1. Problems

Problem 1. Show that there exist arbitrarily large gaps between any two consecutive primes.

Problem 2. Let $p$ be a prime number, and let $a, b \in \mathbb{Z}$. Prove that

$$(a + b)^p \equiv a^p + b^p \pmod{p}.$$ 

Problem 3. Let $a, b \in \mathbb{C}$ and assume the quadratic equation $x^2 - ax - b = 0$ has two distinct roots $r_1, r_2 \in \mathbb{C}$.

(a) For each $c_1, c_2 \in \mathbb{C}$ define the sequence $\{\alpha_n\}_{n \geq 0}$ by the following formula:

$$\alpha_n = c_1 r_1^n + c_2 r_2^n.$$ 

Prove that

$$\alpha_n = a\alpha_{n-1} + b\alpha_{n-2} \quad \text{for each} \quad n \geq 2.$$ 

(b) Let $\{\beta_n\}_{n \geq 0}$ be a sequence of complex numbers satisfying

$$\beta_n = a\beta_{n-1} + b\beta_{n-2} \quad \text{for each} \quad n \geq 2.$$ 

Prove that there exist $d_1, d_2 \in \mathbb{C}$ such that for each $n \geq 0$ we have

$$\beta_n = d_1 r_1^n + d_2 r_2^n.$$ 

Problem 4. Let $a, b, c_0, c_1 \in \mathbb{Z}$ and let $\{\alpha_n\}_{n \geq 0}$ be defined as follows:

$$\alpha_0 = c_0, \quad \alpha_1 = c_1 \quad \text{and for each} \quad n \geq 2, \quad \alpha_n = a\alpha_{n-1} + b\alpha_{n-2}.$$ 

Let $m \in \mathbb{N}$. Prove that there exist integers $k \geq 0$ and $\ell \geq 1$ such that

$$\alpha_{k+n\ell} \equiv \alpha_k \pmod{m} \quad \text{for all} \quad n \geq 0.$$ 

Problem 5. Let $\{F_n\}_{n \geq 0}$ be the Fibonacci sequence, i.e.

$$F_0 = 0; \quad F_1 = 1 \quad \text{and} \quad F_{n+2} = F_{n+1} + F_n \quad \text{for all} \quad n \geq 0.$$ 

Is $F_{2011}$ odd or even? Explain your answer.

Problem 6. Let $k$ and $n$ be odd positive integers. Show that

$$\sum_{i=1}^{n-1} i^k \equiv 0 \pmod{n}.$$ 

Problem 7. Show that if $p$ is a prime number, then the only solutions of the congruence $x^2 \equiv x \pmod{p}$ are those integers $x$ such that $x \equiv 0 \pmod{p}$ or $x \equiv 1 \pmod{p}$. 

1
Problem 8. Let $p$ be an odd prime number such that $p \equiv 2 \pmod{3}$. Show that the equation $x^3 \equiv 1 \pmod{p}$ has a unique solution modulo $p$. Conclude that for each nonzero residue $a$ modulo $p$, there exists a solution to the congruence equation $x^3 \equiv a \pmod{p}$.

Problem 9. Let $p$ be a prime number such that $p \equiv 1 \pmod{4}$. Show that

$\left( \frac{p-1}{2} \right)!^2 \equiv -1 \pmod{p}$

Conclude that the equation $x^2 \equiv -1 \pmod{p}$ has two solutions modulo $p$.

Problem 10. Show that if $p$ and $q$ are distinct primes, then $p^{q-1} + q^{p-1} \equiv 1 \pmod{pq}$.

Problem 11. Show that the sequence defined recursively by

$b_0 = 5; b_1 = 3$ and $b_{n+2} = 6b_{n+1} - 9b_n$

has the general term

$b_n = 3^n(-4n + 5)$.

Problem 12. Let $P \in \mathbb{C}[x]$ be a polynomial of degree $n \geq 1$.

(a) Let $a_0, \ldots, a_n \in \mathbb{C}$ be any distinct complex numbers. For each $k \in \{0, \ldots, n\}$ let $c_k = P(a_k)$. Prove that

$P(x) = \sum_{k=0}^{n} c_k \cdot \prod_{\substack{0 \leq i \leq n \atop i \neq k}} (x - a_i) \cdot \prod_{\substack{0 \leq i \leq n \atop i \neq k}} (a_k - a_i)$

(b) Assume $P(k) \in \mathbb{Z}$ for each $k \in \{0, \ldots, n\}$. Prove that $P(x) \in \mathbb{Z}$ for each $x \in \mathbb{Z}$.

(c) Show that if $P(k) \in \mathbb{Z}$ for each $k \in \mathbb{Z}$, then $n! \cdot P(x) \in \mathbb{Z}[x]$ (i.e., each coefficient of $n!P(x)$ is an integer).

(d) Give an example of a polynomial $P(x)$ of degree $n \geq 2$ which does not have all its coefficients integers, but for which $P(k) \in \mathbb{Z}$ for each $k \in \mathbb{Z}$.

Problem 13. Let $\{F_n\}_{n \geq 1}$ be the sequence defined as follows:

$F_0 = 0, F_1 = 1$, and for $n \geq 2$ we have $F_n = F_{n-1} + F_{n-2}$.

(a) Prove that

$F_n = \frac{1}{\sqrt{5}} \left( \frac{1 + \sqrt{5}}{2} \right)^n - \frac{1}{\sqrt{5}} \left( \frac{1 - \sqrt{5}}{2} \right)^n$

for each $n \geq 0$.

(b) Prove that for each $m \in \mathbb{N}$ there exist infinitely many $n \in \mathbb{N}$ such that $m \mid F_n$. 


Problem 14. Let \( p \) be a prime number. Show that for each \( k \in \{0, \ldots, p - 1\} \) we have
\[
\binom{p-1}{k} \equiv (-1)^k \pmod{p}.
\]

Problem 15. Let \( a, b \in \mathbb{Z} \) and let \( p \) be a prime number. Show that if \( a^p \equiv b^p \pmod{p} \), then \( a^p \equiv b^p \pmod{p^2} \).

Problem 16. Find all the prime numbers \( p \) and all the positive integers \( n \) such that
\[
(p-2)! = p^n + 1.
\]

Problem 17. Show that \( 30 \mid (n^3 - n) \) for all \( n \in \mathbb{Z} \).

Problem 18. Let \( \ell \) be a prime number such that \( 2^\ell - 1 \) is not a prime number. Prove that \( 2^\ell - 1 \) is not a power of a prime number.

Problem 19. Let \( p \) be a prime number. Prove that each positive integer \( n \) has a unique \( p \)-adic expansion, i.e., there exists a nonnegative integer \( m \) and there exist \( c_0, \ldots, c_m \in \{0, \ldots, p-1\} \) with \( c_m > 0 \) such that
\[
n = c_0 + c_1 p + c_2 p^2 + \cdots + c_m p^m = \sum_{i=0}^{m} c_i p^i = c_m a_{m-1} \cdots c_1 c_0.
\]

Problem 20. Let \( \{a_n\}_{n \in \mathbb{N}} \) be a sequence defined by
\[
a_{n+2} = na_{n+1} + (n+1)a_n
\]
where \( a_1 = 2 \) and \( a_2 = 1 \). Find \( a_n \) for all \( n \in \mathbb{N} \).

Problem 21. Write the \( p \)-adic expansion for 2012 when \( p \in \{2, 3, 5, 7\} \).

Problem 22. Let \( p \) be a prime number and let \( n, k \in \mathbb{N} \) with \( k \leq n \). Let
\[
n = a_m a_{m-1} \ldots a_1 a_0 \quad \text{and} \quad k = b_{\ell} b_{\ell-1} \ldots b_1 b_0
\]
be their \( p \)-adic expansions. Prove that \( p \mid \binom{n}{k} \) if and only if there exists \( i \in \{0, \ldots, \ell\} \) such that \( b_i > a_i \).

Problem 23. Let \( \{a_n\}_{n \in \mathbb{N}} \) be a sequence defined by \( a_1 = 1 \), \( a_2 = 3 \) and for each \( n \geq 1 \) we have
\[
a_{n+2} = a_{n+1} + a_n.
\]
Prove that for each \( n \geq 1 \) we have
\[
a_{2n} = \left( \frac{3 + \sqrt{5}}{2} \right)^n + \left( \frac{3 - \sqrt{5}}{2} \right)^n.
\]

Problem 24. Prove that \( 4^n + 15n - 1 \) is divisible by 9 for all \( n \in \mathbb{N} \).

Problem 25. Show that 21 divides \( 10^n - 2^n - 8 \) if and only if 6 divides \( n^2 - 1 \).

Problem 26. Find all positive integers \( n \) such that
\[
1! + 4! + \cdots + (3n + 1)!
\]
is a perfect square.
Problem 27. Find all functions \( f : \mathbb{N} \to \mathbb{N} \) such that for all \( x, y \in \mathbb{N} \) we have
\[
x \cdot 3^{f(y)} \mid f(x) \cdot 3^y.
\]

Problem 28. Determine with proof whether there exists a positive integer \( m \) such that for each positive integer \( n \) the number \( n! \cdot 2^{m-n} \) is a positive integer.

Problem 29. Let \( a, b \) be integers larger than 1. We construct two sequences \( \{a_n\}_{n \in \mathbb{N}} \) and \( \{b_n\}_{n \in \mathbb{N}} \) as follows:
\[
a_1 = a \quad \text{and for all } n \geq 1, \quad a_{n+1} = na_n - 1
\]
and
\[
b_1 = b \quad \text{and for all } n \geq 1, \quad b_{n+1} = nb_n + 1.
\]
Prove that if there exist infinitely many pairs \( (m, n) \in \mathbb{N} \times \mathbb{N} \) such that \( a_m = b_n \), then the famous number \( e \) is a rational number.

**Useful note:** \( e \) is the number defined either as the limit
\[
\lim_{n \to \infty} \left( 1 + \frac{1}{n} \right)^n
\]
or as the sum of the series
\[
\sum_{n=0}^{\infty} \frac{1}{n!}
\]
and it is the base of the natural logarithm.
2. Solutions

Problem 1. Let \( k \in \mathbb{N} \); we’ll show that there exist at least \( k \) consecutive composite integers, which yields the desired claim. Indeed, we claim that each number

\[
(k + 1)! + i
\]

is composite for \( 2 \leq i \leq k + 1 \) – clearly this suffices for our proof.

In order to show that each number \((k + 1)! + i\) is composite for \( 2 \leq i \leq k + 1 \) we note that

\( i \mid (k + 1)! \) and thus \( i \mid ((k + 1)! + i) \) for each \( 2 \leq i \leq k + 1 \).

Furthermore, \((k + 1)! + i > i\) and thus \((k + 1)! + i\) is a composite number since it is divisible by \( i > 1 \) and it is larger than \( i \).

Problem 2. From the binomial expansion, we know that

\[
(a + b)^p = \sum_{i=0}^{p} \binom{p}{i} a^i b^{p-i}.
\]

Since \( \binom{0}{0} = \binom{p}{p} = 1 \), all we need to prove is that

\[ p \mid \binom{p}{i} \text{ for } i = 1, \ldots, p - 1. \]

Now, for each \( 1 \leq i \leq p - 1 \) we have

\[
\binom{p}{i} = \frac{p!}{i!(p-i)!} = p \cdot \frac{(p-1)!}{D_i},
\]

where \( D_i = i!(p-i)! \).

**Claim.** \( D_i \mid (p-1)! \) for each \( i = 1, \ldots, p - 1 \).

**Proof.** Indeed, we know that

\[ C_i = \binom{p}{i} \text{ is an integer.} \]

So, \( D_i C_i = p \cdot (p - 1)! \), which means that

\[ D_i \mid p \cdot (p - 1)! \].

However, \( p \nmid D_i \) since no factor in \( i! \) nor in \((p-i)!\) is divisible by \( p \) (they are all less than \( p \)). Because \( D_i \mid p \cdot (p - 1)! \) and \( \gcd(D_i, p) = 1 \), we conclude that \( D_i \mid (p - 1)! \) as desired.

Using the above **Claim** we conclude that \( p \mid \binom{p}{i} \) since \( \frac{(p-1)!}{D_i} \) is an integer, and thus

\[
\binom{p}{i} = C_i = p \cdot \frac{(p-1)!}{D_i}
\]

is indeed divisible by \( p \). Therefore

\[(a + b)^p \equiv a^p + b^p \pmod{p}.
\]

Problem 3.
(a) For each $n \geq 2$ we compute:

$$\alpha_n - a\alpha_{n-1} - b\alpha_{n-2} = (c_1r_1^n + c_2r_2^n) - a(c_1r_1^{n-1} + c_2r_2^{n-1}) - b(c_1r_1^{n-2} + c_2r_2^{n-2})$$

$$= c_1r_1^{n-2}(r_1^2 - ar_1 - b) + c_2r_2^{n-2}(r_2^2 - ar_2 - b) = 0,$$

since both $r_1$ and $r_2$ are roots of the equation $x^2 - ax - b = 0$.

(b) We let $c_1$ and $c_2$ be the unique solutions of the system of equations:

$$\begin{cases}
  c_1 + c_2 &= \beta_0 \\
  c_1r_1 + c_2r_2 &= \beta_1
\end{cases}$$

Note that the above system has indeed a unique solution because $r_1 \neq r_2$ and thus the two rows of the system are linearly independent. We let $\{\alpha_n\}_{n \geq 0}$ be the sequence defined by

$$\alpha_n = c_1r_1^n + c_2r_2^n$$

for each $n \geq 0$.

As seen in part (a) above, we know that

$$\alpha_n = a\alpha_{n-1} + b\alpha_{n-2}$$

for each $n \geq 2$.

We already know, by construction of $c_1$ and $c_2$, that $\alpha_0 = \beta_0$ and $\alpha_1 = \beta_1$. Since the sequence $\{\alpha_n\}_{n \geq 0}$ satisfies the same (linear) recurrence relation of order 2 as the sequence $\{\beta_n\}_{n \geq 0}$, and in addition the two sequences have the same first two terms, we conclude that $\alpha_n = \beta_n$, as desired.

Note that we can prove $\alpha_n = \beta_n$ easily by induction on $n$. The statement holds for $n = 0, 1$, and for $n \geq 2$ we use the fact that

$$\alpha_n = a\alpha_{n-1} + b\alpha_{n-2} = a\beta_{n-1} + b\beta_{n-2} = \beta_n.$$  

**Problem 4.** We define the function

$$\Phi : \mathbb{N} \rightarrow \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$$

by

$$\Phi(n) = (\bar{\alpha_n}, \bar{\alpha_{n-1}}),$$

where $\bar{z}$ represents always the residue class of the integer $z$ modulo $m$. Since $|\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}| = m^2$ while $\mathbb{N}$ is infinite, we conclude that there exist positive integers $k$ and $\ell$ such that $\Phi(k) = \Phi(k + \ell)$. Thus

$$\alpha_{k-1} \equiv \alpha_{k-1+\ell} \pmod{m} \text{ and } \alpha_k \equiv \alpha_{k+\ell} \pmod{m}.$$  

**Claim.** For each integer $n \geq k - 1$ we have $\alpha_n \equiv \alpha_{n+\ell} \pmod{m}$.

Indeed, the above Claim already holds, for $n = k - 1$ and $n = k$. So, we proceed by induction on $n$ and assume that for some $N \geq k + 1$ we already know that

$$\alpha_n \equiv \alpha_{n+\ell} \pmod{m} \text{ if } k - 1 \leq n < N,$$

and we will derive that $\alpha_N \equiv \alpha_{N+\ell} \pmod{m}$.

Indeed, since $N \geq k + 1$ we can argue as follows:

$$\alpha_{N+\ell} \equiv a\alpha_{N+\ell-1} + b\alpha_{N+\ell-2} \equiv a\alpha_{N-1} + b\alpha_{N-2} \equiv \alpha_N \pmod{m},$$

as desired. This concludes the proof of Claim.

Using Claim above we conclude that for each $n \in \mathbb{N}$ we have

$$\alpha_{k+n\ell} \equiv \alpha_{k+(n-1)\ell} \equiv \cdots \equiv \alpha_k \pmod{m}.$$
Problem 5. We compute
\[ F_2 = 1; F_3 = 2; F_4 = 3; F_5 = 5; F_6 = 8; \text{ etc.} \]
So, we have the following sequence of parities
\[ F_0 \text{ is even; } \]
\[ F_1 \text{ is odd; } \]
\[ F_2 \text{ is odd; } \]
\[ F_3 \text{ is even; } \]
\[ F_4 \text{ is odd; } \]
\[ F_5 \text{ is odd; } \]
\[ F_6 \text{ is even; } \text{ etc.} \]
Because of the recurrence relation satisfied by the Fibonacci sequence, we note that the parity of \( F_{n+2} \) is uniquely determined by the parities of \( F_{n+1} \) and of \( F_{n} \). In particular, we observe that for any \( m, n \in \mathbb{N}_0 \), if \( F_m \) and \( F_n \) have the same parity, then also \( F_{m+2} \) and \( F_{n+2} \) have the same parity – see also the solution to Problem 4.
Inspecting the above sequence of parities, we note that \( F_0 \) and \( F_3 \) have the same parity, and \( F_1 \) and \( F_4 \) have the same parity. This means that also \( F_2 \) and \( F_5 \) have the same parity; that \( F_3 \) and \( F_6 \) have the same parity, etc. So, the sequence of parities for \( F_n \) repeats itself with period 3, i.e.
\[ F_{3n} \text{ has the same parity as } F_0; \]
\[ F_{3n+1} \text{ has the same parity as } F_1; \text{ and } \]
\[ F_{3n+2} \text{ has the same parity as } F_2. \]
Now, \( 2011 = 3 \cdot 670 + 1 \), which means that \( F_{2011} \) has the same parity as \( F_1 \), i.e. \( F_{2011} \) is odd.

Problem 6. For each \( i \in \{1, 2, \ldots, \frac{n-1}{2}\} \) we have that \( n - i \equiv -i \) (mod \( n \)) and so,
\[ (n - i)^k \equiv (-i)^k = -i^k \pmod{n}, \]
because \( k \) is an odd integer. Therefore \( i^k + (n - i)^k \equiv 0 \pmod{n} \) for each such \( i = 1, \ldots, \frac{n-1}{2} \). Adding all these congruences, we obtain the desired result.

Problem 7. Because \( x^2 \equiv x \pmod{p} \), we get that \( p \mid (x^2 - x) \), i.e.
\[ p \mid x(x - 1). \]
Because \( p \) is a prime number we obtain that either \( p \mid x \), or \( p \mid (x - 1) \). Therefore \( x \equiv 0 \pmod{p} \), or \( x \equiv 1 \pmod{p} \).

Problem 8. Let \( x_0 \in \mathbb{Z} \) such that \( x_0^3 \equiv 1 \pmod{p} \). Thus \( p \nmid x_0 \); otherwise \( x_0^3 \equiv 0 \pmod{p} \). Because \( p \nmid x_0 \), we get that \( \gcd(x_0, p) = 1 \) and so, by Fermat’s Theorem, we know that
\[ x_0^{p-1} \equiv 1 \pmod{p}. \]
Because \( p \equiv 2 \pmod{3} \), we obtain that there exists \( k \in \mathbb{N} \) such that \( p = 3k + 2 \), and so \( p - 1 = 3k + 1 \). Now, because
\[ x_0^3 \equiv 1 \pmod{p}, \]
raising it to power $k$, we obtain

\[(1) \quad x_{0}^{3k} \equiv 1 \pmod{p}.
\]

But also $x_{0}^{p-1} \equiv x_{0}^{3k+1} \equiv 1 \pmod{p}$. Therefore, using also (1), we obtain

\[1 \equiv x_{0}^{3k+1} \equiv x_{0} \cdot x_{0}^{3k} \equiv x_{0} \pmod{p}.
\]

So, $x_{0} \equiv 1 \pmod{p}$ which shows that indeed there exists a unique solution modulo $p$ of the congruence equation $x^{3} \equiv 1 \pmod{p}$.

Consider now the set $S := \{i^{3} \pmod{p} : 1 \leq i \leq p-1\}$. Each element of $S$ is a nonzero residue modulo $p$. Moreover, for each $i \neq j$ in $\{1, \ldots, p-1\}$, we have

\[(2) \quad i^{3} \not\equiv j^{3} \pmod{p}.
\]

Using (2) we see that indeed $S$ contains $p-1$ distinct elements, and as there are $p-1$ nonzero residues modulo $p$, we conclude that for each nonzero residue $a$ modulo $p$ there exists a unique residue $x$ modulo $p$ such that

\[x^{3} \equiv a \pmod{p}.
\]

Now, in order to prove (2), assume for some $i \neq j$ in $\{1, \ldots, p-1\}$ we have

\[(3) \quad i^{3} \equiv j^{3} \pmod{p}.
\]

Let $\ell \in \{1, \ldots, p-1\}$ such that $\ell \cdot i \equiv 1 \pmod{p}$, i.e. $\ell$ is the inverse of $i$ modulo $p$. Multiplying (3) by $\ell^{3}$ we obtain

\[(j\ell)^{3} \equiv j^{3} \cdot \ell^{3} \equiv i^{3} \cdot \ell^{3} \equiv (i \cdot \ell)^{3} \equiv 1^{3} \equiv 1 \pmod{p}.
\]

So, $x_{1} := j\ell$ is a solution to $x^{3} \equiv 1 \pmod{p}$. However, we saw before that there exists a unique residue modulo $p$ whose cube equals 1 modulo $p$; i.e. $x_{1} \equiv 1 \pmod{p}$. Hence $j\ell \equiv 1 \pmod{p}$ which means that $j$ is the inverse of $\ell$. However, $i$ is the inverse of $\ell$, which means that $i \equiv j \pmod{p}$, which is a contradiction to our assumption that $i \neq j \pmod{p}$. Therefore (2) holds.

**Problem 9.** Using Wilson’s theorem, we have $(p-1)! \equiv -1 \pmod{p}$. So,

\[(4) \quad 1 \cdot 2 \cdot \ldots \left(\frac{p-1}{2}\right) \cdot \left(\frac{p+1}{2}\right) \ldots (p-1) \equiv -1 \pmod{p}.
\]

We have

\[
\begin{align*}
\frac{p+1}{2} & \equiv -\frac{p-1}{2} \pmod{p}, \\
\frac{p+3}{2} & \equiv -\frac{p-3}{2} \pmod{p}, \\
\ldots & \\
(p-1) & \equiv -1 \pmod{p}.
\end{align*}
\]

Using all of the above congruences in (4) we obtain

\[-1 \equiv \left(\frac{p-1}{2}\right) ! \cdot \left(\frac{p-1}{2}\right) \cdot \left(\frac{p-3}{2}\right) \ldots (-1) \equiv (-1)^{\frac{p-1}{2}} \cdot \left(\frac{p-1}{2}\right)!^{2} \pmod{p}.
\]

Because $p \equiv 1 \pmod{4}$, we get that $\frac{p-1}{2}$ is even; hence

\[-1 \equiv (-1)^{\frac{p-1}{2}} = 1.
\]

So, we obtain

\[\left(\frac{p-1}{2}\right)!^{2} \equiv -1 \pmod{p},
\]
which means that indeed, the congruence equation $x^2 \equiv -1 \pmod{p}$ has a solution $x_0$ modulo $p$. Once $x_0$ is a solution, then also $-x_0 \pmod{p}$ is a solution modulo $p$. Obviously,

$$x_0 \not\equiv -x_0 \pmod{p}$$

because otherwise, it would mean that $2x_0 \equiv 0 \pmod{p}$, i.e. $p \mid 2x_0$. Because $p$ is odd, then we would need $x_0 \equiv 0 \pmod{p}$ which is impossible because that would imply that also $x_0^2 \equiv 0 \pmod{p}$, while we know that $x_0^2 \equiv -1 \pmod{p}$. So, indeed $x^2 \equiv -1 \pmod{p}$ has two distinct solutions modulo $p$.

**Problem 10.** Let $S := p^{q-1} + q^{p-1}$. By Fermat’s Theorem, because $\gcd(p, q) = 1$, we obtain that $p^{q-1} \equiv 1 \pmod{q}$. So, $S \equiv 1 \pmod{q}$. Similarly, we obtain that $q^{p-1} \equiv 1 \pmod{p}$, and thus $S \equiv 1 \pmod{p}$. Therefore we obtained that both

$$q \mid (S - 1)$$

and

$$p \mid (S - 1).$$

Because $\gcd(p, q) = 1$ we get that $pq \mid (S - 1)$, and so, $S \equiv 1 \pmod{pq}$.

**Problem 11.** It is easy to check that

$$b_0 = 5 = 3^0(-4\cdot 0 + 5)$$

and

$$b_1 = 3^1(-4\cdot 1 + 5).$$

We prove the statement by induction on $n$; the cases $n = 0$ and $n = 1$ already hold.

So, we assume that for some integer $N \geq 2$ we already proved that

$$b_n = 3^n(-4n + 5)$$

for $0 \leq n < N$.

and next we prove that also $b_N = 3^n(-4N + 5)$. Indeed, we compute using the recursive defined formula and the inductive hypothesis that

$$b_N = 6b_{N-1} - 9b_{N-2}$$

$$= 6 \cdot 3^{N-1}(-4(N - 1) + 5) - 9 \cdot 3^{N-2}(-4(N - 2) + 5)$$

$$= 3^N(-8(N - 1) + 10) - 3^N(-4(N - 2) + 5)$$

$$= 3^N(-8N - 18 + 4N - 8 - 5)$$

$$= 3^N(-4N + 5),$$

as claimed.

**Problem 12.**

(a) Let

$$Q(x) = \sum_{k=0}^{n} c_k \cdot \frac{\prod_{0 \leq i \leq n (x-a_i)} \prod_{0 \leq i \leq n (a_k-a_i)}}{\prod_{0 \leq i \leq n (a_k-a_i)}}.$$ 

then $Q(x) \in \mathbb{C}[x]$ is a polynomial of degree at most $n$. Furthermore, just by construction, we note that $Q(a_k) = c_k = P(a_k)$ for each $k = 0, \ldots, n$.

Indeed, when we plug in $x = a_k$ in $Q(x)$ then all of its terms vanish with the exception of its $k$-th term which simplifies exactly to $c_k$. 
Therefore the polynomial \( R(x) = P(x) - Q(x) \) has the property that it has degree at most \( n \) (being the difference of two polynomials of degrees at most \( n \)) and furthermore,
\[
R(a_k) = 0 \quad \text{for} \quad k = 0, \ldots, n.
\]
Since a nonzero polynomial cannot have more roots than its degree, we conclude that \( R(x) = 0 \), i.e. \( P(x) = Q(x) \), as desired.

(b) We let \( c_k = P(k) \) for each \( k = 0, \ldots, n \). By part (a), we get that
\[
P(x)
= \sum_{k=0}^{n} (-1)^{n-k} c_k \cdot \frac{\Pi_{0 \leq i \leq n(x-i)}}{\Pi_{i \not\in k}(k-i)}.
\]
We have to prove that \( P(\ell) \in \mathbb{Z} \) for each \( \ell \in \mathbb{Z} \). We already know that \( P(\ell) \in \mathbb{Z} \) for \( \ell = 0, \ldots, n \). So, we split the remaining integers into two cases.

**Case 1.** \( \ell = -m \) for some \( m \in \mathbb{N} \).

In this case,
\[
P(-m)
= \sum_{k=0}^{n} (-1)^{n-k} c_k \cdot \frac{\Pi_{0 \leq i \leq n(-(m-i))}}{\Pi_{i \not\in k}(m-i)}
= \sum_{k=0}^{n} (-1)^{(n-k)+m} c_k \cdot \frac{\Pi_{0 \leq i \leq n(m+i)}}{\Pi_{i \not\in k}(m+i)}
= \sum_{k=0}^{n} (-1)^{-k} c_k \cdot \frac{(m+k-1)!}{k!(m-k)!} \cdot \frac{(m+n)!}{(n-k)!(m+k)!}
= \sum_{k=0}^{n} (-1)^{k} c_k \binom{m+k-1}{k} \binom{m+n}{n-k}
\]
is an integer.

**Case 2.** \( \ell = m \) for some \( m \in \mathbb{N} \) satisfying \( m \geq n+1 \).

In this case,
\[
P(m)
= \sum_{k=0}^{n} (-1)^{n-k} c_k \cdot \frac{\Pi_{0 \leq i \leq n(m-i)}}{\Pi_{i \not\in k}(m-k)!}
= \sum_{k=0}^{n} (-1)^{n-k} c_k \cdot \frac{m!}{(m-k)!} \cdot \frac{(m-k-1)!}{(n-k)!((m-n-1)!}
= \sum_{k=0}^{n} (-1)^{n-k} c_k \binom{m}{k} \binom{m-k-1}{n-k}
\]
is an integer as well.

(c) For each \( k = 0, \ldots, n \) we let \( c_k = P(k) \). Then we know that
\[
P(x)
= \sum_{k=0}^{n} (-1)^{n-k} c_k \cdot \frac{\Pi_{0 \leq i \leq n(x-i)}}{\Pi_{i \not\in k}(x-i)}
= \frac{1}{n!} \sum_{k=0}^{n} (-1)^{n-k} c_k \binom{n}{k} \cdot \Pi_{0 \leq i \leq n}(x - i).
\]
Therefore \( n! P(x) \) is a polynomial with integer coefficients (note that each \( c_k \) is an integer).

(d) For each \( n \geq 2 \), we let

\[
P_n(x) = \frac{x(x-1) \cdots (x-n+1)}{n!}.
\]

Then for \( x = -m \) for \( m \in \mathbb{N} \), we have

\[
P_n(-m) = (-1)^n \frac{m(m+1) \cdots (m+n-1)}{n!} = (-1)^n \binom{m+n-1}{n}
\]

is an integer. Clearly for \( x \in \{0, \ldots, n-1\} \) we have \( P(x) = 0 \), while for \( x = m \geq n \) we have

\[
P_n(m) = \binom{m}{n}
\]

is also an integer.

So, \( P_n(x) \in \mathbb{Z} \) for each \( x \in \mathbb{Z} \). However, the leading coefficient of \( P_n(x) \) is \( \frac{1}{n!} \) which is not an integer (for \( n \geq 2 \)).

**Problem 13.**

(a) As in the Problem 3, in order to find the general term of the above linear recurrence sequence, we first find the roots of the quadratic equation:

\[
x^2 - x - 1 = 0
\]

which are \( r_1 = \frac{1+\sqrt{5}}{2} \) and \( r_2 = \frac{1-\sqrt{5}}{2} \). Then all we need to do is find \( c_1, c_2 \in \mathbb{C} \) such that

\[
F_0 = c_1 + c_2 \quad \text{and} \quad F_1 = c_1 r_1 + c_2 r_2.
\]

A simple computation yields that \( c_1 = \frac{1}{\sqrt{5}} \) and \( c_2 = -\frac{1}{\sqrt{5}}. \) Thus indeed

\[
F_n = \frac{1}{\sqrt{5}} \left( \frac{1+\sqrt{5}}{2} \right)^n - \frac{1}{\sqrt{5}} \left( \frac{1-\sqrt{5}}{2} \right)^n
\]

for each \( n \geq 0 \).

(b) Let \( m \in \mathbb{N} \). We consider the function

\[
\Phi : \mathbb{N} \rightarrow \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}
\]

given by \( \Phi(n) = (\overline{F_n}, \overline{F_{n-1}}) \) where \( \overline{x} \) always represents the reduction of the integer \( x \) modulo \( m \). Note that \( |\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}| = m^2 \), which yields that the function \( \Phi \) cannot be injective. Let \( n_0 \) be the smallest positive integer such that there exists \( n_1 > n_0 \) such that \( \Phi(n_0) = \Phi(n_1) \). In particular this means that

\[
\overline{F_{n_0}} = \overline{F_{n_1}} \quad \text{and} \quad \overline{F_{n_0-1}} = \overline{F_{n_1-1}}.
\]

**Claim 1.** \( n_0 = 1 \).

Indeed, assume \( n_0 \geq 2 \). Then

\[
\overline{F_{n_0-2}} = \overline{F_{n_0}} - \overline{F_{n_0-1}} = \overline{F_{n_0}} - \overline{F_{n_0-1}} = \overline{F_{n_1}} - \overline{F_{n_1-1}} = \overline{F_{n_1}} - \overline{F_{n_1-1}} = \overline{F_{n_1-2}}.
\]

But that means that \( \overline{F_{n_0}} = \overline{F_{n_1}} \) and \( \overline{F_{n_0-1}} = \overline{F_{n_1-1}} \), which yields that \( \Phi(n_0 - 1) = \Phi(n_1 - 1) \), contradicting hence the minimality assumption regarding \( n_0 \). Therefore \( n_0 \) has to equal 1.

**Claim 2.** Let \( \ell = n_1 - 1 \). Then \( \overline{F_{n+\ell}} = \overline{F_n} \) for each integer \( n \geq 0 \).
We prove this Claim 2 by induction on \( n \). We already know that the statement holds for \( n = 0 \) and \( n = 1 \) (note that we just proved that \( a_0 = 1 \) and thus \( F_0 = F_{n_1} \) and \( F_1 = F_{n_1} \)). So, we assume that the conclusion of Claim 2 holds for all \( n < k \) (for some \( k \geq 2 \)) and next we show that it holds also for \( n = k \). Indeed,
\[
F_k = F_{k-1} + F_{k-2} = F_{k-1} + F_{k-2} = F_{k-1+\ell} + F_{k-2+\ell} = F_{k+\ell}.
\]
This concludes the proof of Claim 2.

Using Claim 2 we conclude that for each \( n \in \mathbb{N} \) we have
\[
F_{n\ell} = F_{n-1}\ell = \cdots = F_{\ell} = F_0 = 0.
\]
Thus \( m \mid F_{n\ell} \) for each \( n \geq 0 \) which yields the conclusion of part (b).

**Problem 14.** First we check the statement for \( p = 2 \). We note that
\[
\binom{1}{0} \equiv 1 \equiv (-1)^0 \pmod{2}
\]
and
\[
\binom{1}{1} \equiv 1 \equiv (-1)^1 \pmod{2}.
\]
So, from now on we assume \( p \) is an odd prime. Let \( k \in \{0, \ldots, p-1\} \). Clearly, for each \( i \in \{k+1, \ldots, p-1\} \) we have \( i \equiv -(p-i) \pmod{p} \). So,
\[
\prod_{i=k+1}^{p-1} i \equiv (-1)^{p-k-1} \prod_{i=k+1}^{p-1} (p-i) \equiv (-1)^k(p-k-1)! \pmod{p}.
\]
Note that in the above congruence we used the fact that \( (p-k-1) \equiv k \pmod{2} \) since \( p \) is an odd number.

Therefore
\[
(p-1)! \equiv k! \cdot \prod_{i=k+1}^{p-1} i \equiv (-1)^k \cdot k!(p-1-k)! \pmod{p}.
\]
Now let \( a \in \mathbb{F}_p \) represent the residue class of \( k!(p-1-k)! \) modulo \( p \). Since for each \( k \in \{0, \ldots, p-1\} \) we know that \( p \) divides none of the factors appearing in \( k!(p-1-k)! \) we conclude that \( a \in \mathbb{F}_p^* \) and hence it has an inverse \( a^{-1} \). Multiplying the last congruence by this inverse leads to the desired congruence:
\[
\binom{p-1}{k} \equiv (-1)^k \pmod{p}.
\]

**Problem 15.** By Fermat’s Theorem we know that
\[
a^p \equiv a \pmod{p} \quad \text{and also} \quad b^p \equiv b \pmod{p}.
\]
Since \( a^p \equiv b^p \pmod{p} \) we get that \( a \equiv b \pmod{p} \). So, there exists \( k \in \mathbb{Z} \) such that \( a = b + pk \). Hence
\[
a^p - b^p = (b + pk)^p - b^p = \sum_{i=1}^{p} \binom{p}{i} b^{p-i}(pk)^i = \sum_{i=1}^{p} p^i \binom{p}{i} b^{p-i} k^i.
\]
Now, as proved in Practice Set 2, \( \binom{p}{i} \) is divisible by \( p \) for each \( i = 1, \ldots, p - 1 \). So, for each \( i = 1, \ldots, p - 1 \),
\[
p^2 \mid p^i \binom{p}{i} p^{p-i} k^i.
\]
For \( i = p \), we have the following term in the above sum: \( p^p k^p \) which is clearly divisible by \( p^2 \) since \( p \geq 2 \). In conclusion,
\[
a^p - b^p \equiv 0 \pmod{p^2},
\]
as desired.

**Problem 16.** We can easily see that for \( p = 2 \) and \( p = 3 \) there are no solutions, while for \( p = 5 \) we get that \( 3! = 5^1 + 1 \), i.e., \( (p, n) = (5, 1) \) is a solution for the above equation. Next we will prove that for \( p > 5 \) there are no solutions of the above equation.

We assume there exists a prime \( p > 5 \) and a positive integer \( n \) such that
\[
(p-2)! = p^n + 1.
\]
Therefore \( p \geq 7 \) and so, \( p - 1 > 4 \) is a composite number (it is even and larger than 4, because \( p \) is prime and larger than 5) which allows us to use one of the results from Practice Set 1 to conclude that
\[
(p-1) \mid (p-2)!
\]
So,
\[
(p-1) \mid p^n + 1.
\]
However
\[
p \equiv 1 \pmod{p-1} \quad \text{which yields that} \quad p^n \equiv 1 \pmod{p-1}.
\]
Hence
\[
0 \equiv p^n + 1 \equiv 2 \pmod{p-1}.
\]
Therefore \( (p-1) \mid 2 \) which contradicts the fact that \( p > 3 \). In conclusion, the only solution \( (p,n) \) to the above equation is \( (5,1) \).

**Problem 17.** We need to show that
\begin{align*}
\text{(5)} & \quad 2 \mid (n^9 - n) \\
\text{(6)} & \quad 3 \mid (n^9 - n) \\
\text{(7)} & \quad 5 \mid (n^9 - n).
\end{align*}
If \( n \) is even, then (5) holds. If \( n \) is odd, we also see that (5) holds. Therefore (5) holds for all \( n \in \mathbb{Z} \) (note that \( n^9 \) and \( n \) have the same parity always).

If \( 3 \mid n \), then (6) holds (since then also \( 3 \mid n^9 \)). If \( 3 \nmid n \), then we may use Fermat’s Theorem and conclude that \( n^2 \equiv 1 \pmod{3} \). Therefore, after raising the last congruence to power 4, we get \( n^8 \equiv 1 \pmod{3} \), and thus \( 3 \mid (n^8 - 1) \). Finally, we multiply by \( n \), and obtain that indeed (6) holds.

If \( 5 \mid n \), then (7) holds (since then also \( 5 \mid n^9 \)). If \( 5 \nmid n \), then we may use Fermat’s Theorem and conclude that \( n^4 \equiv 1 \pmod{5} \). Therefore, after raising the last congruence to power 2, we get \( n^8 \equiv 1 \pmod{5} \), and thus \( 5 \mid (n^8 - 1) \). Finally, we multiply by \( n \), and obtain that indeed (7) holds.
Because \((n^9 - n)\) is divisible by the distinct prime numbers 2, 3 and 5, we conclude that \((n^9 - n)\) is divisible by \(2 \cdot 3 \cdot 5 = 30\).

**Problem 18.** Indeed, if we assume \(2^\ell - 1 = p^a\) for some prime number \(p\) and some integer \(a \geq 2\), then we immediately get that \(p\) must be odd.

Now, if \(a\) were even, then \(p^a \equiv 1 \pmod{8}\) (since \(p\) is odd) and thus we would get that \(2^\ell \equiv 2 \pmod{8}\) which contradicts the fact that \(\ell \geq 2\).

So, \(a\) must be odd. Therefore

\[
2^\ell = p^a + 1 = (p + 1)(p^{a-1} - p^{a-2} + \cdots - p + 1).
\]

Because \(a\) is odd and also \(p\) is odd, we get that each integer from the above parenthesis is odd and there is an odd number of them, thus proving that parenthesis is an odd integer. This contradicts the fact that the left hand side is a power of 2, unless the parenthesis is equal to 1, i.e., \(2^\ell - 1 = p\), as desired.

**Problem 19.** We argue by induction on \(n\). For \(n = 1, \ldots, p - 1\) the statement is obvious. Now, assume the statement holds for all \(n < N\) and we prove it next for \(n = N\). Clearly, we may assume \(N \geq p\).

Let \(M\) be the largest positive integer such that \(p^M \leq N\); hence \(p^{M+1} > N\). Then we let \(c_M = \left\lfloor \frac{N}{p^M} \right\rfloor\).

Therefore, we obtain that \(0 < c_M \leq p - 1\). Moreover by our choice of \(c_M\) we obtain that \(0 \leq N - c_M p^M < p^M\).

If \(N - c_M p^M = 0\), then the \(p\)-adic expansion of \(N\) is simply

\[
c_M \cdot p^M + 0 \cdot p^{M-1} + \cdots + 0 \cdot p + 0.
\]

Now, if \(N - c_M p^M > 0\) then by the induction hypothesis there exists a unique \(p\)-adic expansion of \(N - c_M p^M\); furthermore since \(N - c_M p^M < p^M\), then the left-most \(p\)-adic digit of \(N - c_M p^M\) corresponds to a power less than \(p^M\).

Now to see the uniqueness of the \(p\)-adic expansion for \(N\), note that any \(p\)-adic expansion for \(N\) would have to have the left-most \(p\)-adic digit correspond to the power \(p^M\) because \(p^M \leq N < p^{M+1}\) and

\[
(p - 1)p^{M-1} + (p - 1)p^{M-2} + \cdots + (p - 1) \cdot p + (p - 1) = p^M - 1 < p^M.
\]

Furthermore, the left-most \(p\)-adic digit of any \(p\)-adic expansion for \(N\) would have to be \(\left\lfloor \frac{N}{p^M} \right\rfloor\) because of the same argument as above. The the inductive hypothesis yields the uniqueness of the \(p\)-adic expansion for \(N\) using the uniqueness for the \(p\)-adic expansion of \(N - c_M p^M\).

**Problem 20.** We add \(a_{n+1}\) on both sides of the recurrence formula:

\[
a_{n+2} + a_{n+1} = (n + 1)a_{n+1} + (n + 1)a_n.
\]

We let \(b_n := a_{n+1} + a_n\) for each \(n \in \mathbb{N}\). Then \(b_1 = 3\) and

\[
b_{n+1} = (n + 1) \cdot b_n \text{ for all } n \in \mathbb{N}.
\]

So,

\[
b_n = n \cdot (n - 1) \cdots 3 \cdot 2 \cdot b_1 = 3 \cdot n!.
\]
Therefore
\[ b_n - b_{n-1} + b_{n-2} - b_{n-3} + \cdots + (-1)^{n-1}b_1 \]
\[ = (a_{n+1} + a_n) - (a_n + a_{n-1}) + (a_{n-1} + a_{n-2}) - (a_{n-2} + a_{n-3}) + \cdots + (-1)^{n-1}(a_2 + a_1) \]
\[ = a_{n+1} + (-1)^{n-1}a_1 \]

and so,
\[ a_{n+1} = 2(-1)^n + 3(-1)^{n-1} \cdot 1! + \cdots - 3 \cdot (n-3)! + 3 \cdot (n-2)! - 3 \cdot (n-1)! + 3 \cdot n! \]

In conclusion,
\[ a_n = (-1)^n + 3 \cdot \sum_{i=0}^{n-1} (-1)^i \cdot (n-1-i)! \]

**Problem 21.**

\( p = 2 \) We have that \( 2^{10} \leq 2012 < 2^{11} \) and so, \( 2012 = 2^{10} + 988. \) Then \( 2^9 \leq 988 < 2^{10} \) and thus \( 988 = 2^9 + 476. \) Then \( 2^8 \leq 476 < 2^9 \) and so, \( 476 = 2^8 + 220. \) Then \( 2^7 \leq 220 < 2^8 \) and so, \( 220 = 2^7 \cdot 7 \). Then \( 2^7 \leq 92 < 2^8 \) and so, \( 92 = 2^6 + 28 \). Then \( 2^6 \leq 28 < 2^7 \) and so, \( 28 = 2^6 + 2. \) Finally, \( 12 = 2^3 + 2^2. \) So,
\[ 2012 = 2^{10} + 2^9 + 2^8 + 2^7 + 2^6 + 2^4 + 2^3 + 2^2 = \text{1111111111}. \]

\( p = 3 \) We have that \( 3^6 \leq 2012 < 3^7. \) Moreover, \( 2012 = 2 \cdot 3^6 + 554 \) where \( 3^5 \leq 554 < 3^6. \) We have that \( 554 = 2 \cdot 3^5 + 68 \) where \( 3^4 \leq 68 < 3^5. \) So, \( 68 = 2 \cdot 3^3 + 14 \) where \( 3^2 \leq 14 < 3^3. \) Finally, \( 14 = 2^3 + 5, \) and \( 5 = 3^1 + 2. \) Thus
\[ 2012 = 2 \cdot 3^6 + 2 \cdot 3^5 + 2 \cdot 3^3 + 3^2 + 3^1 + 2 = \text{3333112}. \]

\( p = 5 \) We have that \( 5^4 \leq 2012 < 5^5. \) Moreover, \( 2012 = 3 \cdot 5^4 + 137 \) where \( 5^3 \leq 137 < 5^4. \) So, \( 137 = 5^3 + 12, \) where \( 12 = 2 \cdot 5^1 + 2. \) So,
\[ 2012 = 3 \cdot 5^4 + 5^3 + 2 \cdot 5^1 + 2 = \text{311022}. \]

\( p = 7 \) We have that \( 7^3 \leq 2012 < 7^4. \) Moreover \( 2012 = 5 \cdot 7^3 + 297 \) where \( 7^2 \leq 297 < 7^3. \) Moreover \( 297 = 6 \cdot 7^2 + 3 \) and so,
\[ 2012 = 5 \cdot 7^3 + 6 \cdot 7^2 + 3 = \text{5603}. \]

**Problem 22.** We know that the \( p \)-adic exponent in each factorial \( n! \) equals
\[ \sum_{i=1}^{\lfloor n/p \rfloor} \left[ \frac{n}{p^i} \right] \]
where \( \lfloor x \rfloor \) represents the integral part of the real number \( x. \) So, \( p \mid \binom{n}{k} \) if and only if there exists some \( i \geq 1 \) such that
\[ \left[ \frac{n}{p^i} \right] - \left[ \frac{k}{p^i} \right] - \left[ \frac{n-k}{p^i} \right] > 0. \] (8)

Note that the above left-hand side is always at least equal to 0 since \( \lfloor x+y \rfloor \geq \lfloor x \rfloor + \lfloor y \rfloor \) for any two real numbers \( x \) and \( y. \) Now, we know that
\[ n = a_m a_{m-1} \dots a_1 a_0 \] and \( k = b_q b_{q-1} \dots b_1 b_0. \]
so in particular \( \ell \leq m \) since \( k \leq n \). If \( \ell < m \) we let \( b_i = 0 \) for each \( i \in \{ \ell + 1, \ldots, m \} \). For each \( i > m \) clearly (8) cannot be satisfied since \( \left[ \frac{a}{p^i} \right] = 0 \). On the other hand, for each \( i \in \{1, \ldots, m \} \) we have that

\[
\left[ \frac{n}{p^i} \right] = a_m a_{m-1} \ldots a_i
\]

and similarly

\[
\left[ \frac{k}{p^i} \right] = b_m b_{m-1} \ldots b_i
\]

where in the last \( p \)-adic expansion we allow the possibility that the first \( p \)-adic digits be equal to 0. Hence (8) holds if and only if

\[
(a_m - b_m)(a_{m-1} - b_{m-1}) \ldots (a_i - b_i)(a_0 - b_0)
\]

(9)

Alternatively, noting that always we have

\[
\left[ \frac{n - k}{p^i} \right] = a_m a_{m-1} \ldots a_i - b_m b_{m-1} \ldots b_i,
\]

we get that (8) does not hold if and only if

\[
\left[ \frac{n - k}{p^i} \right] = a_m a_{m-1} \ldots a_i - b_m b_{m-1} \ldots b_i.
\]

Now, if \( b_i \leq a_i \) for each \( i \) then

\[ n - k = (a_m - b_m)(a_{m-1} - b_{m-1}) \ldots (a_1 - b_1)(a_0 - b_0) \]

with the same convention as above regarding digits of 0 in the beginning of the expansion, and thus for each \( i \) we would have

\[
\left[ \frac{n}{p^i} \right] - \left[ \frac{k}{p^i} \right] - \left[ \frac{n - k}{p^i} \right] = 0.
\]

So, \( b_i \leq a_i \) for each \( i \) yields that \( p \mid \binom{n}{k} \).

On the other hand, let \( i_0 \) be the largest integer \( i \) such that \( b_i > a_i \); clearly \( i_0 < m \). Then

\[
a_m a_{m-1} \ldots a_{i_0+2} a_{i_0+1} - b_m b_{m-1} \ldots b_{i_0+2} b_{i_0+1} = (a_m - b_m)(a_{m-1} - b_{m-1}) \ldots (a_{i_0+2} - b_{i_0+2})(a_{i_0+1} - b_{i_0+1}).
\]

But \( n - k \) does not have the first \( (m - i_0) \) \( p \)-adic digits (counting possibly some 0’s in the beginning of the expansion) be

\[
(a_m - b_m)(a_{m-1} - b_{m-1}) \ldots (a_{i_0+2} - b_{i_0+2})(a_{i_0+1} - b_{i_0+1})
\]

because \( a_{i_0} < b_{i_0} \). Hence, if \( a_i < b_i \) then indeed \( p \mid \binom{n}{k} \).

**Problem 23.** The characteristic equation for our sequence is \( x^2 - x - 1 = 0 \) whose roots are \( \frac{1+\sqrt{5}}{2} \) and \( \frac{1-\sqrt{5}}{2} \). We search for the general term of the sequence \( a_n \) of the form

\[
ce_1 \cdot \left( \frac{1 + \sqrt{5}}{2} \right)^n + c_2 \cdot \left( \frac{1 - \sqrt{5}}{2} \right)^n.
\]
We solve for \(c_1\) and \(c_2\) by using the fact that \(a_1 = 1\) and \(a_2 = 3\) and obtain that \(c_1 = c_2 = 1\). So,

\[
a_n = \left(\frac{1 + \sqrt{5}}{2}\right)^n + \left(\frac{1 - \sqrt{5}}{2}\right)^n
\]

and thus

\[
a_{2n} = \left(\frac{1 + \sqrt{5}}{2}\right)^{2n} + \left(\frac{1 - \sqrt{5}}{2}\right)^{2n}.
\]

We note that

\[
\left(\frac{1 + \sqrt{5}}{2}\right)^2 = 3 + \sqrt{5} \quad \text{and} \quad \left(\frac{1 - \sqrt{5}}{2}\right)^2 = 3 - \sqrt{5},
\]

which finishes our proof.

**Problem 24.** We first claim that \(4^n - 1 \equiv 0 \pmod{3}\) for all \(n \in \mathbb{N}\). Indeed, \(4 \equiv 1 \pmod{3}\) and therefore \(4^n \equiv 1^n \pmod{3}\) for all \(n \in \mathbb{N}\). In conclusion, 

\[3 \mid (4^n - 1)\] for all \(n \in \mathbb{N}\).

Next we claim that

\[9 \mid (4^{3n} - 1)\] for all \(n \in \mathbb{N}\).

Indeed,

\[4^{3n} - 1 = (4^n - 1) \left((4^n)^2 + 4^n + 1\right) .
\]

But, \((4^n)^2 + 4^n + 1 \equiv 1^2 + 1 + 1 \equiv 0 \pmod{3}\), and therefore,

\[9 \mid 4^{3n} - 1 .
\]

So, \(9 \mid 4^{3n} + 15 \cdot (3n) - 1\) for all \(n \in \mathbb{N}\).

Next we claim that

\[9 \mid 4^{3n+1} + 15 \cdot (3n + 1) - 1 ,
\]

since

\[4^{3n+1} = 4 \cdot 4^{3n} \equiv 4 \pmod{9}\]

and \(15 \cdot (3n + 1) \equiv 15 \equiv -3 \pmod{9}\). So, indeed

\[9 \mid 4^{3n+1} + 15 \cdot (3n + 1) - 1 .
\]

Finally, we claim that

\[9 \mid 4^{3n+2} + 15 \cdot (3n + 2) - 1 .
\]

Indeed,

\[4^{3n+2} = 16 \cdot 4^{3n} \equiv 16 \equiv -2 \pmod{9}\]

and

\[15 \cdot (3n + 2) \equiv 30 \equiv 3 \pmod{9} .
\]

Therefore

\[4^{3n+2} + 15(3n + 2) - 1 \equiv -2 + 3 - 1 \equiv 0 \pmod{9} ,
\]

as desired.

So, for all \(n \in \mathbb{N}\) the above congruence holds.

**Problem 25.** Since \(n^2 - 1 = (n - 1)(n + 1)\), we obtain that

\[6 \mid n^2 - 1\] if and only if \(n \equiv 1 \pmod{2}\) and \(n \equiv \pm 1 \pmod{3}\).
On the other hand, 
\[ 10^n - 2^n - 8 \equiv 1 - (-1)^n + 1 \pmod{3}. \]
Thus \(3 \mid (10^n - 2^n - 8)\) if and only if \(n\) is odd.

Also, letting \(n = 3k + b\) with \(b \in \{0, 1, 2\}\) and \(k\) a nonnegative integer, we obtain
\[
10^n - 2^n - 8 \\
= 1000^k \cdot 10^b - 8^k \cdot 2^b - 8 \\
\equiv (-1)^k \cdot 10^b - 2^b - 1 \pmod{7}.
\]
Now if \(b = 0\), then the above congruence yields
\[ (-1)^k - 1 - 1 \not\equiv 0 \pmod{7}. \]
On the other hand, if \(b = 1\), then \(n = 3k + 1\) and because \(n\) is odd, then \(k\) must be even. Thus the above congruence yields
\[ 1 \cdot 10 - 2 - 1 \equiv 0 \pmod{7}. \]
Now, if \(b = 2\), then \(n = 3k + 2\) and because \(n\) is odd, then \(k\) must be odd. So the above congruence yields
\[ -1 \cdot 100 - 4 - 1 \equiv 0 \pmod{7}. \]
In conclusion, \(21 \mid (10^n - 2^n - 8)\) if and only if \(n\) is odd and also \(n \equiv \pm 1 \pmod{3}\).

**Problem 26.** Assume there exists an integer \(x\) such that
\[ x^2 = 1! + 4! + \cdots + (3n + 1)!. \]
If \(n = 1\) then \(x = 5\) works. On the other hand, if \(n = 2\) we have
\[ 1! + 4! + 7! = 5065 \equiv 15 \pmod{25}. \]
On the other hand, \(x^2 \equiv 15 \pmod{25}\) cannot hold since once \(5 \mid x^2\) then \(5 \mid x\) and so \(25 \mid x^2\).

So, from now on assume \(n \geq 3\). Then
\[ 7! = 5040 \equiv 15 \pmod{25}, \]
while for all \(m \in \{3, \ldots, n\}\) we have
\[ (3m + 1) \geq 10 \text{ and so,} \]
\[ 5 \cdot 10 \mid (3m + 1)!. \]
Therefore
\[ 10! + \cdots + (3n + 1)! \equiv 0 \pmod{25}. \]
So,
\[ x^2 = 1! + 4! + 7! + 10! + \cdots + (3n + 1)! \equiv 15 \pmod{25} \]
which is impossible, as explained above.

**Problem 27.** Let \(x \in \mathbb{N}\) be relatively prime with 3. Then
\[ x \cdot 3^{f(y)} \mid f(x) \cdot 3^y \]
yields \(x \mid f(x)\). So, in particular, \(f(x) \geq x\) if \(3 \nmid x\). We’ll show next that \(f(x) = x\).

We let \(y = x\) (arbitrary positive integer) and then we conclude because of the divisibility that
\[ \frac{3^{f(x)}}{f(x)} \leq \frac{3^x}{x}. \]
We consider the function $g : \mathbb{R}_{\geq 1} \rightarrow \mathbb{R}$ given by
$$g(z) = \frac{3^z}{z}.$$ 

Then
$$g'(z) = \frac{3^z \cdot \ln(3) \cdot z - 3^z}{z^2} > 0,$$
if $z \geq 1$ and so, (12) yields $f(x) \leq x$. Together with $f(x) \geq x$ we obtain that $f(x) = x$ for all $x$ not divisible by 3.

Letting $x$ be relatively prime with 3 and $y$ arbitrary in the divisibility (11) we conclude that $3^f(y) | 3^y$ (since $f(x) = x$), i.e., $f(y) \leq y$ for all $y$.

On the other hand, letting $y$ be relatively prime with 3 and $x$ arbitrary, we use that $f(y) = y$ in (11) and conclude that $x | f(x)$, which yields that $f(x) \geq x$ for all $x$.

Therefore $f(z) = z$ for all $z \in \mathbb{N}$.

**Problem 28.** The answer is no. Here’s the proof: assume there exists such a positive integer $m$. The number $n! \cdot 2^{m-n}$ is a positive integer if and only if the exponent of 2 in $n!$ is at least equal to $n - m$ for every positive integer $n$.

The exponent of 2 in $n!$ is precisely equal to:
$$\sum_{i=1}^{\infty} \left\lfloor \frac{n}{2^i} \right\rfloor.$$ 

For each positive integer $k$ we compute the exponent of 2 in $(2^k - 1)!$ to be equal to:
$$\sum_{i=1}^{\infty} \left\lfloor \frac{2^k - 1}{2^i} \right\rfloor$$
$$= \sum_{i=1}^{k-1} \left\lfloor \frac{2^k - 1}{2^i} \right\rfloor$$
$$= \sum_{i=1}^{k-1} (2^k - 1 - 2^{k-i})$$
$$= (2 + \cdots + 2^{k-1}) - (k - 1)$$
$$= 2^k - k - 1.$$ 

So, the exponent of 2 in $(2^k - 1)! \cdot 2^{m-2^k+1}$ is equal to
$$2^k - k - 1 + m - 2^k + 1 = m - k$$
which is negative if $k > m$. Therefore, there exists no positive integer $m$ such that for all positive integers $n$ we would have that $n! \cdot 2^{m-n}$ is a positive integer.

**Problem 29.** We’ll show that if $e$ is not a rational number, then there exist at most finitely many pairs $(m, n)$ as above.

We first find the general formula for $a_n$, respectively $b_n$. We have:
$$\frac{a_{n+1}}{n!} = \frac{a_n}{(n-1)!} - \frac{1}{n!}.$$
So,

\[
a_{n+1} = a - \sum_{k=1}^{n} \frac{1}{k!};
\]

thus

\[
a_n = (n-1)! \cdot \left( a - \sum_{k=1}^{n-1} \frac{1}{k!} \right).
\]

A similar analysis yields

\[
b_n = (n-1)! \cdot \left( b + \sum_{k=1}^{n-1} \frac{1}{k!} \right).
\]

Since \( a \geq 2 \) and \( \sum_{k=1}^{\infty} \frac{1}{k!} = e - 1 < 2 \) (note that \( \sum_{k=1}^{\infty} \frac{1}{k!} < 1 + \sum_{k=2}^{\infty} \frac{1}{k(k-1)} = 2 \)), we conclude that \( \lim_{n \to \infty} a_n = \infty \). Similarly, \( \lim_{n \to \infty} b_n = \infty \).

Assume there exist infinitely many pairs \((m_i, n_i) \in \mathbb{N} \times \mathbb{N}\) such that \( a_{m_i} = b_{n_i} \).

Because \( \lim_{n \to \infty} a_n = \infty \) and \( \lim_{n \to \infty} b_n = \infty \), then both the first and the second entries in those pairs \((m_i, n_i)\) grow arbitrarily large (i.e., \( \lim_{i \to \infty} m_i = \infty \) and \( \lim_{i \to \infty} n_i = \infty \)). Therefore

\[
\lim_{i \to \infty} \frac{a - \sum_{k=1}^{m_i-1} \frac{1}{k!}}{b + \sum_{k=1}^{n_i-1} \frac{1}{k!}} = \frac{a - e + 1}{b + e - 1}.
\]

Furthermore, since \( e \notin \mathbb{Q} \), then \( \frac{a - e + 1}{b + e - 1} \notin \mathbb{Q} \). Since \( a_{m_i} = b_{n_i} \), the formulas for the \( a_k \)'s and for the \( b_k \)'s coupled with limit (13) yield that

\[
\lim_{i \to \infty} \frac{(n_i - 1)!}{(m_i - 1)!} = \frac{a - e + 1}{b + e - 1} \notin \mathbb{Q}.
\]

In case it exists, there are three possibilities for the limit

\[
\lim_{i \to \infty} \frac{(n_i - 1)!}{(m_i - 1)!}
\]

either 0, or 1, or \( \infty \) depending on whether \( m_i > n_i \) for all \( i \) sufficiently large, or \( m_i = n_i \) for all \( i \) sufficiently large, or \( m_i < n_i \) for all \( i \) sufficiently large. (If at least two of the possibilities: \( m_i > n_i \), or \( m_i = n_i \), or \( m_i < n_i \) occur infinitely often then the limit (14) does not exist.) In either case, the limit (14) cannot be \( \frac{a - e + 1}{b + e - 1} \notin \mathbb{Q} \) which yields the desired conclusion.