Solutions to selected problems from homework 3

(1) Give a proof by induction of the following statement used class:

Let \( m > 1 \) be a natural number. Then for any \( n \geq 0 \) there exists an integer \( r \) such that \( 0 \leq r < m \) and \( n \equiv r \pmod{m} \).

Solution

We prove it by induction on \( n \geq 0 \). When \( n = 0 \) then \( r = 0 \) obviously satisfies \( 0 \equiv 0 \pmod{m} \). This verifies the base of induction.

Suppose we have proved the statement for some \( n \geq 0 \). We need to prove it for \( n + 1 \).

\begin{align*}
\text{Case 1.} & \quad 0 \leq r < m - 1. \\
& \quad \text{Then } 0 \leq r + 1 < m \text{ and } n + 1 \equiv r + 1 \pmod{m}, \text{i.e. } r + 1 \text{ satisfies the statement for } n + 1.
\end{align*}

\begin{align*}
\text{Case 2.} & \quad r = m - 1. \\
& \quad \text{Then } r + 1 = m \text{ and } n + 1 \equiv r + 1 \equiv m \equiv 0 \pmod{m}, \text{i.e. } 0 \text{ satisfies the statement for } n + 1.
\end{align*}

This concludes the induction step. \( \square \).

(2) (a) Find \( 2^{3^{100}} \pmod{5} \)

(b) Find the last digit of \( 2^{3^{100}} \).

Hint: use part a) but remember that 10 is not prime.

Solution

(a) Since 5 is prime and 5 does not divide 2, by Fermat’s theorem \( 2^4 \equiv 1 \pmod{5} \). This can also be seen directly by computing \( 2^4 = 16 \equiv 1 \pmod{5} \). Therefore, \( 2^{4k} \equiv 1^{4k} \equiv 1 \pmod{5} \) for any \( k \geq 1 \). Thus we need to find the remainder \( r \) when \( 3^{100} \) is divided by 4. Then \( 3^{100} = 4k + r \) and \( 2^{3^{100}} \equiv 2^{4k+r} \equiv 2^{4k} \cdot 2^r \equiv 2^r \pmod{5} \).

To this end observe that \( 3 \equiv -1 \pmod{4} \) and hence \( 3^2 \equiv (-1)^2 \equiv 1 \pmod{4} \). Therefore \( 3^{2m} \equiv 1 \pmod{4} \) for any \( m \geq 1 \). In particular, \( 3^{100} = 3^{2 \cdot 50} \equiv 1 \pmod{4} \). Therefore, \( 3^{100} = 4k + 1 \) for some \( k \) and hence \( 2^{3^{100}} \equiv 2^{4k+1} \equiv 2^{4k} \cdot 2 \equiv 2 \pmod{5} \).

Answer: \( 2^{3^{100}} \equiv 2 \pmod{5} \).

(b) by part a) we know that \( 2^{3^{100}} \equiv 2 \pmod{5} \), i.e. \( 5 | (2^{3^{100}} - 2) \). Since \( 2^{3^{100}} - 2 \) is obviously even we also have that \( 2 | (2^{3^{100}} - 2) \). Since 2 and 5 are distinct prime numbers by a result from last homework this implies that \( 10 = 2 \cdot 5 \) also divides \( 2^{3^{100}} - 2 \), i.e. \( 2^{3^{100}} \equiv 2 \pmod{10} \)

Answer: The last digit of \( 2^{3^{100}} \) is 2.

(3) Find \( 1 + 2 + 2^2 + 2^3 + \ldots + 2^{19} \pmod{13} \).

Solution
Recall that we have proved a general formula that for any \( a \neq 1 \) and \( n \geq 1 \) we have

\[
1 + a + \ldots + a^n = \frac{a^{n+1} - 1}{a - 1}
\]

For \( a = 2, n = 219 \) this gives

\[
1 + 2 + 2^2 + 2^3 + \ldots + 2^{219} = \frac{2^{220} - 1}{2 - 1} = 2^{220} - 1
\]

Thus we need to find \( 2^{220} \pmod{13} \). By Fermat’s theorem we have \( 2^{12} \equiv 1 \pmod{13} \). We have \( 220 = 216 + 4 = 12 \cdot 18 + 4 \). Therefore

\[
2^{220} = (2^{12})^1 \cdot 2^4 \equiv 1 \cdot 16 \equiv 3 \pmod{13}
\]

and hence

\[
1 + 2 + 2^2 + 2^3 + \ldots + 2^{219} \equiv 2^{220} - 1 \equiv 3 - 1 \equiv 2 \pmod{13}
\]

**Answer:** \( 1 + 2 + 2^2 + 2^3 + \ldots + 2^{219} \equiv 2 \pmod{13} \).

(4) Prove the following result used in class.

Let \( a = p_1^{k_1} \cdot \ldots \cdot p_m^{k_m} \) where all \( p_i \) are prime and \( p_i \neq p_j \) for \( i \neq j \).

Suppose \( p_1^{t_1} \mid a \) where \( t_1 \) is a nonnegative integer.

Prove that \( t_1 \leq k_1 \).

**Solution**

Suppose \( t_1 > k_1 \) and \( p_1^{t_1} \mid a \). Then \( p_1^{t_1}d = a = p_1^{k_1} \cdot \ldots \cdot p_m^{k_m} \) for some integer \( d \). Dividing by \( p_1^{k_1} \), we get \( p_1^{t_1 - k_1}d = p_2^{k_2} \cdot \ldots \cdot p_m^{k_m} \). Since \( t_1 - k_1 > 0 \) this means that \( p_1 \) divides \( p_2^{k_2} \cdot \ldots \cdot p_m^{k_m} \). By a corollary to the Fundamental Theorem of Arithmetic, if a prime number \( p \) divides \( a_1 \cdot \ldots \cdot a_n \) then \( p \mid a_i \) for some \( i \). Since \( p_1 \) divides \( p_2^{k_2} \cdot \ldots \cdot p_m^{k_m} \) this implies that \( p_1 \mid p_i \) for some \( i \geq 2 \). This is a contradiction since \( p_1, \ldots, p_l \) are distinct primes.

Therefore, \( t_1 \leq k_1 \).  \( \square \).

(5) problem #17 from the book. We need to show that if \( 2^k + 1 \) is prime then \( k \) has no other prime divisors other than 2, i.e. \( k = 2^m \) for some \( m \). Suppose not. Then \( k = p_1 \cdot \ldots \cdot p_n \) where all \( p_i \) are prime and at least one \( p_i \neq 2 \).

Without loss of generality \( p_n \neq 2 \). Then \( p_n \) is odd as 2 is the only prime number which is even. Also \( p_n > 1 \).

We have \( k = (p_1 \cdot \ldots \cdot p_{n-1}) \cdot p_n = ab \) where \( a = p_1 \cdot \ldots \cdot p_{n-1} \) and \( b = p_n > 1 \) and is odd.

**Claim:** \( 2^a + 1 \) divides \( 2^k + 1 \). Indeed, we have \( 2^a \equiv -1 \pmod{2^a + 1} \) and therefore \( 2^k = (2^a)^b \equiv (-1)^b \equiv -1 \pmod{2^a + 1} \) since \( b \) is odd. Therefore, \( 2^a + 1 \) divides \( 2^k + (-1) = 2^k + 1 \) which proves the Claim.

Next observe that \( 2^a + 1 \) is odd, since \( a \geq 1 \). Also, \( 2^a + 1 < 2^k + 1 \) since \( k = ab > a \). This means that \( 2^k + 1 \) is not prime. This is a contradiction and therefore \( k \) has no other prime divisors other than 2.  \( \square \)