That would mean, using the Chinese Remainder Theorem, that also the congruence equation

\[
z_0^6 \equiv a \pmod{r}
\]

is solvable and so there exists some integer \( m \) so that \( z_0^6 = a + mr \) (note that we may easily ensure that \( z_0^6 > a \) and thus \( m \in \mathbb{N} \) by simply replacing \( z_0 \) with another larger integer in the same congruence class modulo \( r \)).

So, in order to prove that the congruence equation

\[
z^6 \equiv a \pmod{p^\alpha}
\]

is solvable, we split our analysis into two cases:

**Case 1.** \( p \nmid a \)

In this case, we know that also \( p \nmid x_0 \) and \( p \nmid y_0 \). Therefore, there exists some integer \( z_0 \) such that

\[
z_0 y_0 \equiv x_0 \pmod{p^\alpha}.
\]

Then

\[
z_0^6 a^2 \equiv z_0^6 \cdot y_0^6 \equiv x_0^6 \equiv a^3 \pmod{p^\alpha}
\]
and thus $z_0^6 \equiv a \pmod{p^\alpha}$ since we can divide both sides of the above congruence by $a^2$ which is coprime with $p$. (Note that in the above congruences we used the fact that $y_3^3 \equiv a \pmod{p^\alpha}$ and $x_2^2 \equiv a \pmod{p^\alpha}$.)

**Case 2.** $p \mid a$

We replace $a$ by the corresponding residue class $a_0$ modulo $p^\alpha$ in \{0, ..., $p^\alpha - 1\}$. If $a_0 = 0$, then we simply choose $z_0 = 0$ and this solves the congruence equation $z_0^6 \equiv a \pmod{p^\alpha}$. So, assume from now on, that $1 \leq a_0 \leq p^\alpha - 1$.

Since $p \mid a$, we know that there exists some $\beta \in \{1, \ldots, \alpha - 1\}$ such that $p^\beta$ is the exact power of $p$ in $a_0$. Since the congruence equation $x_2^2 \equiv a_0 \pmod{p^\alpha}$ is solvable, then we obtain that $2 \mid \beta$. Indeed, if $p^\gamma$ is the power of $p$ in a minimal solution $x_1 \in \{0, \ldots, p^\alpha - 1\}$ of the above congruence, then $2\gamma = \beta$ (note that we use the fact that $\beta < \alpha$). Similarly, using the fact that the congruence equation $y_3^3 \equiv a_0 \pmod{p^\alpha}$ is solvable, we obtain that $3 \mid \beta$. Therefore $6 \mid \beta$; let $\beta = 6\beta_0$ for some positive integer. Hence the congruence equation

\[(13)\quad z_0^6 \equiv a_0 \pmod{p^\alpha}\]

is equivalent with the congruence equation

\[(14)\quad z_0^6 \equiv \frac{a_0}{p^\beta} \pmod{p^{\alpha-\beta}}\]

since once we found a solution $z_1$ to equation (14), then $z_1 \cdot p^{\beta_0}$ is a solution to equation (13). The advantage with equation (14) is that $\gcd\left(\frac{a_0}{p^\beta}, p\right) = 1$. Furthermore, knowing that

$$x_0^2 \equiv a_0 \pmod{p^\alpha}$$

we have that

$$x_0^2 \equiv \frac{a_0}{p^\beta} \pmod{p^{\alpha-\beta}}$$

is solvable. Similarly, the congruence equation

$$y_3^3 \equiv \frac{a_0}{p^\beta} \pmod{p^{\alpha-\beta}}$$

is also solvable. Moreover $a_1 := \frac{a_0}{p^\beta}$ is not divisible by $p$ and so, we are in **Case 1** above and conclude that the congruence equation (14) is indeed solvable. This means that also the congruence equation (13) is solvable, and we are done.

Using **Cases 1, 2** we get that we can solve all congruence equations

(15)

$$z_0^6 \equiv a \pmod{p^\alpha}$$

for each prime power $p^\alpha$ dividing $r$. Chinese Remainder Theorem finishes off the problem by finding a simultaneous solution to all of the above congruence equations (15).

**Problem 21.** Assume that each $a_i$ is not a prime number. For each $i = 1, \ldots, n$ let $p_i$ be the smallest prime number dividing $a_i$. Then by our assumption, $p_i^2 \leq a_i$ and thus

$$2 \leq p_i \leq 2n - 2.$$
However, between 2 and $2n - 2$ there are only $(n - 2)$ odd integers, and thus between 2 and $2n - 2$ there are at most $(n - 1)$ prime numbers (since at most one of them is even). Therefore, by the pigeonhole principle, there must be $i \neq j$ such that $p_i = p_j$. But then $\gcd(a_i, a_j) > 1$ which is a contradiction. In conclusion, at least one of the numbers $a_i$ is prime.