1. Problems

**Problem 1.** Let \( f : \mathbb{N} \rightarrow \mathbb{C} \) be a multiplicative function. Prove that the function \( F : \mathbb{N} \rightarrow \mathbb{C} \) defined by
\[
F(n) = \sum_{d|n} f(d)
\]
for each \( n \in \mathbb{N} \) is also a multiplicative function.

**Problem 2.** For each \( n \in \mathbb{N} \), let \( \sigma(n) \) be the sum of all positive divisors of \( n \).

(i) Prove that \( \sigma : \mathbb{N} \rightarrow \mathbb{N} \) is a multiplicative function.

(ii) Prove that for each prime number \( p \) and for each \( \alpha \in \mathbb{N} \),
\[
\sigma(p^\alpha) = \frac{p^{\alpha+1} - 1}{p - 1} - 1.
\]

(iii) Prove that if \( \prod_{i=1}^r p_i^{\alpha_i} \) is the factorization of \( n \) into a product of powers of primes, then
\[
\sigma(n) = \prod_{i=1}^r \frac{p_i^{\alpha_i+1} - 1}{p_i - 1}.
\]

**Problem 3.** If \( n \in \mathbb{N} \) has the property that \( \sigma(n) = 2n \), then \( n \) is called a perfect number. Prove that if \( k \in \mathbb{N} \) has the property that \( 2^{k+1} - 1 \) is a prime number, then \( n = 2^k \cdot (2^{k+1} - 1) \) is a perfect number.

**Problem 4.** If \( n \in \mathbb{N} \) is an even perfect number, then there exists \( k \in \mathbb{N} \) such that \( (2^{k+1} - 1) \) is a prime number, and
\[
n = 2^k \cdot (2^{k+1} - 1).
\]

**Problem 5.** Let \( p \) and \( q \) be two distinct odd prime numbers, and let \( a, b \in \mathbb{N} \). Show that \( p^aq^b \) is not a perfect number.

**Problem 6.** Let \( k \in \mathbb{N} \), let \( a_0, a_1, \ldots, a_k \in \mathbb{R} \) with \( a_k \neq 0 \). If \( f : \mathbb{N} \rightarrow \mathbb{R} \) given by
\[
 f(n) = a_k n^k + a_{k-1} n^{k-1} + \cdots + a_1 n + a_0
\]
is a multiplicative function, show that \( a_k = 1 \), and that \( a_i = 0 \) for \( 0 \leq i < k \).

**Problem 7.** Show that \( \sigma(mn) < \sigma(m) \cdot \sigma(n) \) for all positive integers \( m \) and \( n \) which are not relatively prime.

**Problem 8.** Show that there is no perfect number \( n \) which is of the form \( pqr \), where \( p, q \) and \( r \) are distinct prime numbers.
Problem 9. Prove that for each \( n \in \mathbb{N} \), we have
\[
\sum_{d \mid n} \phi(d) = n.
\]

Problem 10.
(i) Prove that there are infinitely many prime numbers of the form \( 3n + 1 \), with \( n \in \mathbb{N} \).
(ii) Prove that there are infinitely many prime numbers of the form \( 3n + 2 \), with \( n \in \mathbb{N} \).

Problem 11. For each positive integer \( n \), let \( \omega(n) \) be the number of distinct prime factors of \( n \). We define the Möbius function \( \mu : \mathbb{N} \rightarrow \mathbb{Z} \) by
\[
\mu(n) = \begin{cases} 
(-1)^{\omega(n)} & \text{if } n \text{ is square-free} \\
0 & \text{otherwise}
\end{cases}
\]
for each \( n \in \mathbb{N} \). Prove that \( \mu \) is a multiplicative function and that for each \( n \in \mathbb{N} \),
\[
\sum_{d \mid n} \mu(d) = \begin{cases} 
1 & \text{if } n = 1 \\
0 & \text{if } n > 1
\end{cases}.
\]

Problem 12. Let \( f : \mathbb{N} \rightarrow \mathbb{C} \) and \( F : \mathbb{N} \rightarrow \mathbb{C} \).
(i) Prove that if for each \( n \in \mathbb{N} \),
\[
F(n) = \sum_{d \mid n} f(d),
\]
then for each \( n \in \mathbb{N} \), we have
\[
f(n) = \sum_{d \mid n} \mu(d) F\left(\frac{n}{d}\right).
\]
(ii) Prove that if for each \( n \in \mathbb{N} \),
\[
f(n) = \sum_{d \mid n} \mu(d) F\left(\frac{n}{d}\right),
\]
then for each \( n \in \mathbb{N} \), we have
\[
F(n) = \sum_{d \mid n} f(d).
\]

Problem 13. Let \( f : \mathbb{N} \rightarrow \mathbb{C} \), and let \( F : \mathbb{N} \rightarrow \mathbb{C} \) such that
\[
F(n) = \sum_{d \mid n} f(d),
\]
for each \( n \in \mathbb{N} \). Prove that if \( F \) is multiplicative, then \( f \) is multiplicative.

Problem 14. Let \( m > 1 \) be an odd integer, and let \( a \in \mathbb{Z} \) such that \( \gcd(a, m) = 1 \). Show that the number of solutions to the congruence equation \( x^2 \equiv a \pmod{m} \) is
\[
\prod_{\substack{p \mid m \\text{prime}}} \left( 1 + \left(\frac{a}{p}\right) \right).
\]
Problem 15.

(i) Let \( p \) be an odd prime number, and assume there exists \( x \in \mathbb{Z} \) such that \( p \mid (x^4 + 1) \). Prove that \( p \equiv 1 \pmod{8} \).

(ii) Prove that there exist infinitely many prime numbers \( p \) such that \( p \equiv 1 \pmod{8} \).

Problem 16. Let \( p \) be a prime number and let \( a, b, c \in \mathbb{N} \) such that

\[
ab^2 \equiv c^2 \pmod{p}.
\]

Show that if \( \left( \frac{a}{p} \right) = -1 \), then

\[
b^2 \equiv c^2 \pmod{p^2}.
\]

Problem 17. For any positive integer \( n \) prove that \( \phi(n) + \sigma(n) \geq 2n \), with equality if and only if \( n = 1 \) or \( n \) is a prime.

Problem 18. If \( a \) and \( b \) are positive integers such that \( a \mid b \) then prove that

\[
2^a - 1 \mid 2^b - 1.
\]

Problem 19. Let \( p \) be a prime number satisfying \( p \equiv 3 \pmod{4} \). Prove that for each \( a \in \mathbb{Z} \), there exist \( x, y \in \mathbb{Z} \) such that \( x^4 + y^4 \equiv a \pmod{p} \).

Problem 20. Let \( a_0, a_1, \ldots, a_n \in \mathbb{Z} \) such that \( |a_0| \) is a prime number, and \( |a_0| > |a_1| + \cdots + |a_n| \). Prove that

\[
a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0
\]

is irreducible, i.e. there exist no nonconstant polynomials \( g, h \in \mathbb{Z}[x] \) such that \( f = g \cdot h \).

Problem 21. Let \( n \) be a positive integer. Show that \( 2^n + 1 \) has no prime factor \( p \) satisfying \( p \equiv 7 \pmod{8} \).

Problem 22. Let \( P \in \mathbb{Z}[x] \) be a polynomial of degree \( n > 1 \). Let \( r \in \mathbb{N} \) and \( x_0, a_1, a_2, \ldots, a_r \in \mathbb{Z} \) such that for each \( i = 1, \ldots, r \) we have \( P(a_i) = x_0 + i \). Find with proof the largest value of \( r \).
2. Solutions

Problem 1. We start with the following easy lemma.

Lemma 2.1. If \( m, n \in \mathbb{N} \) such that \( \gcd(m, n) = 1 \), then each positive divisor \( d \) of \( mn \) can be uniquely written as \( d_1 \cdot d_2 \), where \( d_1 \mid m \) and \( d_2 \mid n \).

Proof. Indeed, we let \( d_1 = \gcd(d, m) \) and \( d_2 = \gcd(d, n) \). Since \( \gcd(m, n) = 1 \) we get that \( \gcd(d_1, d_2) = 1 \). Because both \( d_1 \mid d \) and \( d_2 \mid d \), we obtain that \( (d_1 \cdot d_2) \mid d \).

Now, since \( d \mid m \cdot n \), and \( d_2 \mid d \) and also \( d_2 \mid n \), we get that

\[
\frac{d}{d_2} \mid m \cdot \frac{n}{d_2}.
\]

Moreover, \( \gcd\left(\frac{d}{d_2}, \frac{n}{d_2}\right) = 1 \), which yields that

\[
\frac{d}{d_2} \mid m.
\]

Since \( d_1 \mid \frac{d}{d_2} \) and also \( d_1 \mid n \), we get that

\[
(1) \quad \frac{d}{d_1d_2} \mid \frac{m}{d_1}.
\]

Because \( \gcd(d, m) = d_1 \) we get that \( \gcd\left(\frac{d}{d_1}, \frac{m}{d_1}\right) = 1 \) and thus also

\[
(2) \quad \left(\frac{d}{d_1d_2}, \frac{m}{d_1}\right) = 1.
\]

Using (1) and (2) we conclude that

\[
\frac{d}{d_1d_2} = 1,
\]

as desired for this lemma.

As for the uniqueness part, if \( d = d_3d_4 \) where \( d_3 \mid m \) and \( d_4 \mid n \), then we would get that \( d_3 \mid d_1 = \gcd(d, m) \) and also \( d_4 \mid d_2 = \gcd(d, n) \). Therefore, using that \( d_3d_4 = d_1d_2 \) we would get that indeed \( d_3 = d_1 \) and \( d_4 = d_2 \). \( \square \)

Let \( m, n \in \mathbb{N} \) such that \( \gcd(m, n) = 1 \). Using Lemma 2.1 for each divisor \( d \) of \( mn \), there exist unique divisors \( d_1 \) of \( m \) and respectively \( d_2 \) of \( n \) such that \( d = d_1d_2 \). Conversely, if \( d_1 \) is a divisor of \( m \), and \( d_2 \) is a divisor of \( n \), then clearly \( d_1d_2 \) is a
The divisor of \( mn \). So, using also the fact that \( f \) is multiplicative, we have

\[
F(mn) = \sum_{d|mn} f(d)
\]

\[
= \sum_{d_1|m, \ d_2|n} f(d_1d_2)
\]

\[
= \sum_{d_1|m} \sum_{d_2|n} f(d_1)f(d_2)
\]

\[
= \left( \sum_{d_1|m} f(d_1) \right) \cdot \left( \sum_{d_2|n} f(d_2) \right)
\]

\[
= F(m)F(n),
\]

as desired.

**Problem 2.**

(i) We know that \( \sigma(n) = \sum_{d|n} d \), and because the function \( f : \mathbb{N} \to \mathbb{N} \) given by \( f(n) = n \) is multiplicative, the conclusion of **Problem 1** yields that also \( \sigma \) is a multiplicative function.

(ii) We compute easily

\[
\sigma(p^\alpha)
= 1 + p + \cdots + p^\alpha
= \frac{p^{\alpha+1} - 1}{p - 1}.
\]

(iii) Using parts (i) and (ii) above, the conclusion is immediate.

**Problem 3.** Assuming that \( (2^{k+1} - 1) \) is a prime number, and using the formula for \( \sigma(n) \) (as in **Problem 2**) we conclude that

\[
\sigma(n) = \sigma(2^k) \cdot \sigma(2^{k+1} - 1) = (2^{k+1} - 1) \cdot 2^k
\]

Therefore \( n \) is a perfect number.

**Problem 4.** Since \( n \) is even, there exists \( k \in \mathbb{N} \) such that \( n = 2^k \cdot m \), where \( m \) is an odd positive integer. Assuming that \( n \) is perfect we get that

\[
2^{k+1}m = 2n = \sigma(n) = \sigma(2^k) \cdot \sigma(m) = (2^{k+1} - 1) \cdot \sigma(m).
\]

Since \( \gcd(2^{k+1}, 2^{k+1} - 1) = 1 \), we get that \( (2^{k+1} - 1) \mid m \), i.e., there exists \( m_1 \in \mathbb{N} \) such that

\[
m = m_1 \cdot (2^{k+1} - 1).
\]

We prove first that \( m_1 = 1 \). Indeed, otherwise (if \( m_1 > 1 \)) we would have that

\[
\sigma(m) \geq 1 + m_1 + (2^{k+1} - 1)m_1 \geq 2^{k+1}m_1.
\]

So, in this case we could not get the equality above: \( 2^{k+1}m = (2^{k+1} - 1)\sigma(m) \). Hence, indeed \( m_1 = 1 \).
Next we prove that \( m = 2^{k+1} - 1 \) must be a prime number. Indeed, otherwise there exists a divisor \( d \) of \((2^{k+1} - 1)\) other than 1 and itself. Thus \( \sigma(m) = \sigma(2^{k+1} - 1) \geq 1 + d + 2^{k+1} - 1 > 2^{k+1} \). This last inequality again would contradict the fact that \( 2^{k+1}m = (2^{k+1} - 1)\sigma(m) \). Hence, indeed \((2^{k+1} - 1)\) is a prime number, as desired.

**Problem 5.** Assume that \( \sigma(p^aq^b) = 2p^aq^b \); then
\[
\sum_{0 \leq i \leq a, 0 \leq j \leq b} p^i q^j = 2p^aq^b.
\]
This yields
\[
\sum_{0 \leq i \leq a, 0 \leq j \leq b} p^{i-a} q^{j-b} = 2,
\]
or equivalently
\[
2 = \sum_{0 \leq i \leq a, 0 \leq j \leq b} p^{-i} q^{-j} < \sum_{i \geq 0, j \geq 0} p^{-i} q^{-j} = \left( \sum_{i \geq 0} p^{-i} \right) \cdot \left( \sum_{j \geq 0} q^{-j} \right) = \frac{p}{p-1} \cdot \frac{q}{q-1}.
\]
But we know that \( p \) and \( q \) are distinct odd prime numbers which yields a contradiction:
\[
2 < \left( 1 + \frac{1}{p-1} \right) \cdot \left( 1 + \frac{1}{q-1} \right) \leq \left( 1 + \frac{1}{3-1} \right) \cdot \left( 1 + \frac{1}{5-1} \right) < 2.
\]
Therefore \( p^aq^b \) is never a perfect number.

**Problem 6.** Since \( \gcd(n, n+1) = 1 \) for all \( n \in \mathbb{N} \) we conclude that \( f(n^2 + n) = f(n)f(n + 1) \).

It is immediate to see that
\[
\lim_{n \to \infty} \frac{f(n)}{n^k} = a_k.
\]
So,
\[
a_k = \lim_{n \to \infty} \frac{f(n^2 + n)}{(n^2 + n)^k} = \lim_{n \to \infty} \frac{f(n+1)}{(n+1)^k} \cdot \lim_{n \to \infty} \frac{f(n)}{n^k} = a_k \cdot a_k.
\]
Therefore, since \( a_k \neq 0 \), we conclude that \( a_k = 1 \).

Assume now that not all \( a_i \) are 0, for \( i < k \); so let \( \ell \) be the largest index \( i < k \) such that \( a_i \neq 0 \). Then

\[
\lim_{n \to \infty} \frac{f(n) - n^k}{n^\ell} = a_\ell.
\]

So,

\[
0 = \lim_{n \to \infty} \frac{f(n)^{k\ell}}{n^{k\ell}} = \lim_{n \to \infty} \frac{f(n) - n^k}{n^\ell} = \lim_{n \to \infty} \frac{f(n)(n+1)^{k\ell} - n^{k(1+k)\ell}}{(n+1)^{k\ell} - n^{k\ell}}.
\]

Therefore \( a_\ell = 0 \) which contradicts our assumption that \( a_\ell \neq 0 \). Therefore indeed \( a_i = 0 \) for each \( i < k \), as desired.

**Problem 7.** Let \( p_1, \ldots, p_k \) be all the distinct prime numbers dividing \( \gcd(m, n) \) (since \( m \) and \( n \) are not relatively prime, we know that \( k \geq 1 \)).

We let \( \alpha_i = \exp_{p_i}(m) \) and \( \beta_i = \exp_{p_i}(n) \). Also, we let

\[
m_1 = \frac{m}{\prod_{i=1}^{k} p_i^{\alpha_i}}, \quad n_1 = \frac{n}{\prod_{i=1}^{k} p_i^{\beta_i}}.
\]

Because the \( p_i \)'s are all the prime factors of \( \gcd(m, n) \) we conclude that \( \gcd(m_1, n_1) = 1 \). Also, by the choice of \( \alpha_i \) and \( \beta_i \) we get that no \( p_i \) divides \( m_1 n_1 \); i.e.,

\[
\gcd\left( m_1, \prod_{i=1}^{k} p_i^{\alpha_i} \right) = \gcd\left( n_1, \prod_{i=1}^{k} p_i^{\beta_i} \right) = 1.
\]

So, we compute:

\[
\sigma(m) = \sigma(m_1) \cdot \prod_{i=1}^{k} \frac{p_i^{\alpha_i+1} - 1}{p_i - 1},
\]

\[
\sigma(n) = \sigma(n_1) \cdot \prod_{i=1}^{k} \frac{p_i^{\beta_i+1} - 1}{p_i - 1},
\]

\[
\sigma(mn) = \sigma(m_1)\sigma(n_1) \cdot \prod_{i=1}^{k} \frac{p_i^{\alpha_i+\beta_i+1} - 1}{p_i - 1}.
\]

In order to prove that \( \sigma(mn) < \sigma(m) \cdot \sigma(n) \), it suffices to prove that for each prime number \( p \) and for each \( \alpha, \beta \in \mathbb{N} \), we have

\[
\frac{p^{\alpha+\beta+1} - 1}{p - 1} < \frac{p^{\alpha+1} - 1}{p - 1} \cdot \frac{p^{\beta+1} - 1}{p - 1}.
\]
This last inequality is equivalent with showing that
\[(p^{\alpha+\beta+1} - 1)(p - 1) < (p^{\alpha+1} - 1)(p^{\beta+1} - 1).\]
A simple computation yields that we need to show that
\[p^{\alpha+1} + p^{\beta+1} < p^{\alpha+\beta+1} + p.\]
But
\[p^{\alpha+\beta+1} + p - p^{\alpha+1} - p^{\beta+1} = p(p^\alpha - 1)(p^\beta - 1) > 0,\]
since \(\alpha, \beta > 0\). This concludes our proof.

**Problem 8.** We know that \(\sigma(n) = (p+1)(q+1)(r+1)\). So, if all three prime numbers \(p, q\) and \(r\) are odd, then \(\exp_2(\sigma(n)) \geq 3\). On the other hand, if we assume that \(\sigma(n) = 2n\), then
\[\exp_2(\sigma(n)) = \exp_2(2pqr) = 1,\]
which is then a contradiction. So, one of the prime numbers \(p, q\) or \(r\) equals 2. Without loss of generality we assume \(r = 2\), and thus
\[\sigma(n) = 3(p+1)(q+1) = 3pq + 3p + 3q + 3.\]
So, if \(\sigma(n) = 2n = 4pq\), we get that
\[pq - 3p - 3q - 3 = 0,\]
and so,
\[(p - 3)(q - 3) = 12.\]
Hence \(p, q \in \{4, 5, 6, 7, 9, 15\}\). Hence \(p\) and \(q\) must be 5 and 7; however,
\[(5 - 3)(7 - 3) \neq 12.\]
Therefore there exist no distinct prime numbers \(p, q\) and \(r\) such that
\[\sigma(pqr) = 2pqr.\]

**Problem 9.** We know that \(\phi\) is a multiplicative function and then by the conclusion of Problem 1, we know that also the function \(F : \mathbb{N} \rightarrow \mathbb{N}\) defined by
\[F(n) = \sum_{d|n} \phi(d)\]
is also a multiplicative function. Therefore, in order to find out \(F\), all we need to compute is \(F(p^\alpha)\) for primes \(p\), and for \(\alpha \in \mathbb{N}\). Now, we know that for each \(\beta \in \mathbb{N}\),
\[\phi(p^\beta) = p^\beta - p^{\beta-1}.\]
So,

\[ F(p^\alpha) = \sum_{d|p^\alpha} \phi(d) \]

\[ = \phi(1) + \sum_{\beta=1}^{\alpha} \phi(p^\beta) \]

\[ = 1 + \sum_{\beta=1}^{\alpha} (p^\beta - p^{\beta-1}) \]

\[ = p^\alpha. \]

Therefore, for each \( n \in \mathbb{N} \), if \( n = 1 \), clearly \( F(1) = 1 \), while if \( n > 1 \), we let

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

be the factorization of \( n \) into a product of powers of primes. Then, using the fact that \( F \) is multiplicative we find that

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

as desired.

Problem 10.

(i) We start with the following claim.

**Claim 2.2.** If \( x \in \mathbb{Z} \) and if \( p > 3 \) is a prime number such that \( p \mid (x^2 + x + 1) \), then \( p \equiv 1 \pmod{3} \).

**Proof.** Since \( p \mid (x^2 + x + 1) \), then also \( p \mid (x^3 - 1) \) (because \( x^3 - 1 = (x - 1)(x^2 + x + 1) \)). Therefore the order of \( x \) modulo \( p \) divides 3. There are two cases.

**Case 1.** the order of \( x \) modulo \( p \) is 1

Then \( p \mid (x - 1) \), and since

\[ x^2 + x + 1 = (x - 1)^2 + 3(x - 1) + 3, \]

we get that \( p \mid 3 \). This is impossible since \( p > 3 \) by our assumption.

**Case 2.** the order of \( x \) modulo \( p \) is 3

Then \( 3 \mid (p - 1) \) because always the order of \( x \) modulo \( p \) divides \( p - 1 \).

This concludes the proof of our Claim. \( \Box \)

Now, assume there exist only finitely many prime numbers of the form \( 3n + 1 \) (note that 7 is one of them, for example). We label then these finitely many primes as: \( p_1, \ldots, p_\ell \). We let

\[ x = 3 \cdot \prod_{i=1}^{\ell} p_i. \]
Clearly, $x \geq 21$ and thus $x^2 + x + 1 > 1$ (which yields that $x^2 + x + 1$ is divisible by at least one prime number $p$). On the other hand, because $3 \mid x$, then
\[ x^2 + x + 1 \equiv 1 \pmod{3}. \]
So, by Claim 2.2, $x^2 + x + 1$ is divisible only by primes which are congruent with 1 modulo 3. However, for each $i = 1, \ldots, \ell$, we have
\[ x^2 + x + 1 \equiv 1 \pmod{p_i}, \]
which means that $x^2 + x + 1$ cannot be divisible by any prime number $p_i$. This provides a contradiction to our assumption that the $p_i$’s are all the prime numbers congruent with 1 modulo 3; we just saw that $x^2 + x + 1$ must be divisible by another prime number of the form $3n + 1$ which is not from the list $p_1, \ldots, p_\ell$. So, there exist infinitely many prime numbers of the form $3n + 1$.

(ii) Assume there exist only finitely many primes of the form $3n + 2$; let $q_1, \ldots, q_k$ be all these such primes (note that the first such prime is $q_1 = 2$ and $q_2 = 5$). We let
\[ N = -1 + 3 \cdot \prod_{j=1}^{k} q_j. \]
Then $N > 1$ is a number of the form $3n + 2$ itself. So, it must be divisible by a prime number $p$ which is of the form $3n + 2$. Indeed, otherwise all its prime factors would be of the form $3n + 1$ and since product of two numbers which are congruent with 1 modulo 3 is also a number congruent with 1 modulo 3 we would obtain that $N$ is congruent with 1 modulo 3, which would be a contradiction.

Now we claim that the above prime number $p$ which divides $N$ and which is of the form $3n + 2$ is not from the list: $q_1, \ldots, q_k$. Indeed, if $p = q_j$, say, then because
\[ q_j \nmid 3 \cdot q_1 \cdots q_k, \]
we would obtain that $q_j \mid 1$, which is a contradiction. So, $p \equiv 2 \pmod{3}$, but $p \neq q_j$ for $j = 1, \ldots, k$; this provides a contradiction with our assumption that the list: $q_1, \ldots, q_k$ contains all prime numbers of the form $3n + 2$.

In conclusion there exist infinitely many prime numbers of the form $3n + 2$.

**Problem 11.** Since 1 is divisible by no prime factor, we have $\omega(1) = 0$ and thus $\mu(1) = 1$. Also, in general, if $p_1, \ldots, p_r$ are distinct prime factors, we have
\[ \mu(p_1 \cdots p_r) = (-1)^r, \]
while if there exists $m > 1$ such that $m^2 \mid n$, then $\mu(n) = 0$. Hence, if $\gcd(n_1, n_2) = 1$, we have two cases.

**Case 1.** both $n_1$ and $n_2$ are square-free
In this case $\mu(n_i) = (-1)^{\omega(n_i)}$ for $i = 1, 2$. Moreover, $n_1n_2$ is also square-free and $\omega(n_1n_2) = \omega(n_1) + \omega(n_2)$ because $\gcd(n_1, n_2) = 1$. Thus
\[ \mu(n_1n_2) = (-1)^{\omega(n_1n_2)} = (-1)^{\omega(n_1)+\omega(n_2)} = \mu(n_1) \cdot \mu(n_2). \]

**Case 2.** at least one of the two numbers $n_1$ or $n_2$ is not square-free
In this case also \( n_1n_2 \) is not square-free, and therefore
\[
\mu(n_1n_2) = 0 = \mu(n_1) \cdot \mu(n_2).
\]

Therefore in the above two cases we proved that \( \mu \) is a multiplicative function. Using Problem 1 we conclude that also the function \( F : \mathbb{N} \rightarrow \mathbb{Z} \) defined by
\[
F(n) = \sum_{d|n} \mu(d)
\]
is a multiplicative function. Therefore in order to compute \( F \) all we need to do is find out \( F(p^\alpha) \) for each prime number \( p \) and for each \( \alpha \in \mathbb{N} \) (clearly, \( F(1) = \mu(1) = 1 \)). So,
\[
F(p^\alpha) = \mu(1) + \mu(p) + \sum_{\beta=2}^\alpha \mu(p^\beta) = 1 + (-1) + 0 = 0.
\]
Hence, for each \( n \in \mathbb{N} \) larger than 1, we let \( n = \prod_{i=1}^r p_i^{\alpha_i} \) be its factorization into a product of powers of primes and so, using that \( F \) is multiplicative, we have:
\[
F(n) = \prod_{i=1}^r F(p_i^{\alpha_i}) = 0.
\]

**Problem 12.**

(i) For each \( n \in \mathbb{N} \) we compute
\[
\sum_{d|n} \mu(d)F\left(\frac{n}{d}\right)
\]
\[
= \sum_{d|n} \mu(d) \sum_{e|\frac{n}{d}} f(e)
\]
\[
= \sum_{e|n} f(e) \cdot \sum_{d|\frac{n}{e}} \mu(d)
\]
\[
= f(n),
\]
since for each \( e \mid n \) but \( e \neq n \), the integer number \( \frac{n}{e} \) is larger than 1 and then
\[
\sum_{d|\frac{n}{e}} \mu(d) = 0,
\]
according to Problem 11.

(ii) For each \( n \in \mathbb{N} \) we compute
\[
\sum_{d|n} f(d)
\]
\[
= \sum_{d|n} \sum_{e|d} \mu(e)F\left(\frac{d}{e}\right)
\]
\[
= \sum_{d_1|n} F(d_1) \cdot \sum_{e|\frac{n}{d_1}} \mu(e)
\]
\[
= F(n),
\]
since for each \( d_1 \mid n \) but \( d_1 \neq n \), the integer number \( \frac{n}{d_1} \) is larger than 1 and then

\[
\sum_{e \mid \frac{n}{d_1}} \mu(e) = 0,
\]

according to Problem 11.

**Problem 13.** According to Problem 13 (i), we have

\[
f(n) = \sum_{d \mid n} \mu(d)F \left( \frac{n}{d} \right).
\]

Let now \( m,n \in \mathbb{N} \) such that \( \gcd(m,n) = 1 \). Using Lemma 2.1 and also the fact that \( \mu \) and \( F \) are multiplicative functions, we compute

\[
f(mn) = \sum_{d \mid mn} \mu(d)F \left( \frac{mn}{d} \right)
\]

\[
= \sum_{d_1 \mid m, d_2 \mid n} \mu(d_1d_2)F \left( \frac{mn}{d_1d_2} \right)
\]

\[
= \sum_{d_1 \mid m, d_2 \mid n} \mu(d_1)\mu(d_2)F \left( \frac{m}{d_1} \right)F \left( \frac{n}{d_2} \right)
\]

\[
= \left( \sum_{d_1 \mid m} \mu(d_1)F \left( \frac{m}{d_1} \right) \right) \cdot \left( \sum_{d_2 \mid n} \mu(d_2)F \left( \frac{n}{d_2} \right) \right)
\]

\[
= f(m) \cdot f(n).
\]

This proves that \( f \) is indeed a multiplicative function.

**Problem 14.** Let

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

be the factorization of \( m \) into a product of powers of primes. Note that each \( p_i \) is odd since \( m \) is odd.

Using the Chinese Remainder Theorem, we get that the number of solutions to the congruence equation

\[
x^2 \equiv a \pmod{m}
\]

is \( \prod_{i=1}^{r} N_i \), where for each \( i = 1, \ldots, r \), \( N_i \) is the number of solutions to the congruence equation

\[
x^2 \equiv a \pmod{p_i^{a_i}}.
\]

So, we are done if we can prove that for each odd prime number \( p \) which does not divide \( a \) (note that \( \gcd(a,m) = 1 \)), and for each \( \alpha \in \mathbb{N} \), the number of solutions to the congruence equation

\[
x^2 \equiv a \pmod{p^\alpha}
\]

equals \( 1 + \left( \frac{a}{p} \right) \).
Case 1. \( \left( \frac{a}{p} \right) = -1 \)
In this case, \( a \) is not a quadratic residue modulo \( p \) and therefore there exists no \( x \in \mathbb{Z} \) such that \( x^2 \equiv a \pmod{p} \). In particular, for each \( \alpha \in \mathbb{N} \), there is no solution to the congruence equation (3).

Case 2. \( \left( \frac{a}{p} \right) = 1 \)
In this case we immediately get that the congruence equation

\[
x^2 \equiv a \pmod{p}
\]

has exactly two solutions \( x_1 \) and \( x_2 \). We claim that each solution \( x_1 \) and \( x_2 \) has a unique lifting to a solution of the congruence equation (3). Indeed, for this it suffices to show that for each \( \alpha \in \mathbb{N} \) if \( x_\alpha \) is a solution for the congruence equation

\[
x^2 \equiv a \pmod{p^\alpha}
\]

then there exists a unique lifting \( x_{\alpha+1} \) which is a solution for the congruence equation

\[
x^2 \equiv a \pmod{p^{\alpha+1}}.
\]

This statement follows by Hensel’s Lemma once we observe that the derivative of \( x^2 \) is \( 2x \) and thus its value at \( x = x_\alpha \) is relative prime with \( p \) because \( x_\alpha \) is not divisible by \( p \) (note that \( a \) is not divisible by \( p \) and \( x_\alpha^2 \equiv a \pmod{p} \)) and also \( \gcd(2,p) = 1 \) since \( p \) is odd.

In conclusion, the congruence equation (3) has indeed 2 solutions, as desired.

Problem 15.

(i) We know that

\[
x^4 \equiv -1 \pmod{p}.
\]

So, in particular, \( x^8 \equiv 1 \pmod{p} \). We claim that the order of \( x \) modulo \( p \) is precisely 8. Indeed, it has to be a divisor of 8, but we already know that \( x^4 \not\equiv 1 \pmod{p} \) (since \( 1 \not\equiv -1 \pmod{p} \) for odd \( p \)); thus the order of \( x \) modulo \( p \) is not 4. In conclusion, the order of \( x \) modulo \( p \) is 8. But always the order of a nonzero residue class modulo \( p \) must divide \( p - 1 \); so, 8 \( | \) \( p - 1 \), which yields

\[
p \equiv 1 \pmod{8}.
\]

(ii) Assume there exist only finitely many prime numbers congruent with 1 modulo 8. So, let \( p_1, \ldots, p_k \) be all such prime numbers (we know already that \( k \geq 1 \) since 17 is a prime number). Let

\[
x = 2 \cdot \prod_{i=1}^{k} p_i.
\]

Then \( x^4 + 1 \) is an odd integer larger than 1, and therefore it is divisible by some prime number \( p \), which must be odd. According to part (i), we get that \( p \equiv 1 \pmod{8} \). Therefore, \( p \) must be one of the prime numbers \( p_i \) in the above list. However, in that case we would have that

\[
p \mid x
\]

which coupled with \( p \mid (x^4 + 1) \) yields a contradiction. In conclusion, there must be infinitely many prime numbers of the form \( 8n + 1 \).
Problem 16. We claim that both $b$ and $c$ must be divisible by $p$, which immediately yields the desired conclusion.

Now, we first observe that $p \nmid a$ since $\left(\frac{a}{p}\right) = -1$. Hence $ab^2 \equiv c^2 \pmod{p}$ yields that $p \mid b$ if and only if $p \mid c$. So, assume $p \nmid b$. Let $d \in \mathbb{N}$ such that

$$bd \equiv 1 \pmod{p}.$$ 

Then

$$(cd)^2 \equiv ab^2 \cdot d^2 \equiv a \cdot (bd)^2 \equiv a \pmod{p},$$

which contradicts the fact that $\left(\frac{a}{p}\right) = -1$. Therefore, indeed both $b$ and $c$ are divisible by $p$ and thus

$$b^2 \equiv c^2 \equiv 0 \pmod{p^2}.$$ 

Problem 17. Clearly, if $n = 1$ we have $\phi(n) = \sigma(n) = 1$ and thus $\phi(n) + \sigma(n) = 2n$. So, from now on we assume $n > 1$. Let

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

be the factorization of $n$ into a product of powers of primes. Then

$$\phi(n) = n \cdot \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right)$$

and

$$\sigma(n) = \prod_{i=1}^{r} p_i^{\alpha_i+1} - 1 = n \cdot \prod_{i=1}^{r} \frac{p_i - p_i^{-\alpha_i}}{p_i - 1}.$$ 

It is immediate then to see that for each prime $p$ and for each $\alpha \in \mathbb{N}$ we have

$$\frac{p - p^{-\alpha}}{p - 1} \geq \frac{p - p^{-1}}{p - 1} = \frac{p + 1}{p} = 1 + \frac{1}{p},$$

with equality if and only if $\alpha = 1$. Thus

$$\frac{\phi(n) + \sigma(n)}{n} \geq \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right) + \prod_{i=1}^{r} \left(1 + \frac{1}{p_i}\right)$$

$$= 2 \cdot \left(1 + \sum_{s=1}^{\left[\frac{r}{2}\right]} \sum_{1 \leq i_1 < i_2 < \cdots < i_{2s} \leq r} \frac{1}{\prod_{j=1}^{2s} p_{i_j}}\right)$$

$$\geq 2,$$

with equality if and only if $r = 1$ so that the above double sum is empty (since then $s$ would range from 1 to $\left[\frac{1}{2}\right] = 0$). So, if $n > 1$ the equality is attained only when $n$ is divisible by a unique prime number $p_1$, and moreover, $\exp_{p_1}(n) = 1$. In conclusion,

$$\phi(n) + \sigma(n) \geq 2n,$$

with equality if and only if $n = 1$, or if $n = p_1$ is a prime number.
Problem 18. We know that
\[ 2^a \equiv 1 \pmod{2^a - 1} \]
and so because \( b \in \mathbb{N} \) we have that
\[ (2^a)^b \equiv 1 \pmod{2^a - 1} \]
and thus
\[ 2^b \equiv 1 \pmod{2^a - 1} \]
which yields that
\[ 2^a - 1 | 2^b - 1. \]

Problem 19. We first claim that the set
\[ A := \{ x^4 \pmod{p} : x \in \mathbb{Z} \} \]
has precisely \((p + 1)/2\) elements. Indeed, we note that if \( x \equiv -y \pmod{p} \), then \( x^4 \equiv y^4 \pmod{p} \). So, on one hand, there are no more than \((p + 1)/2\) distinct elements in \( A \). On the other hand, we claim that if
\[ x^4 \equiv y^4 \pmod{p}, \]
then \( x \equiv \pm y \pmod{p} \), or in other words, \( x^2 \equiv y^2 \pmod{p} \). Indeed, if \( p \mid (x^4 - y^4) \), and if \( p \nmid (x^2 - y^2) \), then we must have \( p \mid (x^2 + y^2) \).

Now, if \( p \mid y \), then we must have \( p \mid x^4 \), and so, \( p \mid x \), which would also yield that \( p \mid (x^2 - y^2) \). So, we may assume \( p \nmid y \), and letting \( z \) be the inverse of \( y \) modulo \( p \), we conclude that
\[ p \mid (xz)^2 + 1, \]
or in other words that
\[ (xz)^2 \equiv -1 \pmod{p}. \]
But \( p \equiv 3 \pmod{4} \), which yields a contradiction. So, indeed, if \( x^4 \equiv y^4 \pmod{p} \), then \( x \equiv \pm y \pmod{p} \). In conclusion, all of the following numbers have distinct residues modulo \( p \):
\[ 0^4, 1^4, \ldots, ((p - 1)/2)^4. \]
So, indeed, \( |A| = (p + 1)/2 \). We let
\[ B := \{ a - x^4 \pmod{p} : x \in \mathbb{Z} \}. \]
Then \( |B| = (p + 1)/2 \), and since both \( A \) and \( B \) are contained in the set of \( p \) residues modulo \( p \), and \( |A| + |B| > p \), there exists \( w \in A \cap B \). But this means that there exist \( x, y \in \mathbb{Z} \) such that
\[ x^4 \equiv w \equiv a - y^4 \pmod{p}. \]
Hence \( x^4 + y^4 \equiv a \pmod{p} \).

Problem 20. First we claim that \( f(x) \) has no root \( z \) of absolute value at most equal to 1. Indeed, otherwise
\[
0 = |f(z)| 
\geq |a_0| - |a_1| \cdot |z| - |a_2| \cdot |z|^2 - \cdots - |a_n| \cdot |z|^n 
\geq |a_0| - |a_1| - |a_2| - \cdots - |a_n| 
> 0,
\]
which is a contradiction.
Secondly, assume $f$ is reducible, and therefore there exist $g, h \in \mathbb{Z}[x]$ such that $f = g \cdot h$. Then $f(0) = g(0)h(0)$ and since $|f(0)| = |a_0|$ is a prime number while both $g(0)$ and $h(0)$ are integers, we conclude that either $|g(0)|$ or $|h(0)|$ equals 1. Say that $|g(0)| = 1$. Then
\[
g(x) = b_m x^m + \cdots + b_1 x + b_0,
\]
where each $b_i \in \mathbb{Z}$ and $b_0 = \pm 1$. If we let $z_1, \ldots, z_m$ be all the roots of $g(x) = 0$ (listed with repetition, if needed), then
\[
z_1 z_2 \cdots z_m = (-1)^m \frac{b_0}{b_m}
\]
because $b_m x^m + \cdots + b_1 x + b_0 = b_m (x - z_1) \cdots (x - z_m)$. So,
\[
|z_1| \cdot |z_2| \cdots |z_m| = \frac{|b_0|}{|b_m|} \leq 1,
\]
since $|b_0| = 1 \leq |b_m|$. But this yields that there exists a root $z \in \{z_1, \ldots, z_m\}$ such that $|z| \leq 1$, and this root is then also a root of $f$ (since $g \mid f$) and thus we obtain a contradiction. So, $f$ is irreducible.

**Problem 21.** Assume there exists a prime number $p$ dividing $2^n + 1$ such that $p \equiv 7 \pmod{8}$.

**Case 1.** $n$ even.

\[
\left( \frac{2^n}{2} \right)^2 = 2^n \equiv -1 \pmod{p}.
\]
But because $p \not\equiv 1 \pmod{4}$, then $-1$ is not a perfect square modulo $p$. So we obtain a contradiction in this Case 1.

**Case 2.** $n$ odd.

\[
\left( \frac{2^{(n+1)/2}}{2} \right)^2 = 2^{n+1} \equiv -2 \pmod{p}.
\]
So, $1 = \left( \frac{-2}{p} \right) = \left( \frac{-1}{p} \right) \cdot \left( \frac{2}{p} \right)$ and $\left( \frac{2}{p} \right) = 1$ since $p \equiv 7 \pmod{8}$. Therefore
\[
\left( \frac{-1}{p} \right) = 1,
\]
which is a contradiction with the fact that $p \not\equiv 1 \pmod{4}$.

This finishes our proof.

**Problem 22.** Assume $P(a_i) = x_0 + i$ for $i = 1, \ldots, r$, where $x_0 \in \mathbb{Z}$ and also $a_i \in \mathbb{Z}$ for each $i$. Since $P \in \mathbb{Z}[X]$, then
\[
(a_i - a_j)(P(a_i) - P(a_j)) \text{ for each } i \neq j.
\]
So, $a_{i+1} - a_i = \pm 1$ for $i = 1, \ldots, r - 1$. On the other hand, since $a_i \neq a_j$ for $i \neq j$ (because $P(a_i) \neq P(a_j)$), we conclude that there exists $\epsilon \in \{-1, 1\}$ such that
\[
a_{i+1} - a_i = \epsilon \text{ for } i = 1, \ldots, r - 1.
\]
But this means that if we let $Q(X) = \epsilon X + x_0 + 1 - \epsilon a_1$, then
\[
Q(a_i) = Q(a_1 + \epsilon(i - 1)) = a_1 + (i - 1) + x_0 + 1 - \epsilon a_1 = x_0 + i.
\]
So, $(P - Q)(a_i) = 0$ for all $i = 1, \ldots, r$. On the other hand $\deg(P - Q) = \deg(P) = n > 1$. So, $r \leq n$ since a polynomial of degree $n$ cannot have more than $n$ roots.
On the other hand, the following is an example of a polynomial of degree $n$ which takes $n$ consecutive integer values:

$$P(X) = \prod_{i=1}^{n}(X - i) + X.$$ 

Indeed, $P(i) = i$ for all $i = 1, \ldots, n.$